Cédula de Documento
Sellado

Información de Documento Sellado Digitalmente	
Entidad universitaria	Dirección General de Orientación y Atención Educativa
Nombre del documento	Documento de Seguridad de Datos Personales de la DGOAE_Censurado_Reducido_v2.pdf
Tipo de documento	Otro
Identificador único del documento	girPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Número de páginas	425
Fecha de emisión del sello	17 de agosto del 2022 a las 09:55 AM

Información de la Entidad Emisora del Sello	
Entidad universitaria	Coordinación de Sistemas DGOAE

Este es un comprobante de la recepción de un documento
emitido y sellado digitalmente en la UNAM.
Esta cédula es informativa y
no forma parte del documento sellado al que hace referencia.

Universidad Nacional Autónoma de México

DIRECCIÓN GENERAL DE ORIENTACIÓN Y ATENCIÓN EDUCATIVA

Documento de Seguridad de Datos Personales de la Dirección General de Orientación y Atención Educativa (DGOAE)

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Direción General de Orientación y Atención Educativa (DGOAE), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

mayo 2022.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —1 de 425—

ÍNDICE

INTRODUCCIÓN 3
DIRECCIÓN DE ORIENTACIÓN EDUCATIVA 4
PROGRAMA DE ACTUALIZACIÓN PARA ORIENTADORES 4
DIRECCIÓN DE BECAS Y ENLACE CON LA COMUNIDAD 5
SISTEMA INTEGRA 5
MÓDULO DE SOLICITUDES PARA SECE 38
DIRECCIÓN DE SERVICIO SOCIAL 48
SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL 48
CONTROL DE CONSTANCIAS 65
PERAJ UNAM 81
PREMIO AL SERVICIO SOCIAL "DR. GUSTAVO BAZ PRADA" 99
PROGRAMAS MULTIDISCIPLINARIOS 115
UNIVERSITARIOS POR LA EDUCACIÓN DE JÓVENES Y ADULTOS 126
IMPULSO AL DESARROLLO DE EMPRESAS SOCIALES 142
VOLUNTARIADO 152
DIRECCIÓN DE PLANEACIÓN 153
REGISTRO DE ACTIVIDADES EN LÍNEA 153
ENCUENTRO VIRTUAL DE EMPLEABILIDAD 174
SISTEMA DE INFORMACIÓN AUTOMATIZADA DE PRÁCTICAS PROFESIONALES 195
ESTRATEGIAS DE VINCULACIÓN E INSERCIÓN LABORAL 218
FERIA DEL EMPLEO 239
DIRECCIÓN DE APOYO TÉCNICO 259
PROGRAMA REGISTRO DEL PREMIO AL TALENTO BACHILLER UNIVERSITARIO 259
PROGRAMA REGISTRO DE LA PRESEA BERNARDO QUINTANA ARRIOJA 282
CENTRO DE ORIENTACIÓN EDUCATIVA (COE) 301
INSTRUMENTO MANUAL DE EVALUACIÓN PSICOLÓGICA EN LÍNEA MEPSI. 301
INSTRUMENTO PROUNAM II E INVOCA EN LÍNEA 328
INSTRUMENTOS DE ORIENTACIÓN EDUCATIVA. 357
CUESTIONARIO DE RESLIENCIA ESCOLAR 387
UNIDAD ADMINISTRATIVA 415
SISTEMA INSTITUCIONAL DE COMPRAS SIC 415
SISTEMA ADMININSTRATIVO INTEGRAL UNAM 416
SISTEMA INTEGRACIÓN DE PERSONAL 417
SISTEMA DE CONTROL PATRIMONIAL 418
REGISTRO REMOTO DE TRÁMITES PARA PAGO 419

ID del Documento: gIPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —2 de 425—

FACTURA FISCAL DIGITAL **420**
SISTEMA DE INFORMACIÓN DE LA ADMINISTRACIÓN UNIVERSITARIA **421**
APLICACIONES FINANZAS **422**
APROBACIÓN DEL DOCUMENTO DE SEGURIDAD **423**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —3 de 425—

Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de la Direción General de Orientación y Atención Educativa (DGOAE), con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

Este modelo pretende brindar a las áreas universitarias homogeneidad en la redacción, organización y contenido para que elaboren su propio documento de seguridad en el que se describan las tres medidas de seguridad para la protección de los datos personales.

El marco jurídico del documento de seguridad se regula por el capítulo II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, que establece un conjunto mínimo de medidas de seguridad que cada dependencia o entidad universitaria deberá considerar al perfilar su estrategia de seguridad para la protección de los datos personales bajo su custodia, según el tipo de soportes —físicos, electrónicos o ambos — en los que residen dichos datos y dependiendo del nivel de protección que tales datos requieran.

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC 27002:2013 "*Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información*".

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —4 de 425—

Dirección de Orientación Educativa

Programa de Actualización para Orientadores

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Orientación Eduicativa.**	
Identificador único*	**DGOAE-DOE-2022-01**
(Nombre del sistema A1	**Formulario: Registro de asistencia a videoconferencias del Programa de Actualización para Orientadores**
Datos personales (sensibles o no) contenidos en el sistema*:	**Para registro de primera vez:** Nombre completo, sexo, correo electrónico, nivel educativo en que se desarrolla Institución Educativa a la que pertenece, nivel educativo en que se desarrolla y función que desempeña. **Para Registros subsecuentes:** correo electrónico
Responsable*:	
Nombre*:	Mtro. Pedro Benítez Mejía
Cargo*:	**Jefe del Departamento de Informática**
Funciones*:	Generar y en su caso, actualizar y/o modificar el sistema del formulario para contar con un registro de asistencia por sesión, de los participantes en el Programa de Actualización de la Dirección de Orientación Educativa.
Obligaciones*:	Mantener a buen resguardo la información generada por este formulario, así como realizar las actualizaciones o modificaciones requeridas por la Dirección de Orientación Educativa y en su caso, compartir la base de datos de los asistentes para generar las constancias correspondientes.
	Encargado:
(Nombre)	Lic. Marco Antonio Bonaparte Madrigal
Cargo*:	**Jefe de Departamento de Programas y Proyectos de Orientación Educativa**
Funciones*:	Acceder a la base de datos para generar los reportes estadísticos requeridos en la MIR, así como para solicitar las constancias de asistencia para los docentes que participan en esta actividad.
Obligaciones*:	Revisar cada ciclo del evento si se debe hacer alguna modificación al sistema y en su caso solicitarlo al área correspondiente, así como acordar con el responsable las fechas en que se va a requerir, los horarios en que se debe

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —5 de 425—

	abrir y cerrar y mandar los datos que éste requiera para actualizar la presentación de este.

Dirección de Becas y Enlace con la Comunidad

Sistema Integra

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.	
Identificador único*	**DGOAE-DBEC–2022-01**
(Nombre del sistema) *	**Sistema Integra**
Datos personales (sensibles o no) contenidos en el sistema*:	• **Datos de identificación para registro de usuario en el portal web Integra:** Nombre completo, número de cuenta, plantel, nivel escolar y, en su caso, carrera de estudios, CURP, género, teléfono fijo o celular y dirección de correo electrónico. • **Información personal:** si pertenece a un pueblo indígena, nombre del pueblo indígena al que pertenece, si habla una lengua indígena, si tiene alguna discapacidad y de que tipo, estado civil, número de hijos, si está embarazada, si fue beneficiaria de beca de madres embarazadas, si está inscrita en el registro nacional de víctimas, si es migrante y beneficiario de un programa de atención migrante, teléfonos casa y celular. • **Información del domicilio:** estado, municipio o delegación, asentamiento, tipo de vialidad, dirección con número, vialidades colindantes y descripción de la ubicación. • **Información académica:** turno de inscripción, si eres egresado de la UNAM, mes y año de egreso, si cuenta con título profesión, mes y año de titulación. • **Vinculación escolar:** tiempo transcurrido una vez terminados tus estudios, tipo de ocupación o trabajo, número de horas trabajadas al día, número de días trabajados a la semana, salario o percepción mensual. • **Apoyos escolares:** si recibe o ha recibido alguna beca, nombre de la organización que otorgó la beca, de qué forma se recibe o recibió la beca, nivel educativo en el que se recibió la beca, frecuencia temporal de su recepción, recepción de algún crédito educativo, quién, y de qué forma lo otorgó, si suspendió estudios por más

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —6 de 425—

	de 6 meses y si el motivo fueron problemas económicos, si ha recibido ayuda económica de un extranjero. • **Desempeño laboral:** si trabaja, ocupación a la que se dedica, puesto, tipo de percepción laborales que recibe, si goza de servicio médico, número de horas que trabaja al día, número de días trabajados a la semana, salario o percepción mensual. • **Información del hogar:** número de personas que viven en tu hogar, número de personas que aportan al ingreso familiar mensual, comprobantes de ingreso mensual neto, si es el jefe(a) de familia, persona que toma decisiones en el hogar y que tipo de ocupación tiene, tipo de contratación laboral, civil o irregular, si goza de servicio médico, número de horas que trabaja al día, número de días trabajados a la semana, monto de salario o percepción mensual. • **Vivienda:** Familiares beneficiados de programa prospera, si es/fue beneficiario del Programa Prospera, materiales de elaboración de la vivienda, número de habitaciones de la vivienda, habitaciones utilizadas como dormitorios, número de servicios sanitario, tipo de servicio sanitario, servicio sanitario compartido, servicio de drenaje en la vivienda, procedencia del agua potable, existencia del servicio de luz eléctrica, cantidad de luminarias, tipo de combustible para cocinar, cantidad de teléfonos celulares en la familia, cantidad y/o existencia de personas en servicio doméstico. • **Bienes:** Tipo de enseres domésticos, tipo de mobiliario de casa, tipo de equipo audiovisual, tipo y cantidad de automóviles. • **Gasto:** Cantidad de dinero utilizada en alimentos y bebidas, cantidad de dinero utilizado en: servicios de educación, compra de artículos de cultura-recreación, pago de servicios, compra de prendas de vestir, servicio médico, mantenimiento y servicio vehicular. • **Becas:** Información de acceso a la beca, razones para solicitar una beca y uso o destino de la beca. • **Datos familiares:** De los padres o tutores: nombres completos, escolaridad y si feneció. • **DGECI:** • **PUIC**:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —7 de 425—

Responsable*:	
Nombre*:	**Mauricio Reyna Lara**
Cargo*:	**Director de Becas y Enlace con la Comunidad**
Funciones*:	• Coordinar y supervisar que la información sea enviada a la comunidad estudiantil de la UNAM por los medios oficiales y autorizados (página web, redes sociales, correo electrónico). • Fungir como enlace ante la Entidad Federativa que corresponda, para los procesos de reglas de operación. • Elaborar los proyectos de convocatorias operadas por la Dirección y coordinar los trabajos con las dependencias externas e internas cuando sea necesario; así como establecer los mecanismos y medios para difundirlas oportunamente entre los aspirantes a obtener una beca de Bachillerato, Licenciatura o Posgrado. • Coordinar y supervisar la recepción de solicitudes de beca que se realicen a través del Sistema INTEGRA o aquel sistema que se estipule con las dependencias externas. • Establecer los mecanismos que permitan realizar la verificación y el seguimiento de la situación socioeconómica del aspirante a becario, así como la documentación probatoria de ingresos familiares y/o del solicitante. • Verificar la adecuada aplicación de los mecanismos para evaluar las solicitudes de beca e información académica y socioeconómica proporcionada por los

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —8 de 425—

	aspirantes. • Diseñar y aplicar mecanismos y sistemas para la asignación de becas y para el seguimiento del desempeño académico de los beneficiarios. • Supervisar que el pago de las becas se realice en tiempo y forma de acuerdo con las fechas establecidas por cada programa. • Coordinar la elaboración del informe anual sobre el seguimiento de los beneficiarios, el otorgamiento de becas, la evaluación del programa y el uso de los recursos. • Coordinar y administrar el proceso de asignación de tutores a los becarios de los diferentes programas de becas tanto de bachillerato como de licenciatura. • Instrumentar mecanismos de apoyo que atiendan necesidades de los becarios en materia personal y escolar. • Coordinar la atención oportuna de las solicitudes de información de la UNAM o del Comité Técnico, sobre los programas de becas, los becarios y sus expedientes académicos. • Implementar y coordinar los mecanismos de colaboración con entidades de los sectores público, social y privado que faciliten el financiamiento de los programas de becas. • Realizar todas aquellas actividades que le sean encomendadas por la Dirección General.
Obligaciones*:	

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —9 de 425—

Encargados[1]:	
Nombre*:	**Antonio Baruch Cuevas Ortiz**
Cargo*:	**Coordinador**
Funciones*:	• Definir los estándares de Desarrollo que serán utilizados por el equipo de desarrollo. • Planear, organizar, coordinar y supervisar el desarrollo del sistema integra de la DGOAE. • Definir las funciones y niveles de acceso a la información del sistema de acuerdo con los perfiles de los usuarios.
Obligaciones*:	• Asegurar el correcto funcionamiento del sistema Integra • Coordinar la Implementación de las medidas de seguridad Administrativas, Físicas y Técnicas aplicables en el sistema Integra, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que contiene.
Usuarios:	
(Nombre del Usuario 1*)	**Dora Fuentes Arriaga**
Cargo*:	**Jefa de departamento de Seguimiento y Evaluación**
Funciones*:	• Fungir como operadora y dar seguimiento a aquellas modalidades de becas que le asigne la Dirección de Becas y Enlace con la Comunidad con las dependencias internas o externas que participen en los diferentes procesos. • Planear, operar y asignar a los beneficiarios de las modalidades de Beca que le sean asignadas por la Dirección de Becas y Enlace con la Comunidad. • Gestionar los medios de pagos para los beneficiarios correspondientes a cada ciclo escolar, así como programación de los pagos de las modalidades que le sean asignadas por la Dirección de Becas y Enlace con la Comunidad. • Confrontar los padrones con las diferentes instituciones y dependencias. • Revisar y coordinar la actualización permanente de la información del Sistema Universitario de Información de Becas de la UNAM.

[1] Se tienen que ingresar los datos de todos los Encargados del sistema de tratamiento de datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —10 de 425—

	• Efectuar el seguimiento académico de los programas de becas a fin de contar con indicadores que permitan medir su eficiencia e impacto.
Obligaciones*:	
(Nombre del Usuario 2*)	**Fernando Misael Castro Fernández**
Cargo*:	**Jefe de Departamento de Becas**
Funciones*:	• Asignar las becas de manera transparente con apego a los proceso y normatividad que regulan los diferentes programas. • Coordinar el seguimiento de programas que coadyuven a la formación integral de los alumnos becarios de Bachillerato, Licenciatura y Posgrado de la UNAM. • Coordinar el manejo de incidencias de los programas de suspensión, cancelación y prórroga de becas. • Coordinar en conjunto con la DGAE la actualización de los datos académicos de los becarios y la documentación respectiva. • Coordinar y supervisar los procesos para definir e implementar los medios de pago para los beneficiarios de los distintos programas, de conformidad con los lineamientos y la normatividad de cada convocatoria. • Supervisar la operación del programa beca idioma. • Establecer vínculos e implementar acciones con las entidades académicas. • Garantizar la confidencialidad de la información de los becarios remitida a la Fundación UNAM AC, las instituciones bancarias que participan en los programas de becas y aquellas instituciones internas y gubernamentales que participen en los procesos de becas. • Garantizar la confidencialidad de la información de la base de datos de los solicitantes y los becarios incluyendo los aspectos personales, académicos y de apoyo económico en concordancia con el marco normativo aplicable. • Colaborar en las actualizaciones y mejoras del Sistema INTEGRA. • Colaborar en la implementación de mecanismos para generar las estadísticas sobre el uso y manejo del Sistema INTEGRA. • Operar los Programas de Becas para Estudiantes de Bachillerato, Licenciatura y Posgrado que le sean asignados por la Dirección de Becas y Enlace con la Comunidad.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —11 de 425—

	• Operar el Programa de becas para estudio de idiomas. • Realizar todas aquellas actividades que le sean encomendadas por la Dirección de Becas y Enlace con la Comunidad.
Obligaciones*:	
(Nombre del Usuario 3*)	**Esperanza Vitela Ibañez**
Cargo*:	**Jefa de Departamento de Enlace con la Comunidad**
Funciones*:	• Dirigir interfaz, para operar el servidor por el cual se enviará la información a los correos electrónicos de la comunidad estudiantil de la UNAM. • Supervisar el funcionamiento del hardware y software para lograr que la comunicación entre el servidor y el exterior se mantenga activa y disponible de manera permanente. Supervisar la actualización de la base de datos de correos electrónicos de la comunidad estudiantil de la UNAM para el envío de información electrónica. • Fungir como enlace y responsable de la operación en aquellas modalidades de becas que la Dirección de Becas y Enlace con la Comunidad, le asigne, ya sea con instituciones internas o externas de la UNAM. • Diseñar las bases de datos bajo la plataforma más adecuada para estar en condiciones de realizar el correo masivo a la comunidad estudiantil Iniciación, Bachillerato, Licenciatura y Posgrado de la UNAM. • Vigilar que la comunicación sea permanente con las direcciones que ofrecen servicios a la comunidad estudiantil de la UNAM para identificar la información relevante que les pudiera ser transmitida. • Actualizar y dar mantenimiento permanente al Sistema de Enlace con la Comunidad Estudiantil (SECE), para garantizar un servicio de calidad y eficiente para la comunidad estudiantil. • Analizar y difundir en su totalidad las solicitudes de difusión de información vía correo electrónico por medio del SECE. • Asegurar la confidencialidad de las cuentas de correo y la información manejada. • Asegurar el resguardo del hardware conforme a los lineamientos establecidos por la Administración Central.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —12 de 425—

	• Mantener e impulsar el uso de las redes sociales para la comunicación con los estudiantes por medio del Sistema de Enlace con la Comunidad Estudiantil. • Administrar las redes sociales del área de Becas como Facebook, YouTube y Twitter. • Diseñar y editar las convocatorias a publicar. • Diseñar y editar los videos informativos y promocionales de cada una de las convocatorias. • Operar las convocatorias de becas, asignadas por la Dirección de Becas y Enlace con la Comunidad, desempeñando como enlace con las instituciones internas o externas de la UNAM. • Realizando todas aquellas actividades que le sean encomendadas por la Dirección de Becas y Enlace con la Comunidad.
Obligaciones*:	

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.	
Identificador único**	DGOAE-DBEC-2022-01
Nombre del sistema DGOAE-1*	Sistema Integra
Tipo de soporte:*	El sistema se encuentra en soporte electrónico.
Descripción:*	Base de datos relacional en MySQL

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —13 de 425—

Características del lugar donde se resguardan los soportes:*	Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico: • **El personal registra fecha y hora de entrada/salida.** • **Registra equipo de cómputo externo.** • **El acceso es con credencial de la institución.** • **Existe vigilancia de personal autorizado y cámaras de video.** Nivel 2: Seguridad en la infraestructura del hardware: • **Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido.** • **El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores.** • **Etiquetado en los cables de conexión.** Nivel 3: Seguridad en la infraestructura del software: • **Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware.** • **Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red.** • **Restricción en los puertos de entrada/salida por dirección IP** • **Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos del Sistema Integra.** Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. **Nivel 5: Seguridad en la aplicación:** • **Control de accesos a usuarios dependiendo del tipo de rol asignado.** ✓ **Estudiantes requiere usuario y contraseña.**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —14 de 425—

	✓ **Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida.** • **Desarrollo e implementación del módulo que administra auditorias por usuario, nombre de módulo y dirección IP.** **Nivel 6: Seguridad en la Base de Datos:** • **Acceso restringido por usuario y dirección IP de acceso local.** • **Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol que tiene los desarrolladores.** • **La información se recibe y envía cifrada en 128 bits.** • **La base de datos guarda registros auditables.** • **Respaldos de Base de Datos**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —15 de 425—

DIAGRAMA DE NIVELES DE SEGURIDAD DEL SISTEMA

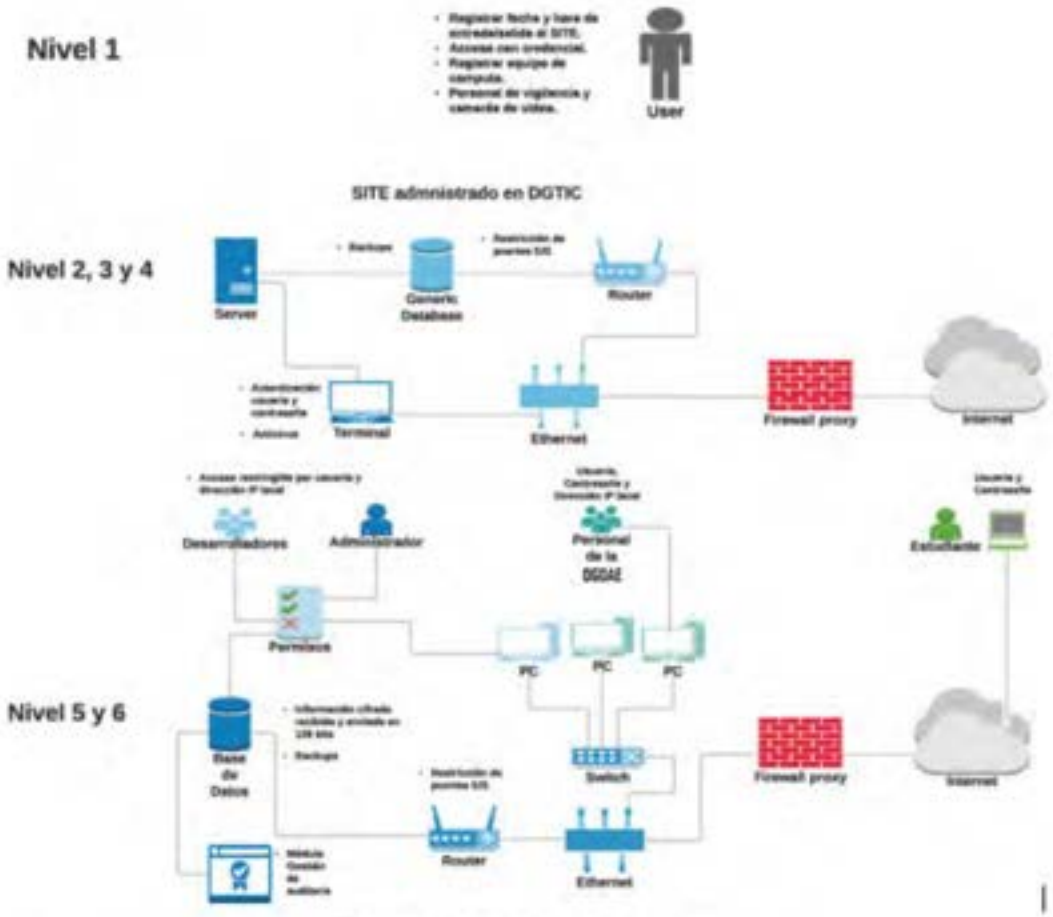
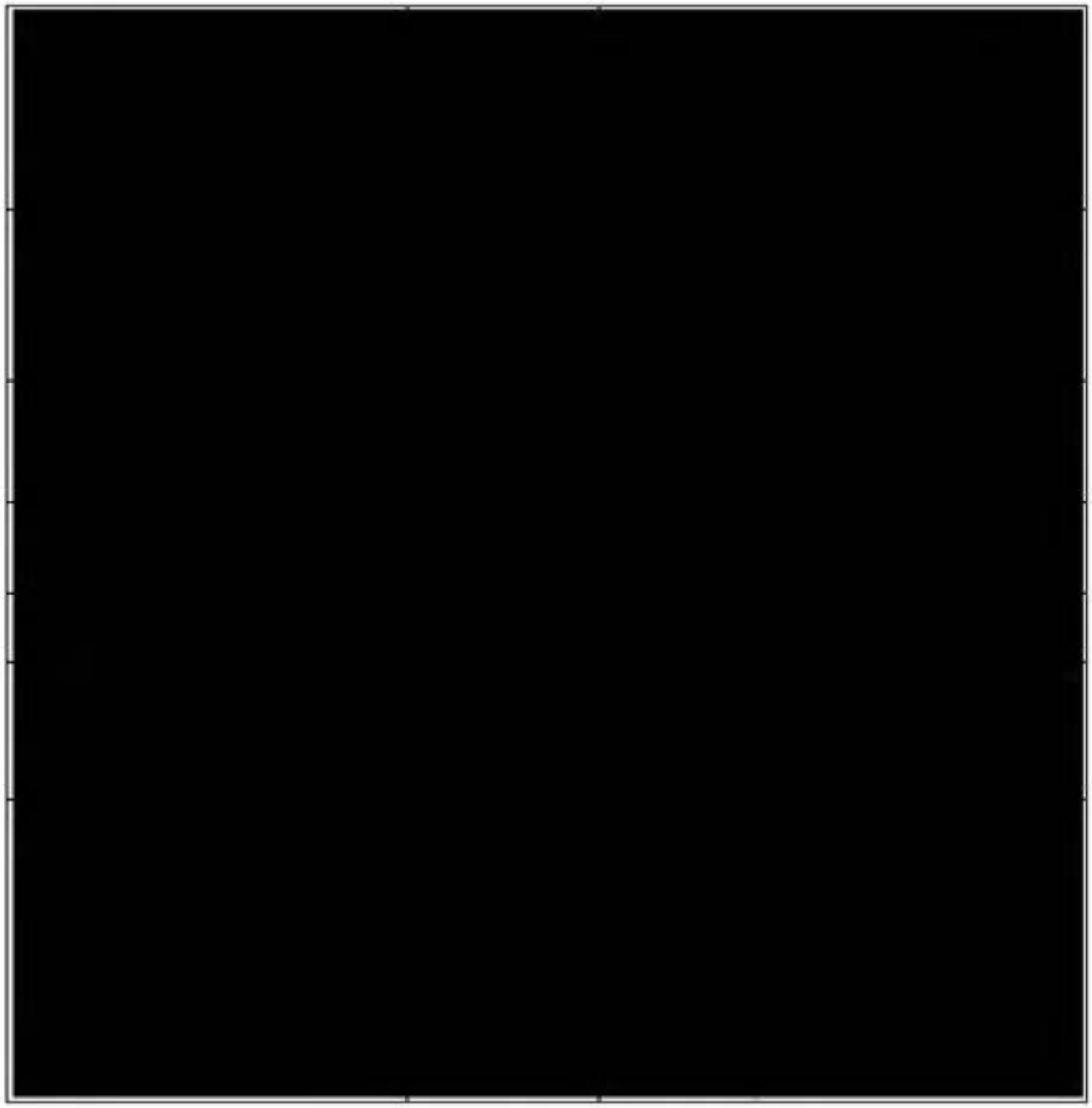


Ilustración 1 - Niveles de Seguridad

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	**DGOAE-DBEC–2022-01**	
Nombre del sistema DGOAE-1*	**Sistema Integra**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —16 de 425—



4. Análisis de brecha

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	DGOAE-DBEC–2022-01	
Nombre del sistema *	**Sistema Integra**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —17 de 425—

[redacted]

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.			
Identificador único*	**DGOAE-DBEC–2022-01**		
Nombre del sistema *	**Sistema Integra**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

6. Medidas de seguridad implementadas

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 18 de 425 —

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.	
Identificador único*	**DGOAE-CS–2017-01**
Nombre del sistema DGOAE-1*	**Sistema Integra**
TRANSFERENCIAS DE DATOS PERSONALES - BECA BENITO JUÁREZ	
Transferencias mediante el traslado de soportes físicos:	El intercambio con la Coordinación Nacional de Becas para el Bienestar Benito Juárez (CNBBBJ), es por medio de oficio, con mensajería institucional. Cuando es requerido por la Coordinación, que es la que asigna y dispersa la beca.
Transferencias mediante el traslado de soportes electrónicos:	La validación de los alumnos para la asignación de la beca es por medio del Sistema de Reinscripción Electrónica de la Coordinación Nacional. Cada plantel sube al sistema en formato Excel a los alumnos inscritos, reinscritos, cambios de plantel y bajas. Todo lo relacionado a la beca esta suscrito por un convenio firmado entre la UNAM y la CNBBBJ.
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza transferencia de datos a los Enlaces de becas de cada plantel por medio de correo electrónico, en formato .ZIP Lo anterior para dar a conocer los aceptados o bien a los alumnos que están inscritos. La solicitud de la inscripción es compartida por DGAE a la Dirección de Becas y Enlace con la Comunidad se hace por servidor FTP.

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.	
Identificador único*	**DGOAE-CS–2017-01**
Nombre del sistema DGOAE-1*	**Sistema Integra**
TRANSFERENCIAS DE DATOS PERSONALES - BECA MANUTENCIÓN	
Transferencias mediante el traslado de soportes físicos:	**1.** El envío de la información cuando se refiere a soportes físicos se realiza a través del servicio de mensajería de la dependencia proporcionado por el Departamento de Bienes, Suministros y Servicios Generales. **2.** La correspondencia cuando contiene padrones, o

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 19 de 425—

	documentación que incorpore datos personales de los alumnos(as) se protege en un sobre cerrado y engrapado o en ocasiones sellado con cinta adhesiva; de esta manera es posible identificar si este fue abierto antes de su entrega. **3.** Regularmente la correspondencia (que en este caso va en sobre cerrado y sellado) se entrega en la oficialía de partes u oficina de correspondencia de la dependencia, acusando la recepción de este con el mensajero. **4.** El departamento de becas si solicita que se informe inmediatamente en caso de que el sobre o paquete presente alguna alteración o daño. **5.** Deberá informar si el destinatario envía acuse de recibo al remitente una vez recibidos los datos personales, y **6.** El área de control de gestión de las instancias a donde se realizan las transferencias de datos lleva un control de la documentación que ingresa de forma general y cada área o departamento en particular lleva su propia bitácora de recepción. **7.** Todas las transferencias que se realizan con las dependencias o instituciones se encuentran justificadas mediante la celebración del instrumento jurídico respectivo, el cual se renueva de manera constante dependiendo de las necesidades del área y de los programas de beca vigentes.
Transferencias mediante el traslado de soportes electrónicos:	**a)** El envío de la información cuando se refiere a soportes físicos se realiza a través del servicio de mensajería de la dependencia proporcionado por el Departamento de Bienes, Suministros y Servicios Generales. La correspondencia cuando contiene padrones, o documentación que incorpore datos personales de los alumnos(as) se protege en un sobre cerrado y engrapado o en ocasiones sellado con cinta adhesiva; de esta manera es posible identificar si este fue abierto antes de su entrega. Regularmente la correspondencia (que en este caso va en sobre cerrado y sellado) se entrega en la oficialía de partes u oficina de correspondencia de la dependencia, acusando la recepción de este con el mensajero. El departamento de becas si solicita que se informe inmediatamente en caso de que el sobre o paquete presente alguna alteración o daño. El área de control de gestión de las instancias a donde se realizan las transferencias de datos lleva un control de la

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —20 de 425—

	documentación que ingresa de forma general y cada área o departamento en particular lleva su propia bitácora de recepción. **b)** Los archivos electrónicos que contienen datos personales son enviados con contraseña, para su protección. **c)** Todas las transferencias que se realizan con las dependencias o instituciones se encuentran justificadas mediante la celebración del instrumento jurídico respectivo, el cual se renueva de manera constante dependiendo de las necesidades del área y de los programas de beca vigentes
Transferencias mediante el traslado sobre redes electrónicas:	**a)** Envío de datos con archivos con contraseña; **b)** Deberá precisar si utiliza un canal de comunicación dedicado o una red privada virtual especificando detalles técnicos relativos al cifrado de dicho canal como la longitud de llave (o clave); en su caso, deberá precisar si para dicho canal utiliza una red pública (como Internet) especificando el protocolo de transferencias protegidas utilizado; **c)** Deberá manifestar si el remitente y/o el destinatario cuentan con dispositivos que faciliten la detección de intrusiones en el canal de comunicaciones. **d)** El destinatario envía acuse de recibo al remitente una vez recibidos los datos personales y **e)** El remitente registra la o las transferencias en su bitácora, pudiendo ser por oficio o correo electrónico **f)** Todas las transferencias que se realizan con las dependencias o instituciones se encuentran justificadas mediante la celebración del instrumento jurídico respectivo, el cual se renueva de manera constante dependiendo de las necesidades del área y de los programas de beca vigentes.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

Las renuncias los alumnos las hacen llegar de manera digital al correo electrónico en formato PDF.

1. Respecto de este punto, informamos que los expedientes físicos de los alumnos y/o documentación que contiene información personal y/o confidencial, se encuentra mayormente resguardada en una bodega dentro de la dependencia, la cual se encuentra bajo llave, misma que tiene a su cargo el

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 21 de 425 —

Jefe del Departamento de Becas y de manera ocasional quien el instruya derivado de sus funciones o de las tareas propias del departamento.

2. Tienen acceso a la bodega en donde se encuentra la documentación física las siguientes personas:

Nombre	Cargo
1.- Fernando Misael Castro Fernández (resguarda la llave)	Jefe del Departamento de Becas
2.- Vanesa Cortés Esparza	Jefe de Área
3.-Patsy Guadalupe Aguirre Ramos (solo por instrucción)	Asistente de Procesos
4.-María del Carmen Domínguez Sánchez (Sólo por instrucción)	Asistente de Procesos
5.-Rocío Torres (sólo por instrucción)	Asistente de Procesos

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) El sistema Integra cuenta con Auditoria de movimientos en donde se almacena la fecha, hora, tipo de movimiento, descripción, usuario que lo realiza y Dirección IP.

b) No se cuenta con expedientes físicos.

c) El sistema Integra cuenta con Auditoria de movimientos y un módulo de reportes, donde se puede realizar la búsqueda de movimientos , el reporte incluye la fecha, hora, tipo de movimiento, descripción, usuario que lo realiza y Dirección IP.

2. Las bitácoras están en soporte electrónico.

3. La bitácora de movimientos se almacena en la Base de Datos.

4. La integridad de las bitácoras sé asegura con:

- Acceso restringido por usuario y dirección IP de acceso local y privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol que tiene los desarrolladores.
- La información se recibe y envía cifrada en 128 bits.
- La base de datos guarda registros auditables.
- Los respaldos de base de datos se realizan diariamente de manera automática a las 00:00 horas, etiquetándolos con la fecha de respaldo, ejemplo bd_integra_23052019_00:01:01.sql.gz.
- El respaldo de información se almacena en una NAS asignada por DGTIC.
- Todos los viernes se realiza una copia de los respaldos en un disco duro externo de 2Tb.

ID del Documento: gIPdH8ZIn+0FpWtuTZETKtsDSzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —22 de 425—

- En el caso de que no se puedan hacer los respaldos por algún problema con el Servidor (Virus o falla en unidad de almacenamiento) se procede a realizarlos al día siguiente.

5. Respecto del análisis de las bitácoras:

a) La coordinación de Sistemas de la DGOAE es responsable de analizar las bitácoras, cada que se presenta algún incidente o reporte por parte de los usuarios.

b) Para revisar las bitácoras se utilizan gestores de base de datos como Heidi SQL y Navicat).

IV. REGISTRO DE INCIDENTES

En caso de presentar un incidente seguir los siguientes pasos.

1. Resolver el incidente
2. Pedir el archivo en formato electrónico "Registro de incidentes de datos personales" (pdf).
3. Recopilar la siguiente información:
    a. Resumen del incidente
    b. Resumen de cómo se solucionó el incidente
    c. Especificar si el incidente daño algún archivo, base de datos, servidor, respaldo etc.
    d. Fecha de inicio
    e. Fecha de término o resolución del incidente
    f. El impacto del incidente
    g. La persona quien resolvió el incidente
    h. Nombre del responsable y firma
4. El archivo de registro se actualiza y se crea un respaldo en un soporte electrónico portable para su almacenamiento.
5. La resolución del incidente tiene un tiempo máximo de 3 días hábiles.
6. El encargado de sistema deberá de registrar el incidente en un archivo donde se encuentre el resumen de lo sucedido.
7. Si el incidente es un robo o extravío de información se deberá reportar inmediatamente a los encargados y responsables del sistema, ellos avisaran al titular y a los encargados en la UNAM de lo sucedido.

La recuperación de datos de los sistemas de respaldo la podrá solicitar los encargados y el responsable del sistema.

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —23 de 425—

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos,

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 24 de 425—

centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de video vigilancia, entre otras medidas.

NOTA: cada dirección de departamento, es responsable de su archivo físico, la dependencia no cuenta con un área y personal exclusivo para el almacenamiento de archivos físicos, en el caso del centro de datos para soportes electrónicos, se tendrá que ver con el área de informática.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Las personas a quienes atendemos son: alumnado, egresadas y egresados de la UNAM.

2. ¿Cómo las autentifica?
   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.
3. ¿Cómo les autoriza el acceso?
   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En el caso de que un titular identifique que sus datos personales son incorrectos, se podrá hacer un cambió si y solo si el titular sigue el siguiente protocolo:

1. Obtener y llenar el documento del ANEXO II donde el titular requiere una actualización en los datos personales.
2. Mandar al correo dgoae.sistemas@unam.mx lo siguiente:
   a. Adjuntar el documento firmado del ANEXO II en el correo electrónico, junto con identificación oficial, para validar la identidad
3. El titular recibirá un correo donde se le avisará de la recepción del correo en un tiempo aproximado de 3 días hábiles.
4. Esperar el aviso dé que se realizó el cambio en los datos personales solicitados
5. Revisar que el cambió se realizó correctamente.
   a. Se tiene un tiempo de espera de 2 días hábiles para cualquier corrección de los datos que se cambiaron.
   b. SI todo es correcto, dejar como está.

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 25 de 425 —

c. Si hay algún dato que no se cambió, favor de enviar el dato incorrecto con el correcto como respuesta del aviso. Y verificar nuevamente. Estos cambios se deben de realizar en menos de 12 horas.

Para los responsables y encargados de cambiar los datos, seguir el siguiente protocolo.

1. Al recibir el correo, el encargado responderá al titular:
   a. El cambio se realizará dentro de 3 días hábiles.
   b. Hay que informar que persona va a realizar el cambio, deberá ser la misma que mande la respuesta de los días hábiles.
2. Levantar un reporte de la incidencia.
3. Se realiza el cambio.
4. Se envía un correo para que el titular verifique que el cambio se hizo correctamente pidiendo que mande una respuesta si el cambio se hizo correctamente o no.
   a. Si se recibe una respuesta afirmativa, ponemos fin a la incidencia.
   b. Si se recibe un correo donde sigue la inconsistencia en los datos, revisar de nuevo la petición y hacer el cambio inmediatamente y volver a confirmar que se realizó el cambio.
   c. Si no se recibe el correo, después de dos días del envío del correo de verificación de la realización de cambios en los datos personales. Podemos poner fin a la incidencia.
   d. Si llegara la información después de los dos días hábiles el titular deberá de volver a pedir el cambio.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. El sistema INTEGRA maneja un Modelo de control de acceso basado en roles de usuario, cada rol tiene acceso a diferentes módulos, dependiendo de los privilegios
2. No se cuenta con perfiles de usuario y contraseñas en el sistema operativo de red
3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **SI**

   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

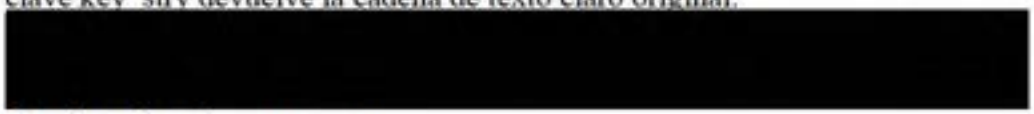
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —26 de 425—

Encriptación de datos personales y datos sensibles.
El sistema Integra implementa el algoritmo oficial AES (Advanced Encryption Standard), para el cifrado y descifrado de los datos sensibles que se almacenan en el sistema, utilizando una longitud de clave de 128 bits.

AES_ENCRYPT () encripta la cadena str usando la cadena de clave key_str y devuelve una cadena binaria que contiene la salida encriptada.



AES_DECRYPT () descifra la cadena cifrada crypt_str utilizando la cadena de clave key_str y devuelve la cadena de texto claro original.



Encriptación de contraseñas
El sistema integra utiliza encriptación de contraseña mediante pasword_hash, el cual crea un nuevo hash de contraseña usando un algoritmo fuerte de único sentido.



4. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles? **El Administrador del sistema**
   b) ¿Quién autoriza la creación de nuevos perfiles? **Se reciben las solicitudes de acceso al siostema por oficio.**
   c) ¿Se lleva registro de la creación de nuevos perfiles? **SI, en el propio sistema**

5. Acceso remoto al sistema de tratamiento de datos personales:
   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? NO
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **SI, solo los administradores de la base de datos puede entrar por este medio**
   c) ¿Cómo se evita el acceso remoto no autorizado? **Mediante la autenticación por llaves Publica y Privada y por IP**

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —27 de 425—

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Para que asegurar que la información personal, académica, socio - económica y financiera de los estudiantes no se pierda y esté disponible en caso de desastre, o cualquier contingencia, como daño en los discos duros, o eliminación accidental de la información o bien un caso de desastre físico, a continuación, se detalla el plan de respaldo de información.

Archivos

- Los respaldos de los archivos que se cargan en el servidor se harán diariamente, a las 23:50 horas, etiquetándolos con la fecha de respaldo, ejemplo archivos_23052019_23:50:01.tar.gz.
- El respaldo de información se almacena en una NAS asignada por DGTIC.
- Se realiza una copia de los respaldos en un disco duro externo de 2Tb.
- En el caso de que no se puedan hacer los respaldos por algún problema con el Servidor (Virus o falla en unidad de almacenamiento) se procede a realizarlos al día siguiente.

Aplicación

- Los respaldos de la aplicación se harán semanalmente, los viernes a las 23:55 horas, etiquetándolos con la fecha de respaldo, ejemplo aplicacion_integra_23052019_23:55:01.tar.gz.
- El respaldo de información se almacenará en una NAS asignada por DGTIC.
- Se realizará una copia de los respaldos en un disco duro externo de 2Tb.
- En el caso de que no se puedan hacer los respaldos por algún problema con el Servidor (Virus o falla en unidad de almacenamiento) se procede a realizarlos al día siguiente.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 28 de 425—

Base de Datos

- Los respaldos de base de datos se harán diariamente a las 00:00 horas, etiquetándolos con la fecha de respaldo, ejemplo bd_integra_23052019_00:01:01.sql.gz.
- El respaldo de información se almacenará en una NAS asignada por DGTIC.
- Se realizará una copia de los respaldos en un disco duro externo de 2Tb.
- En el caso de que no se puedan hacer los respaldos por algún problema con el Servidor (Virus o falla en unidad de almacenamiento) se procede a realizarlos al día siguiente.

Respaldos Automáticos

Para realizar el respaldo automático de los archivos se programó un script bash con el siguiente código:



Para realizar el respaldo automático de la aplicación se programó un script bash con el siguiente código:



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —29 de 425—

Para realizar el respaldo automático de la Base de Datos se programó un script bash con el siguiente código:

Posteriormente se programó una tarea automática en el crontab para que se ejecute automáticamente



IX. PLAN DE CONTINGENCIA

A continuación, se describe el Plan de contingencia que garantiza la continuidad de la operación del sistema. INTEGRA.

- Descargar y descomprimir los respaldos de la base de datos y de la aplicación.
- Ponerse en contacto con el jefe del departamento del Centro de Datos de DGTIC, para solicitar una máquina virtual para montar el sistema INTEGRA.
- Los requerimientos con los que debe contar este espacio son los mismos con los que contaba el sistema a recuperar, previo al problema.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —30 de 425—

- El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
- DGTIC entrega la máquina virtual, únicamente con el sistema operativo CENTOS7 instalado, proporciona usuario y contraseña con privilegios de root, ya que la administración y configuración del servidor la lleva la Coordinación de Sistemas.
- La coordinación de sistemas se encarga de instalar y configurar las herramientas necesarias, montar los respaldos de base de datos y aplicación, para poner en línea nuevamente el sistema INTEGRA.
- Se realizan las pruebas funcionales para garantizar la correcta operación del sistema INTEGRA.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa (DGOAE) **Dirección de Becas y Enlace con la Comunidad.**		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema	**Sistema Integra**	
Recurso*	**Descripción***	**Control***
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicaran el tráfico que existen en el servidor	Se hace manual y solamente será usada cuando se genere un ataque al sistema
Bitácoras generadas por el servidor	Las bitácoras generadas por el servidor nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas en la base de datos	Se crearán tablas donde se maneja que acciones el	Se usa SQL para el registro de la actividad dentro de la base.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 31 de 425—

	usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	
Ambiente de pruebas	Se cuenta con un ambiente de QA donde se pueden hacer pruebas de la funcionalidad	Se tiene un ambiente de QA, el cual es una replica de producción para poder hacer las pruebas necesarias.
Monitorización de servicios con Check_MK	El monitoreo de servicios del servidor mediante Check_MK, permite supervisar los servicios SMTP, HTTP, POP,. - Supervisar los recursos del servidor como CPU, Memoria, Swap	La herramienta de monitoreo Check_MK implementada por DGTIC, se utiliza para realizar el monitoreo de recursos del servidor.

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa (DGOAE) **Dirección de Becas y Enlace con la Comunidad.**		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema DGOAE-1*	**Sistema Integra**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Contar con las medidas de seguridad que DGTIC pide.	Se seguirán las recomendaciones que DGTIC propone para la seguridad en los sistemas	Administrador del Sistema
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones	Administrador del Sistema
Lista de verificación de seguridad	Diseñar un documento donde llevemos una lista de verificación sobre las reglas de seguridad que debe de tener el sistema	Administrador del Sistema

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa (DGOAE)

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —32 de 425—

Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema	**Sistema Integra**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Evaluación del sistema integra por el CERT UNAM de DGTIC.	Se encontraron algunas vulnerabilidades en las pruebas de penetración y detección de vulnerabilidades	Administrador del sistema

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema	**Sistema Integra**	
Medida de seguridad*	**Acciones***	**Responsable***
Implementación de las recomendaciones emitidas por el CERT UNAM.	*Se atendieron las recomendaciones emitidas por el CERT- UNAM para garantizar la seguridad del sistema INTEGRA.*	*Administrador del sistema*

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.			
Identificador único*	**DGOAE-CS–2017-01**		
Nombre del sistema DGOAE-1*	**Sistema Integra**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la protección de datos personales.	*Concientizar a los usuarios de la DGOAE, para conocer que son los datos*	*Duración: Un día*	*Todo el personal de la DGOAE.*

ID del Documento: gIrPdH8ZIni+0FpWluTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —33 de 425—

	personales y como se deben proteger.		
Medidas de seguridad técnico, administrativas y físicas en la PDP.	*Estructura de las normas complementarias y sus Anexos Técnicos*	*Duración: dos semanas*	*Todo el personal de la DGOAE que sea responsable de la protección de datos en sus respectivas áreas.*
Seguridad de Sistemas de Información.	*Introducción a la seguridad en sistemas de información*	*Duración: un mes*	*Personal Técnico de la DGOAE que sea responsable de la protección de datos en sus respectivas áreas.*
Análisis de riesgos en seguridad informática	*Metodología para la implementación de un análisis de riesgos para la protección de la información.*	*Duración: una semana*	*Personal Técnico de la DGOAE que sea responsable de la protección de datos en sus respectivas áreas.*
Buenas prácticas en medidas de seguridad administrativas para la protección de datos personales.	*Implementación de buenas practicas en la protección de Datos Personales.*	*Duración: un día*	*Todo el personal de la DGOAE que sea responsable de la protección de datos en sus respectivas áreas.*

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.			
Identificador único*	**DGOAE-CS–2017-01**		
Nombre del sistema DGOAE-1*	**Sistema Integra**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso de privacidad simplificado	*Se encuentra publicado en un banner al ingresar al sistema INTEGRA*	*Desde que se implemento en el sistema*	*Usuario titular de los datos personales.*
Aviso de privacidad integral	*Se encuentra publicado en el sistema INTEGRA y*	*Desde que se implemento en el sistema*	*Usuario titular de los datos personales.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 34 de 425—

	en el portal de la DGOAE		
Repositorio de presentaciónes de cursos de capacitación en materia de transparencia y protección de Datos	*Se encuentra publicado en el sistema INTEGRA*	*Desde que se implemento en el sistema*	*Personal de la DGOAE*
Material de difusión sobre protección de datos personales	*Se hará difusión de la información sobre protección de datos personales emitida por la Unidad de Transparencia.*	*Difusión constante*	*Usuario titular de los datos personales. Personal de la DGOAE*

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.			
Identificador único*	**DGOAE-CS–2017-01**		
Nombre del sistema DGOAE-1*	**Sistema Integra**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Análisis de los reportes de los usuarios acerca de los bugs, mal funcionamiento y documentación sobre el funcionamiento del sistema.	*Contar con la información necesaria para evaluar los puntos en donde se necesita hacer una actualización del sistema.*	*Actividad Constante*	*Actualización y mejora del sistema integra.*
Actualización de mensajes de error y éxito.	*Actualización de los mensajes que emite el sistema para garantizar la comunicación con los usuarios.*	*Duración: un mes*	*Mejor retroalimentación con los usuarios del sistema integra.*
Avisos de confirmación de movimientos	*Mejor manejo de los avisos de confirmación antes de realizar algún cambio para evitar*	*Duración: un mes*	*Mejor información a los usuarios del sistema integra,*

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 35 de 425—

	modificaciones no deseadas.		*que realizan movimientos.*

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.			
Identificador único*	**DGOAE-CS–2017-01**		
Nombre del sistema DGOAE-1*	**Sistema Integra**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en que estado se encuentran*	Duración: Cada año	*Total*
Actualizar o cambiar los equipos de desarrollo que lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: Cada año	*Total*

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema	**Sistema Integra**	
Proceso*	**Descripción***	**Responsable***
Respaldos Automáticos de Base de Datos, Archivos y Aplicación en la NAS	*Se programaron tareas automáticas para realizar los respaldos de la base de datos, archivos y aplicación. Los respaldos se generan de manera automática y se guardan en la carpeta desiganda por DGTIC en una NAS.*	*Administrador del sistema*
Respaldo en soporte electrónico portable (disco duro)	*Copiar los respaldos que se encuentran almacenados en la NAS al Disco Duro portable para tener otro medio de resguardo de la información.*	*Administrador del sistema*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —36 de 425—

Dirección General de Orientación y Atención Educativa (DGOAE) Dirección de Becas y Enlace con la Comunidad.		
Identificador único*	**DGOAE-CS–2017-01**	
Nombre del sistema	**Sistema Integra**	
Proceso*	**Descripción***	**Responsable***
Proceso de borrado de equipos de computo	*Reportar que equipo y de que persona es el equipo en el cual se va a realizar el borrado.* *Generar un respaldo de la información principal del usuario del equipo.* *Verificación del respaldo para evitar que contenga información de datos personales ajenos.* *Formatear el disco duro mediante una herramienta de bajo nivel para evitar recuperación de información.*	*Departamento de Informática*
Proceso de borrado de respaldos en soporte electrónicos	*La información que se borra de estos dispositivos solamente deberá guardar información del sistema.* *Formatear a bajo nivel para evitar recuperación de información.*	*Departamento de Informática*

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

La DGOAE informará a la Coordinación de Sistemas, sobre la cancelación del sistema mediante un escrito donde indique lo siguiente:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —37 de 425—

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, se llevarán a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema será cancelado y el servicio sera dado de baja o será remplazado por otro sistema y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar las cuentas de usuario activas en el sistema, para evitar accesos.
4. Solamente el administrador del sistema podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Bajar del servidor el sistema para que no pueda ser visto por ningun usuario.

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

En apego a la normativa vigente, se debe realizar el resguardo de información por el tiempo necesario de acuerdo a la clasificación archivistica que corresponda.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el Jefe de Departamento del Centor de Datos de DGTIC, para solicitar borrar toda la información contenida en la maquina virtual donde se alojaba el sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción fisica o desmagnetización.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —38 de 425—

Módulo de solicitudes para SECE

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Becas y Enlace con la Comunidad.**	
Identificador único	**DGOAE-DBEC–2022-02**
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**
Datos personales (sensibles o no) contenidos en el sistema:	Numero de trabajador, apellido paterno, materno, nombres, grado académico, teléfono de casa, celular, Datos laborales, dependencia, cargo, teléfono de oficina, extensión, correo personal, correo UNAM, correo enlace y pagina web
Responsable:	Jefa de enlace con la comunidad
Nombre:	Esperanza Vitela Ibáñez
Cargo:	Jefa del Departamento de Enlace con la Comunidad
Funciones:	Supervisión del correcto uso y manejo de accesos por parte del encargado.
Obligaciones:	Comunicación directa con los responsables de las dependencias registradas
	Encargados:
(Nombre del Encargado 1)	Pamela Ramírez Solis
Cargo:	Becaria
Funciones:	Administración de las solicitudes de publicación en SECE

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —39 de 425—

Obligaciones:	Resguardar y administrar las solicitudes de difusión del SECE

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.	
Identificador único	DGOAE-DBEC–2022-02
(Nombre del sistema A1*)	**Módulo de solicitudes para SECE**
Tipo de soporte	Soporte electrónico
Descripción	Base de datos
Características del lugar donde se resguardan los soportes:	Alojamiento en servidor enlace estudiantil, resguardado por DGTIC y la Coordinación de sistemas de la DGOAE.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Becas y Enlace con la Comunidad.**		
Identificador único*	DGOAE-DBEC–2022-02	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Riesgo	**Impacto**	**Mitigación**
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —40 de 425—

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	DGOAE-DBEC–2022-02	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Medida de seguridad actual	**Medida de seguridad necesaria**	**Acciones para remediación**
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.			
Identificador único	DGOAE-DBEC–2022-02		
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**		
Actividad	**Descripción**	**Duración**	**Cobertura**
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —41 de 425—

Dirección de Becas y Enlace con la Comunidad.	
Identificador único	**DGOAE-DBEC–2022-02**
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	No se requiere
Transferencias mediante el traslado de soportes electrónicos:	Se realiza a través del sistema informático SECE, por medio de la página: http://www.enlaceestudiantil.unam.mx/sitesece/index.html#&panel1-6&panel2-5, él envió está cifrado por Cifrado S/MIME ya que utiliza un cuenta de Hotmail para dar aviso a los enlaces de su alta en el sistema.
Transferencias mediante el traslado sobre redes electrónicas:	Para el envío de estos correos se utiliza una red de internet.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

8. Para este Sistema no se utilizan soportes físicos, ya que todo está alojado electrónicamente en el servidor Enlace Estudiantil a cargo de DGTIC.
9. La persona autorizada para acceder al sistema electrónico es el encargado 1

(Nombre del Encargado 1)	Pamela Ramírez Solis
Cargo:	**Módulo de solicitudes para SECE**
Funciones:	Administración y envió de solicitudes.
Obligaciones:	Resguardar de manera segura los usuarios y contraseñas para acceder, garantizar la secrecía, recuperación y respaldo de información.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

a) Actualmente no se cuenta con una bitácora, ya que solo una persona se

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —42 de 425—

encarga de administrar y manejar el SECE, además de que todo está alojado en el servidor Enlace Estudiantil a cargo de DGTIC y el de becarios UNAM a cargo de la coordinación de sistemas de la DGOAE.

IV. REGISTRO DE INCIDENTES

El responsable del módulo Sece junto con la Coordinación de Sistemas, realizaron una copia fiel de los datos que se generan, para así evitar cualquier pérdida o acceso no controlado a la información de datos personales.

V. ACCESO A LAS INSTALACIONES

a) Seguridad perimetral exterior (las instalaciones del área universitaria):
Hay guardias de seguridad en la entrada del departamento quien vigila el acceso.
Las personas que acceden a las instalaciones se identifican de manera visual y se autentifican por medio de una identificación oficial.
El acceso se autoriza de forma verbal por medio de la persona de seguridad.

b) Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso a soportes electrónicos se realiza por medio de un usuario y contraseña, a través del servidor Enlace Estudiantil alojado en la computadora. Este servidor es resguardado en GDTIC.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1) Modelo de control de acceso.
   - **a)** Es obligatorio
   - **b)** Está basado en reglas

2) Perfiles de usuario y contraseñas en el sistema operativo de red:
   - **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? Si
   - **b)** Se utiliza el SSH
   - **c)** ¿Proporciona dicho sistema operativo un manejo riguroso de

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —43 de 425—

perfiles de usuario y contraseñas? Si

d) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si

3) Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? Si

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? Si, se cifra en SSH

4) Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? La persona encargada de la administración del SECE

b) ¿Quién autoriza la creación de nuevos perfiles? Mtra. Esperanza Vitela Ibañez

c) ¿Se lleva registro de la creación de nuevos perfiles? No

5) Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? Si

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? Si

c) ¿Cómo se evita el acceso remoto no autorizado? Autorizando direcciones IPS específicas y con usuarios y contraseñas

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1) Señalar si realiza respaldos: No se realizan respaldos ya que todo está almacenado en el servidor de GDTIC. Solo se tiene los respaldos que ellos realizan de sus sistemas.

IX. PLAN DE CONTINGENCIA

1) Para el plan de contingencia se hacen respaldos bajo solicitud, con ellos se garantiza mantener fluyendo la información.

2) Para llevarlo a cabo se informa al área de Coordinación de Sistemas y se pide realizar un respaldo de información, esta solicitud y la realización de plan lleva aproximadamente 1 día en ser ejecutada.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu8s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —44 de 425—

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	**DGOAE-DBEC–2022-02**	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Recurso	**Descripción**	**Control**
Servidor remoto	Los servidores están alojados en DGTIC	Acceso remoto al servidor vía SSH

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	**DGOAE-DBEC–2022-02**	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Medida de seguridad	**Procedimiento**	**Responsable**
No se han aplicado	*No se han aplicado*	*No hay responsable*

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	**DGOAE-DBEC–2022-02**	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Medida de seguridad	**Resultado de evaluación**	**Responsable**
No se han aplicado	*No se han aplicado*	*No hay responsable*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —45 de 425—

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	**DGOAE-DBEC–2022-02**	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Medida de seguridad	**Acciones**	**Responsable**
Renovar la contraseña en un tiempo establecido Revisar el software Actualizaciones del sistema operativo	Se esta desarrollando un modulo para que las solictudes sea de manera segura.	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas

8. Programa especifico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.			
Identificador único	**DGOAE-DBEC–2022-02**		
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Curso con presentaciones didácticas	Se puede implementar un curso a los responsables de cada sistema que manejan datos sensibles, para que con ello se pueda saber que hacer en caso de vulnerabilidad del sistema o como implementar algún protocolo de emergencia.	1 a 2 horas por una semana	Responsables de o encargados del sistema, actualización cada 6 meses

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —46 de 425—

Dirección de Becas y Enlace con la Comunidad.			
Identificador único	DGOAE-DBEC–2022-02		
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Difusión por medios electrónicos	Se puede realizar una campaña por medio de las redes sociales haciendo conciencia e importancia de la protección de datos personales, así como las consecuencias que pueden existir si se expone la información	2 semanas	Responsables de o encargados del sistema y todos los departamentos de la DGOAE.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.			
Identificador único	DGOAE-DBEC–2022-02		
(Nombre del sistema A1)	**Portal del SECE**		
Actividad	**Descripción**	**Duración**	**Cobertura**
Solicitud de creación de un módulo	Se desarrollará un módulo dentro del sistema INTEGRA, que permita que las solicitudes sean de manera mas segura para los solicitantes.	Por definir	Implementación de un módulo de solicitudes seguro.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.	
Identificador único	DGOAE-DBEC–2022-02

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —47 de 425—

(Nombre del sistema A1)	Módulo de solicitudes para SECE		
Actividad	**Descripción**	**Duración**	**Cobertura**
No se realiza			

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	DGOAE-DBEC–2022-02	
(Nombre del sistema A1)*	**Módulo de solicitudes para SECE**	
Proceso	**Descripción**	**Responsable**
Solicitud de respaldo completo del servidor con el área de sistemas	Se realiza una copia fiel de todos los archivos y se ejecutan pruebas para cerciorar su correcto funcionamiento	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas 1 día

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. Dirección de Becas y Enlace con la Comunidad.		
Identificador único	DGOAE-DBEC–2022-02	
(Nombre del sistema A1)	**Módulo de solicitudes para SECE**	
Proceso	**Descripción**	**Responsable**
Se realiza la solitud al área de sistemas	Eliminación de los datos requeridos.	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas 2-3 días

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

No se aplica, ya que el sistema que se maneja esta almacenado en el servidor Enlace estudiantil resguardado por DGTIC y en el de becarios unam administrado por la coordinación de sistemas de la DGOAE.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —48 de 425—

Dirección de Servicio Social

Sistema de Información Automatizada de Servicio Social

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social**	
Identificador único*	**DGOAE-DSS–2022-01**
Nombre del sistema *	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**
Datos personales (sensibles o no) contenidos en el sistema*:	• Datos personales de prestadores de servicio social (alumnos y pasantes de la UNAM), estos datos no se le solicitan a los estudiantes, sino que se accede a ellos para verificar su identidad mediante un web service que proporciona la Dirección General de Administración Escolar (DGAE). • Datos laborales de los responsables de Programas de Servicio Social en las Instituciones Receptoras (sector público y social). • Datos laborales de los titulares de las Unidades Responsables de Servicio Social de Escuelas de la UNAM y Sistema Incorporado.
Responsable*:	
Nombre*:	**Lic. Claudia Navarrete García**
Cargo*:	**Directora de Servicio Social**
Funciones*:	Administrar, dirigir, ligerear y delegar responsabilidades para el buen funcionamiento y manejo de los procesos de las distintas áreas que conforman la Dirección de Servicio Social.
Obligaciones*:	Validar los procesos y reglas de negocio con las que opera el sistema con respecto a los datos contenidos en el sistema con base en las normativas del Servicio Social.
	Encargados:
(Nombre del Encargado 1*)	**Biol. Alejandra Hernández Valdivia**
Cargo*:	**Jefa del Departamento de Registro y Seguimiento**
Funciones*:	Administrar, dirigir y delegar, las diferentes actividades dentro del departamento, como dar seguimiento en a los programas de Servicio Social registrados.
Obligaciones*:	Monitorear el cumplimiento de los datos ingresados en el sistema de las Unidades de Responsables de Servicio Social y de la Instituciones Receptoras de Servicio Social.
(Nombre del Encargado 2*)	**Ing. Brian Alfonso Sánchez Vázquez**
Cargo*:	**Técnico Académico**
Funciones*:	Desarrollo de módulos del sistema, administrar, actualizar, dar de

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —49 de 425—

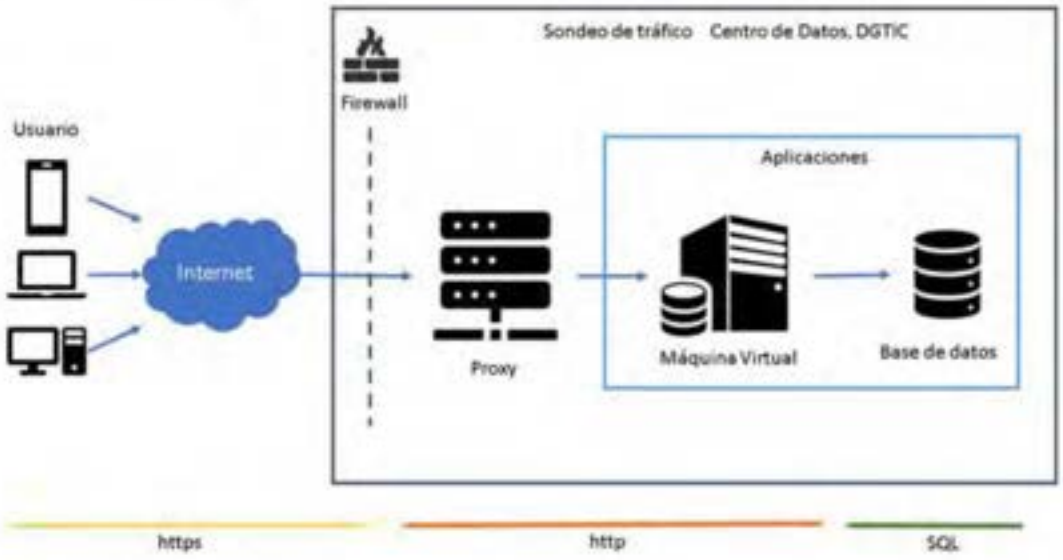
	alta usuarios nuevos e instituciones y depurar el sistema SIASS - UNAM
Obligaciones*:	Administra y monitorear la integridad de las bases y los datos contenidos en el Sistema SIASS, apoyar al Director General en su función de validar y emitir firma electrónica de las cartas de liberación de Servicio Social.
	Usuarios:
(Nombre del Usuario 1*)	**Lic. Jorge Olguín Carro**
Cargo*:	**Auxiliar Administrativo**
Funciones*:	Monitorear, Registros e Ingresos de nuevas Instancias receptoras de Servicio Social, validar datos de usuarios y responsables de Servicio Social
Obligaciones*:	Cotejar y confirmar la información ingresada por las instituciones y los responsables de servicio social.
(Nombre del Usuario 2*)	**Norma Ortega**
Cargo*:	**Auxiliar Administrativo**
Funciones*:	Monitorear, Registros e Ingresos de nuevas Instancias receptoras de Servicio Social, validar datos de usuarios y responsables de Servicio Social
Obligaciones*:	Cotejar y confirmar la información ingresada por las instituciones y los responsables de servicio social.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social	
Identificador único¨*	DGOAE-DSS-2022-01
(Nombre del sistema A1*)	SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL
Tipo de soporte:*	Sistema Electrónico
Descripción:*	Base de datos
Características del lugar donde se resguardan los soportes:*	Alojada en el centro de datos de la Dirección General de Tecnologías de Información y Comunicación, se conoce que posee seis niveles de seguridad: Nivel 1: Seguridad de acceso físico. • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware. • Los servidores se encuentran resguardados dentro de una sala informática de acceso restringido. • La sala debe mantener la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • La infraestructura mantiene las configuraciones de seguridad optimas que propagan a los contenedores donde reside el servidor. • Instalación de programas que permiten la detección y eliminación de

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —50 de 425—

	programas maliciosos y spyware. • Configuración de firewall para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP. • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la base de datos. Nivel 4: Seguridad del sistema operativo: • Se validan los accesos de administración mediante una cuenta de usuario mortal, con creenciales verificables. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. • Se mantiene un numero de intentos limitados, para bloquear ataques de fuerza bruta. Nivel 6: Seguridad en la base de datos: • Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol. • Respaldos de la base de datos. • No se permiten conexiones externas al ambiente donde se aloja el servidor.



3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa Dirección de Servicio Social. Departamento de Registro y Seguimiento.	
Identificador único*	**DGOAE-DSS–2022-01**
(Nombre del sistema A1) *	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**

ID del Documento: gIPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —51 de 425—

Riesgo*	Impacto*	Mitigación*
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —52 de 425—

[redacted]

4. Análisis de brecha

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social			
Identificador único*	**DGOAE-DSS–2022-01**		
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —53 de 425—

[redacted]

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social	
Identificador único*	**DGOAE-DSS–2022-01**
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se efectúan transferencias de datos personales en formatos físicos.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	No se hacen transferencias de datos personales, solo consulta con los mecanismos propios del sistema, los usuarios facultados para hacer estas consultas son los titulares de las Unidades Responsables de Servicio Social de escuelas, facultades, centros e institutos de la UNAM y Sistema Incorporado que los registran mediante el webservice que provee DGAE, el cual está cifrado y restringido, con acceso permitido solamente a la IP del sistema.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Se tiene de manera local una maquina a cargo del responsable del sistema, con el sistema de archivos cifrado, y que se atiene a las medidas de seguridad fisica de la Dependencia.
2. Solo el responsable tiene acceso a esos respaldo adicionales a los que realiza la DGTIC en su estructura interna.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 54 de 425 —

El administrador del sistema accede a dichas bitácoras, mediante conexión SSH a la infraesturctura de DGTIC.

b) **Para soportes físicos: Número o clave del expediente utilizado:** No aplica

c) **Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos:** Registro de prestadores, usuarios URSS, IR, registro de programas de servicios social.

2. **Si las bitácoras están en soporte físico o en soporte electrónico;** Todas las acciones se operan y registran en las bitacoras del sistema.

3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;** En la infraestructura de DGTIC, la permanencia de los datos tiende a ser permanente ya que spn parte del expediente académico de alumnos y egresados de la UNAM y sistema incorporado.

4. **La manera en que asegura la integridad de las bitácoras:**
   - Acceso restringido por usuario, contraseña y dirección IP.
   - Respaldo de la base de datos.
   - Los respaldos se generan en el servidor de DGTIC, posteriormente se copian a una computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro, el cual mantiene cifrado su sistema de archivos.

5. **Respecto del análisis de las bitácoras:**
   c) **Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza:** El administrador del sistema, de manera perióidica y cuando se presenta un incidente detectado desde la administración o reportado por los usuarios,
   d) **Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.** Se utilizan las herramientas de consola del sistema para verificar y filtrar los logs.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —55 de 425—

1. **Los datos que registra:**
   a) **La persona que resolvió el incidente.** Nombre del encargado o de la persona que resolvió el incidente.
   b) **La metodología aplicada.** Se registra la incidencia, los daños y acciones para prevenir otra.
   c) **Para soportes físicos.** No se cuenta con soportes físicos.
   d) **Para soportes electrónicos.** El respaldo que se hace de la base de datos incluye: tablas, campos y registros de cada una de ellas.
2. **Si el registro está en soporte físico o en soporte electrónico.** El soporte se encuentra en electrónico.
3. **Cómo asegura la integridad de dicho registro.** Reglas de validación, realizando transacciones y por medio de los respaldos.
4. **Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.** El encargado y/o el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior**

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones.

a) **¿Cómo las identifica?**
   Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) **¿Cómo las autentifica?**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —56 de 425—

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

C) **¿Cómo les autoriza el acceso?**
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior**

Para las personas que acceden a dichos espacios interiores:

Las oficinas o cubículos de la Bolsa Universitaria de Trabajo son: Oficina 63, cubículo 1, cubículo 4, cubículo 11, cubículo 12, cubículo 16, cubículo 59 y área central, todos se encuentran en la planta baja de la Dirección General de Orientación y Atención Educativa.

a) **¿Cómo las identifica?**
Las personas a quienes atendemos son: enlaces de entidades académicas, alumnado, egresadas y egresados de la UNAM.

b) **¿Cómo las autentifica?**
Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) **¿Cómo les autoriza el acceso?**
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

***Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.**

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Los datos de alumnos son un reflejo fiel de los datos registrados en DGAE en el expediente del estudiante o egresado, para cualquier cambio ya se por errores de apellido o reasignación de género, deben dirigirse directamente a DGAE siguiendo el protocolo correspondiente, para que dicho cambio sea visible también en el SIASS.

En el caso de Instituciones receptoras cualquier cambio en nombre o domicilio laboral, se hace mediante solicitud y oficio electrónicos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. **Modelo de control de acceso**

El sistema y la base de datos se encuentran alojados en la infraestructura virtual de la DGTIC.

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —57 de 425—

a) **¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?** Si
b) **¿Es discrecional (matriz de control de acceso)?** No
c) **¿Está basado en roles (perfiles) o grupos?** Si
d) **¿Está basado en reglas?** Si

2. **Perfiles de usuario y contraseñas en el sistema operativo de red:**
   a) **¿Cuenta con sistema operativo de red instalado en sus equipos?** Sí,de acuerdo a las necesidades de cada sistema DGTIC se encarga de instalar y configurar el sistema operativo adecuado.
   b) **¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?** Sí, los equipos que se encuentran en la DGOAE cuentan con este manejo, así como el equipo de la DGTIC, dónde se encuentra el sistema.
   c) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.
3. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:**
   a) **¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?** Si.
   b) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.
4. **Administración de perfiles de usuario y contraseñas:**
   a) **¿Quién da de alta nuevos perfiles?** El responsable del sistema se pone en contacto con DGTIC y hace esta solicitud mediante el sistema de tickets y / o solicitud vía correo electrónico, ahora que la emergencia sanitaria por COVID-19 ha mermado, se continua la entrega de oficios de solicitud fisicos.
   b) **¿Quién autoriza la creación de nuevos perfiles?** Administrador del sistema y usuarios auxiliares.
   c) **Acceso remoto al sistema de tratamiento de datos personales:**
   d) **¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?** No.
   e) **¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?** Si
   f) **¿Cómo se evita el acceso remoto no autorizado?** Las credenciales de acceso solo se dan a personas que están adscritas a la DGOAE, se firma una carta de confidencialidad.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —58 de 425—

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. **Señalar si realiza respaldos**
   (1) Completos.
   (2) De forma automática y Manual.
   (3) Periodicidad con que los realiza: DGTIC tiene un cronograma de respaldos, localmente se hacen respaldos cada tercer día para que el espaciado entre respaldo sea mínimo.
2. **El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:**
   Los respaldos se realizan mediante el software de administración de base de datos, el cual genera un archivo con toda la información de las tablas que guardan la información de este sistema. Como el espacio que nos brinda DGTIC no es muy grande, los archivos se copian a una máquina que se encuentra en la DGOAE, el cual cuenta con un sistema de archivos cifrado.
3. **Cómo y dónde archiva esos medios:** Instalaciones de la DGOAE.

Quién es el responsable de realizar estas operaciones:
Responsable/Administrador del sistema.
*** DGTIC realiza sus propios respaldos.**

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.
   - Tener respaldos de la base de datos y del código.
   - Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
   - Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
   - El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
   - Una vez se realiza la entrega del espacio, DGTIC deberá proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —59 de 425—

- Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una vez hecha la conexión se carga el respaldo de la base de datos.
- En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
- Realizar pruebas individuales a los módulos que conforman el sistema, para verificar que opera de manera normal y no hace falta algún requisito del framework.

2. Este plan de contingencia se marca con carácter de urgente, y es general para los sistemas de Servicio Social y Bolsa de Trabajo, el cual es aplicable cuando hay un incidente de red o de base de datos, se utiliza en primera instancia una imagen de la maquina virtual y se carga el último respaldo de la base de datos.

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) **El tipo de sitio (caliente, tibio o frío);** No aplica
   b) **Si el sitio es propio o subcontratado con un tercero;** No aplica
   c) **Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio.**
      Descrito en el punto anterior
   d) **Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.**
      Descrito en el punto anterior.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social		
Identificador único*	**DGOAE-DSS--2022-01**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit	Extensión del navegador que esta diseñada para probar vulnerabilidades en el sistema.	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —60 de 425—

Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicarán el tráfico que existen en el servidor.	Se hace manual y solamente será usada cuando se genere un ataque al sistema.
Bitácoras generadas por el servidor	Éstas nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas por la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social		
Identificador único*	**DGOAE-DSS–2022-01**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizaciones.	Revisión de páginas oficiales sobre las actualizaciones del lenguaje de programación.	Encargado del sistema.
Prueba de seguridad por parte de DGTIC	Se realiza una solicitud a DGTIC para que realice pruebas de seguridad y encuentre vulnerabilidades, DGTIC envía un documento con las vulnerabilidades que encontró para que éstas sean corregigas.	DGTIC.
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones.	Encargado del sistema.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social		
Identificador único*	**DGOAE-DSS–2022-01**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

ID del Documento: gIPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 61 de 425—

Pruebas de vulnerabilidad.	No se encontraron fallas.	Encargado del sistema, antes de liberar a producción el CERT de DGTIC realiza pruebas de penetración exhaustivas.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social		
Identificador único*	**DGOAE-DSS–2022-01**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Medida de seguridad*	**Acciones***	**Responsable***
Pruebas de vulnerabilidad	a) Se corrigieron las partes del código que son vulnerables, con base al reporte de seguridad de DGTIC b) Constante actualización del sistema, lenguaje de programación, manejador de base de datos y framework utilizados.	Encargado del sistema

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social			
Identificador único*	**DGOAE-DSS–2022-01**		
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos	Cursos sobre programación en PHP, MySQL, Linux, seguridad informática, creación de certificados SSL, protección a las máquinas virtuales, hacker ético, etc.	Sujeta al tipo de curso y en donde se imparte.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	Sujeta al tipo de curso y en donde se imparte.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 62 de 425 —

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social			
Identificador único*	**DGOAE-DSS–2022-01**		
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cartas de confidencialidad	Se le hace llegar y firmar una carta de confidencialidad al personal que va a tener acceso al sistema.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Para todo el personal de la BUT, su objetivo es que estén enteradas(os) de que trabajaran con datos del alumnado, egresadas y egresados de la UNAM. Una vez firmada la carta comienza la vigencia y esta se actualiza dependiendo las circunstancias por las que esté pasando la UNAM.
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	La distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Permanente.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social			
Identificador único*	**DGOAE-DSS–2022-01**		
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —63 de 425—

Registro y atención de mensajes de error, éxito y de información	Actualizar los mensajes del sistema para que no muestre contenido de la base de datos o de la configuración del servidor.	Permanente.	Total.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social			
Identificador único*	**DGOAE-DSS–2022-01**		
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo, lenguaje de programación y de la base de datos.	Es importante tener las versiones más actualizadas para evitar que nuestro equipo o software quede obsoleto y sin soporte.	Depender de la adquisición del nuevo equipo e instalación del software.	Parcial.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección de Servicio Social. Departamento de Registro y Seguimiento.		
Identificador único*	**DGOAE-DSS-SIASS**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Proceso*	**Descripción***	**Responsable***
Indique el proceso en materia de conservación, preservación y respaldo de información.	*Describa el proceso en todas sus acciones.*	*Indicar:* *a) Nombre del responsable del proceso*

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 64 de 425—

Agregue un renglón por proceso		*b) Tiempo máximo de ejecución en días.*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección de Servicio Social. Departamento de Registro y Seguimiento.		
Identificador único*	**DGOAE-DSS-SIASS**	
Nombre del sistema*	**SISTEMA DE INFORMACIÓN AUTOMATIZADA DE SERVICIO SOCIAL**	
Proceso*	**Descripción***	**Responsable***
Indique el proceso en materia de borrado seguro, disposición final de equipos o componentes de cómputo. Agregue un renglón por proceso	*Describa el proceso en todas sus acciones.*	*Indicar:* *a) Nombre del responsable del proceso* *b) Tiempo máximo de ejecución en días.*

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

F) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:
- a) Denominación
- b) Motivo de la cancelación

G) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

H) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 65 de 425 —

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)

I) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)

J) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —66 de 425—

Control de Constancias

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-02**
(Nombre del sistema A1) *	Control de Constancias_para los programas de la Dirección de Servicio Social.
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo, Nombramiento, Dependencia, Escuela, Facultad o Instituto de origen, rol de participación en cada evento (Voluntario, Asistentes, Participante, Coordinador, Relator, etc.), según sea la naturaleza de cada evento
Responsable*:	
Nombre*:	**Jorge Olguín Carro**
Cargo*:	Asistente de Procesos
Funciones*:	Recabar datos de los Eventos propios de la

	Dirección de Servicio Social, principalmente de Voluntariado, Foros de Servicio Social, Congresos, participaciones en las Reuniones de Responsables de Servicio Social.
Obligaciones*:	Confirmar los datos Particulares y de los eventos para los que se generan las constancias. Concentrar, almacenar y catalogar en bases de datos, cada uno de los participantes y asistentes que solicitan constancias de participación. Confirmar los correos y participación y asistencia de los partícipes en los eventos. Bloquear los archivos PDF, contra modificación.
	Encargados:
(Nombre del Encargado 1*)	**Lic. Celeste Cruz Avilés**
Cargo*:	**Jefa del Departamento de Voluntariado UNAM.**
Funciones*:	Evaluar, supervisar y generar actividades que fomente el Voluntariado
Obligaciones*:	Validar las acciones voluntarias y proponer los mejores procesos con visión objetiva para lograr las metas esenciales del programa.
	Usuarios:
(Nombre del Usuario 1*)	**Lic. Claudia Navarrete Garcia**
Cargo*:	**Directora de Servicio Social y Voluntariado**
Funciones*:	Administrar, dirigir, guiar y delegar responsabilidades para el buen funcionamiento y manejo de los procesos de las distintas áreas que conforman la Dirección.
Obligaciones*:	Validar y mantener la integridad de los datos recabados y contenidos en el sistema con base en las normativas del Servicio Social. Autorizar las constancias generadas, que serán entregadas de forma impresa o enviadas por correo según sea la naturaleza de cada evento, ya sea de forma presencia o virtual.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 67 de 425 —

Identificador único*	DGOAE-DSS–2022-02
(Nombre del sistema A1*)	Control de Constancias para los programas de la Dirección de Servicio Social.
Tipo de soporte: *	Solo soporte electrónico.
Descripción: *	Base de datos Excel.
Características del lugar donde se resguardan los soportes: *	La información se almacena en bases de datos de Excel, contenidos en el disco duro de las maquinas del Responsable y del Encargado.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1) *	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —68 de 425—

Identificador único*	DGOAE-DSS–2022-02	
(Nombre del sistema A1) *	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-02		
(Nombre del sistema A1) *	*Control de Constancias para los programas de la Dirección de Servicio Social.*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	DGOAE-DSS–2022-02

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —69 de 425—

(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario; Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1) Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2) Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

a) **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;**

- No aplica

b) **Para soportes físicos: Número o clave del expediente utilizado, y**

- Los soportes físicos, están clasificados con forme a los

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 70 de 425—

Instrumentos de Control y Consulta Archivística por año

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico:

Los soportes físicos están debidamente catalogados y almacenados en un archivero con cerrojo en la oficina del encargado del programa en la planta alta de la DGOAE.

3. Lugar dónde almacena las bitácoras y por cuánto tiempo

Los soportes físicos están a resguardo del encargado en las instalaciones de la DGOAE catalogados según lo estipulado conforme a los Instrumentos de Control y Consulta Archivística

4. La manera en que asegura la integridad de las bitácoras, y

Se encuentran en un archivero con cerrojo y solo el encargado del programa tiene acceso.

5. Respecto del análisis de las bitácoras:

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   b) La metodología aplicada;
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 71 de 425—

d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para **las personas que acceden a sus instalaciones:**

a) **¿Cómo las identifica?**
Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) **¿Cómo las autentifica?**
Con una identificación oficial que se queda en resguardo del

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 72 de 425—

personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) **¿Cómo les autoriza el acceso?**
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Dentro de las instalaciones, las oficinas están habilitadas con puerta con cerradura a llave que solo el personal autorizado tiene, los documentos en el sistema electrónico están contenidos en los equipos de cómputo, al cual se accede por contraseña.

Para las personas que acceden a dichos espacios interiores:

4. **¿Cómo las identifica?**
Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

5. **¿Cómo las autentifica?**
Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

6. **¿Cómo les autoriza el acceso?**
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 73 de 425—

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
- **b)** ¿Es discrecional (matriz de control de acceso)?
- **c)** ¿Está basado en roles (perfiles) o grupos?
- **d)** ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **c)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
- **d)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:

- **d)** ¿Quién da de alta nuevos perfiles?
- **e)** ¿Quién autoriza la creación de nuevos perfiles?
- **f)** ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales:

- a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
- b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
- c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 74 de 425—

a) Completos__, diferenciales ___ o incrementales___;
b) De forma automática ____ o Manual _____,
c) Periodicidad con que los realiza: _____

2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad·
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 75 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Recurso*	**Descripción***	**Control***
- Programas de antivirus - Programas de malware	Antivirus Kaspersky Software anti malware, Microsoft Defender	Software proporcionado por la unidad de sistemas de la DGOAE Software, propio del sistema operativo, no se cuenta con el dato de la licencia

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Medida de seguridad*	**Procedimiento***	**Responsable***
-Programas de antivirus. -Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	*Indicar:* Área de Sistemas de la DGOAE

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 76 de 425—

Programas de antivirus. Programas de malware	Sin virus detectados Sin incidentes de ataque por malware.	-Área de Sistemas de la DGOAE -Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Medida de seguridad*	**Acciones***	**Responsable***
- Almacenaje	Las bases se encuentran en los equipos de cómputo de la DGOAE y respaldas en un solo contenedor.	*Responsable y Encargados del sistema.*

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-02**		
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 77 de 425—

Platica informativa sobre la protección de datos.	Impartida por la Dra. Pichardo de la Unidad de Transparencia de la UNAM. el 3 de febrero de 2021	3 horas.	Responsables de Servicio Social de facultades, escuelas, institutos y centros.

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-02		
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementación de aviso de privacidad. Implementación de la carta de confidencialidad.	El aviso de privacidad se muestra al pie de los correos enviados, en la publicación de la convocatoria de registro de Voluntariado UNAM. La carta de confidencialidad es solicitada a los responsables que dirijan algún programa de Voluntariado UNAM.	Permanente En proceso, se llevando a cabo con los nuevos registros de programas de Voluntariado UNAM y eventos para los que se tengan que emitir constancias.	Está dirigido a los coordinadores, responsables y prestadores de los programas de Voluntariado UNAM o eventos en los que se emiten constancias. Solo al responsable y el encargado, quienes son los que manipularan los datos.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-02		
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Depurar los datos solicitados para la	Revisión de los datos más esenciales para la	Dependerá de cada solicitud de constancias según	Se homologaran los datos requeridos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 78 de 425—

emisión de constancias.	elaboración de las constancias determinando los primordiales para su elaboración.	el evento, aproximadamente de 1 a 2 días máximo. .	

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-02**		
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de Software Comprobación de licencias vigentes. Mantenimiento correctivo y preventivo del equipo de cómputo.	Mantiene en óptimas condiciones el funcionamiento de los equipos de cómputo y se previenen perdidas parciales o totales de los archivos. La comprobación de las licencias vigentes mantendrá al día contra amenazas contra virus o software malintencionado. Con la revisión periódica del equipo y con su buen funcionamiento se previenen la pérdida total de la información y se podrán programar respaldos1 de la información.	El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo. La comprobación de la vigencia de los antivirus está en automático y se revisan diario. El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo, pero en caso de solicitar una revisión más técnica, por lo general no rebasa 1 día.	Previene la perdida de datos por malfuncionamiento. Previene el acceso a programas mal intencionados. El mantenimiento previene que los circuitos no presenten fallas y no se pierdan los archivos contenidos en los discos duros.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 79 de 425—

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Proceso*	**Descripción***	**Responsable***
Concentrar en un solo contenedor el histórico de las bases de datos. Programar respaldos de los archivos.	De esta manera se contempla que los datos no estén en diferentes dispositivos y prevenir la pérdida o mal uso de los datos. Teniendo contemplado un respaldo periódico de los archivos se mitiga la perdida de los archivos por mal funcionamiento de los equipos de cómputo o por un archivo accidental.	a) Responsable y encargado. b) En proceso, avance de un 70%.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-02**	
(Nombre del sistema A1)*	*Control de Constancias para los programas de la Dirección de Servicio Social.*	
Proceso*	**Descripción***	**Responsable***
Cambio de equipo de cómputo o actualización.	En ocasiones la DGOAE actualiza los equipos de cómputo o se hacen actualizaciones en los dispositivos, para los cuales se hace un respaldo de los archivos y se procede a un formateo a bajo nivel el cual	a) Área de Sistemas de la DGOAE. b) No se ha necesitado este proceso en la actualidad.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —80 de 425—

	modifica el disco de almacenamiento para que los datos sean irrecuperables y no sean usados.	

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —81 de 425—

PERAJ UNAM

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS--2022-03**
(Nombre del sistema A1) *	**Servicio Social DGOAE UNAM PERAJ**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación Datos académicos
Responsable*:	**Lic. Socorro Becerril Quintana**
Cargo*:	Técnico Académico Asociado C Tiempo Completo
Funciones*:	Coordinación académico-administrativa del Programa de Servicio Social Tutorial UNAM – PERAJ "Adopta un Amig@".
Obligaciones*:	Selección, capacitación, coordinación y supervisión de prestadores de servicio social y universitarios voluntarios. Asignación, coordinación y seguimiento de binomios. Gestión de los recursos materiales para la operación del programa. Gestión de visitas a dependencias universitarias u otros recintos culturales. Gestión ante autoridades de escuelas primarias y con los padres de familia. Gestión de apoyos económicos para los universitarios participantes, en la DGOAE y en las otras sedes de la UNAM.
	Encargados:
(Nombre del Encargado 1*)	**Lic. Claudia Navarrete García**
Cargo*:	**Directora de Servicio Social y Voluntariado UNAM**
Funciones*:	Evaluar las actividades a desarrollar en el tratamiento de los datos personales, validar y ponderar los datos que se soliciten para los fines primordiales del Programa de Servicio Social
Obligaciones*:	Dirigir, evaluar y delegar funciones a los responsables que manejan y llevan a conformidad los datos que se requerirán de los participantes en el programa, asignando cargos actividades y roles a cada uno de los participantes

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —82 de 425—

(Nombre del Encargado 2*)	Lic. Griselda G. Gutiérrez Monsalvo
Cargo*:	Jefa del Departamento de Programas Multidisciplinarios
Funciones*:	Evaluación de las funciones, actividades y requerimientos del programa.
Obligaciones*:	Validar las acciones y proponer los mejores procesos con visión objetiva para lograr las metas esenciales del programa.
	Usuarios:
(Nombre del Usuario 1*)	Elizabeth Liselly Abarca González
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 2*)	Mariana Aguilera Roa
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 3*)	Adriana Karina Alavez González
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 4*)	Carolina Carrillo Ortíz
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 5*)	Mario Alberto Durán Escalante
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —83 de 425—

Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 6*)	Paloma Itzel Estrada González
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 7*)	David Arturo Flores Rodríguez
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 8*)	Alejandro Lara Carreño
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 9*)	Daniel Rico de la Torre
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 10*)	Aurora Rivera García
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 11*)	Rodrigo Romero Cárdenas
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —84 de 425—

	participantes, para la realización de actividades binomiales.
(Nombre del Usuario 12*)	Jessica Karen Silva de la Rosa
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.
(Nombre del Usuario 13*)	Pavel Alejandro Villanueva Díaz
Cargo*:	Coordinador becario
Funciones*:	Supervisión de actividades binomiales de un grupo de prestadores de servicio social o voluntarios
Obligaciones*:	Seguimiento y asesoría a los universitarios participantes, para la realización de actividades binomiales.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-03**
(Nombre del sistema A1) *	**Servicio Social DGOAE UNAM PERAJ**
Tipo de soporte: *	Tipo de Soporte Electrónico
Descripción: *	Base de datos en Access
Características del lugar donde se resguardan los soportes: *	Alojamiento en PC, propiedad de la UNAM situada a la DGOAE y asignada al área de Servicio Social en el Programa de Servicio Social UNAM PERAJ "Adopta un Amigo"
Tipo de soporte:*	Tipo de Soporte Electrónico
Descripción:*	Base de datos en Access
Características del lugar donde se resguardan los soportes:*	Alojamiento en Laptop personal

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1) *	**Servicio Social DGOAE UNAM PERAJ**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —85 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-03**	
Servicio Social DGOAE UNAM PERAJ	**Servicio Social DGOAE UNAM PERAJ**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	**DGOAE-DSS–2022-03**
Servicio Social DGOAE UNAM PERAJ	**Servicio Social DGOAE UNAM PERAJ**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —86 de 425—

Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	**DGOAE-DSS–2022-03**
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza envío de documentación vía paquetería
Transferencias mediante el traslado de soportes electrónicos:	No se realiza envío de documentación vía paquetería

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —87 de 425—

Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario; Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Los formatos impresos, documentos, listados y/o expedientes están en carpetas foliadas en archiveros con cerrojo, dentro de una oficina, la puerta de la oficina permanece cerrada cuando está desocupada; la puerta cuenta con doble cerradura.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:
   a. **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;**

   No aplica.

   b. **Para soportes físicos: Número o clave del expediente utilizado, y**

   Los soportes físicos, están clasificados conforme a los Instrumentos de Control y Consulta Archivística por año

   c. Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —88 de 425—

3. Lugar dónde almacena las bitácoras y por cuánto tiempo

   Los soportes físicos están debidamente catalogados y almacenados en un área acondicionada y con un lugar asignado dentro de la DGOAE.

4. La manera en que asegura la integridad de las bitácoras, y

   El área asignada está dentro de las instalaciones de la dirección, con puerta bajo llave y el acceso a los archivos es solo por el responsable del programa.

5. Respecto del análisis de las bitácoras

   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y

      Solo el encardo del programa está facultado y cuenta con acceso a los soportes físicos.

   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES:

FALTA INFORMACIÓN

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —89 de 425—

el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones:

a. **¿Cómo las identifica?**

- Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b. **¿Cómo las autentifica?**

- Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c. **¿Cómo les autoriza el acceso?**

- En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —90 de 425—

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Dentro de las instalaciones, las oficinas están habilitadas con puerta con cerradura a llave que solo el personal autorizado tiene, los documentos en el sistema electrónico están contenidos en los equipos de cómputo, al cual se accede por contraseña.

Para las personas que acceden a dichos espacios interiores:

1. **¿Cómo las identifica?**

   Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

2. **¿Cómo las autentifica?**

   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. **¿Cómo les autoriza el acceso?**

   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

ID del Documento: gIPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —91 de 425—

1. Modelo de control de acceso (alguno de los siguientes):
   a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
   b) ¿Es discrecional (matriz de control de acceso)?
   c) ¿Está basado en roles (perfiles) o grupos?
   d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles?
   b) ¿Quién autoriza la creación de nuevos perfiles?
   c) ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales:
   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
   c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos X , diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X__,
   c) Periodicidad con que los realiza: __cada tres meses_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   - Discos Duros

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —92 de 425—

3. Cómo y dónde archiva esos medios, y
   - En resguardo del responsable del programa.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   - El coordinador responsable del programa, área universitaria.

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   - No se cuenta con un plan detallado de contingencia, solo han contemplado algunas situaciones que afecten el desempeño del programa y que no sean utilizados los datos para fines ajenos al programa.

2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente: No se cuenta con un sitio.
   a. El tipo de sitio (caliente, tibio o frío);
   b. Si el sitio es propio o subcontratado con un tercero;
   c. Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d. Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Recurso*	**Descripción***	**Control***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —93 de 425—

- Programas de antivirus. - Programas de malware	Antivirus McAfee Security Scan Plus Software anti malware McAfee Security Scan Plus	Software proporcionado por la unidad de sistemas de la DGOAE Software adquirido de manera personal No se cuenta con el dato de la licencia

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Medida de seguridad*	**Procedimiento***	**Responsable***
- Programas de antivirus. - Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	*Indicar:*) Área de Sistemas de la DGOAE) Responsable del programa

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 94 de 425 —

- Programas de antivirus. - Programas de malware	Sin incidentes de ataque por malware y sin virus detectados	a) Área de Sistemas de la DGOAE b) Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Medida de seguridad*	**Acciones***	**Responsable***
- Almacenaje - Encriptar - Deshabilitar	- Almacenaje de las bases en un solo contenedor. - Encriptar las bases que conforman el histórico del programa. - Deshabilitar los formularios en la nube que solicitan datos personales.	a) Lic. Socorro Becerril Quintana, con apoyo y asesoría del área de Sistemas de la DGOAE. b) En proceso, avance de un 80%.

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —95 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-03**		
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Platica informativa sobre la protección de datos.	Impartida por la Dra. Pichardo de la Unidad de Transparencia de la UNAM. el 3 de febrero de 2021	3 horas.	Responsables de Servicio Social de facultades, escuelas, institutos y centros.

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-03**		
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —96 de 425—

Reuniones con los coordinadores de apoyo. Implementación de aviso de privacidad. Implementación de la carta de confidencialidad.	Las reuniones son llevadas para comunicar las normas de tratamiento de datos y dar a conocer las acciones a seguir. El aviso de privacidad se muestra al pie de los correos enviados, en la publicación de la convocatoria de registro de Servicio Social. La carta de confidencialidad es solicitada entre los coordinadores y responsables del Servicio Social.	Las reuniones se llevan cada mes para la evaluación de los avances generales y son mencionadas reiterativamente las medidas de tratamiento de datos. En proceso, se está llevando a cabo con los nuevos registros de coordinadores y responsables del Servicio Social para el ciclo 2021-2022	Está dirigido a los coordinadores, responsables y prestadores del programa de Servicio Social.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-03**		
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Depurar y ponderar los datos solicitados para el programa de Servicio Social.	Revisión de los datos solicitados para el programa de Servicio Social y solo mantener los primordiales para el éxito del programa.	De marzo a mayo de 2022.	El sistema será más factible en ejecución y evaluación de los resultados al contemplar las variables más importantes para las metas del programa.

9.2. Actualización y mantenimiento de equipo de cómputo

ID del Documento: gIrPdH8ZIn1+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —97 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-03		
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de Software Comprobación de licencias vigentes. Mantenimiento correctivo y preventivo del equipo de cómputo.	Mantiene en óptimas condiciones el funcionamiento de los equipos de cómputo y se previenen perdidas parciales o totales de los archivos. La comprobación de las licencias vigentes mantendrá al día contra amenazas contra virus o software malintencionado. Con la revisión periódica del equipo y con su buen funcionamiento se previenen la pérdida total de la información y se podrán programar respaldos1 de la información.	El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo de dos a tres veces por año y en caso de demanda son atendidas las solicitudes de dos a tres días dependiendo del recurso solicitado.	Previene la perdida de datos por malfuncionamiento. El mantenimiento previene que los circuitos no presenten fallas y no se pierdan los archivos contenidos en los discos duros.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-03	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Proceso*	**Descripción***	**Responsable***
Concentrar en un solo contenedor el histórico de las bases de datos.	De esta manera se contempla que los datos no estén en diferentes dispositivos y prevenir la pérdida o mal uso de los datos.	c) Lic. Socorro Becerril Quintana, con apoyo y asesoría del área de

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —98 de 425—

Encriptar los contenedores. Asignar permisos y roles en el tratamiento de datos. Programar respaldos de los archivos.	En caso de verse vulnerados los equipos de cómputos archivos tendrán la protección adecuada para no ser usados por terceras personas. La asignación de perfiles se categoriza los datos que pueden ser modificados o consultados en las bases, según sea el proceso que ejecuta cada usuario. Teniendo contemplado un respaldo periódico de los archivos se mitiga la perdida de los archivos por mal funcionamiento de los equipos de cómputo o por un archivo accidental.	Sistemas de la DGOAE. d) En proceso, avance de un 70%.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-03**	
(Nombre del sistema A1)*	**Servicio Social DGOAE UNAM PERAJ**	
Proceso*	**Descripción***	**Responsable***
Cambio de equipo de cómputo o actualización.	En ocasiones la DGOAE actualiza los equipos de cómputo o se hacen actualizaciones en los dispositivos, para los cuales se hace un respaldo de los archivos y se procede a un formateo a bajo nivel el cual modifica el disco de almacenamiento para que los datos sean irrecuperables y no sean usados.	c) Lic. Socorro Becerril Quintana, con apoyo y asesoría del área de Sistemas de la DGOAE. d) No se ha necesitado este proceso en la actualidad.

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —99 de 425—

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —100 de 425—

PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS-2022-04**
(Nombre del sistema A1) *	**PREMIO AL SERVICIO SOCIAL** **"Dr. Gustavo Baz Prada"**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos escolares en general. - Número de Cuenta UNAM - Facultad y Carrera - Programa de Servicio Social en que está

	Inscrito o en el cual participo. Datos de identificación para contactar a los alumnos y asesores en caso de ser seleccionados para otorgarles el reconocimiento. - Número telefónico de casa, celular o de contacto en caso de ser seleccionado. -Correo electrónico. Datos laborales de los asesores. - Facultad y Carrera, Institución prestadora Servicio Social de Origen, Asociación Civil, según sea el caso, teléfono de contacto, correo electrónico.
Responsable*:	
Nombre*:	**Lic. Claudia Navarrete García**
Cargo*:	**Directora de Servicio Social**
Funciones*:	Administrar, dirigir, encauzar y delegar responsabilidades para el buen funcionamiento y manejo de los procesos para la realización del evento en los tiempos estipulados en la convocatoria publicada cada año.
Obligaciones*:	Validar y mantener la integridad de los datos contenidos en el sistema con base en las normativas de la premiación al Servicio Social "Dr. Gustavo Baz Prada".
	Encargados:
(Nombre del Encargado 1*)	**Biol. Alejandra Hernández Valdivia**
Cargo*:	**Jefa del Departamento de Registro y Seguimiento**
Funciones*:	Administrar y dirigir las diferentes actividades dentro del tiempo de recepción de las solicitudes, para ser consideradas a premiación y dar seguimiento a las observaciones de los Responsables de Servicio Social de los diferentes programas a participar.
Obligaciones*:	Validar y mantener la integridad de los datos contenidos en el sistema con base en las normativas de la premiación al Servicio Social "Dr. Gustavo Baz Prada".

2. Estructura y descripción de los sistemas de tratamiento de datos personales

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —101 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	DGOAE-DSS-2022-04
(Nombre del sistema A1*)	**PREMIO AL SERVICIO SOCIAL** "Dr. Gustavo Baz Prada"
Tipo de soporte: *	Sistema Electrónico
Descripción: *	Base de datos en Excel.
Características del lugar donde se resguardan los soportes: *	En disco duro del equipo de cómputo asignado al Encargado y correo electrónico institucional del mismo.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	DGOAE-DSS-2022-04	
(Nombre del sistema A1) *	**PREMIO AL SERVICIO SOCIAL** **"Dr. Gustavo Baz Prada"**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —102 de 425—

Identificador único*	DGOAE-DSS–2022-04	
(Nombre del sistema A1) *	PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-04		
(Nombre del sistema A1) *	PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"		
Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	DGOAE-DSS–2022-04
(Nombre del sistema A1)*	PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —103 de 425—

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario; Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

      No aplica

   b) Para soportes físicos: Número o clave del expediente utilizado, y
      - Los soportes físicos, están clasificados con forme a los Instrumentos de Control y Consulta Archivística por año

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —104 de 425—

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Los soportes físicos están debidamente catalogados y almacenados en un cubículo designado por la dependencia con cerrojo en la planta alta de la DGOAE.

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
Los soportes físicos están a resguardo del encargado en las instalaciones de la DGOAE catalogados según lo estipulado conforme a los Instrumentos de Control y Consulta Archivística.

4. La manera en que asegura la integridad de las bitácoras, y
Se encuentran en un área de signada en la planta alta de la DGOAE con cerrojo y solo el encargado del programa tiene acceso.

5. Respecto del análisis de las bitácoras:
a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
- Solo tiene acceso el responsable en caso de necesitar datos de referencia.

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
a) La persona que resolvió el incidente;
b) La metodología aplicada;
c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
d) Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 105 de 425—

3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —106 de 425—

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

- Dentro de las instalaciones, las oficinas están habilitadas con puerta con cerradura a llave que solo el personal autorizado tiene, los documentos en el sistema electrónico están contenidos en los equipos de cómputo, al cual se accede por contraseña.

Para las personas que acceden a dichos espacios interiores:

1. **¿Cómo las identifica?**

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

2. **¿Cómo las autentifica?**

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. **¿Cómo les autoriza el acceso?**

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —107 de 425—

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
- **b)** ¿Es discrecional (matriz de control de acceso)?
- **c)** ¿Está basado en roles (perfiles) o grupos?
- **d)** ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos?
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles?
- **b)** ¿Quién autoriza la creación de nuevos perfiles?
- **c)** ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —108 de 425—

lo general utilizan para trabajar con el sistema?

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   - **a)** Completos__, diferenciales ___ o incrementales___;
   - **b)** De forma automática ____ o Manual _____,
   - **c)** Periodicidad con que los realiza: _____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   - **a)** El tipo de sitio (caliente, tibio o frío);
   - **b)** Si el sitio es propio o subcontratado con un tercero;
   - **c)** Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   - **d)** Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	**DGOAE-DSS–2022-04**
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —109 de 425—

	"Dr. Gustavo Baz Prada"	
Recurso*	**Descripción***	**Control***
Programas de antivirus Programas de malware	Antivirus Kaspersky Software anti malware, Microsoft Defender	Software proporcionado por la unidad de sistemas de la DGOAE Software, propio del sistema operativo, no se cuenta con el dato de la licencia

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-04	
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**	
Medida de seguridad*	**Procedimiento***	**Responsable***
-Programas de antivirus. -Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	Área de Sistemas de la DGOAE

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-04	
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Programas de antivirus. Programas de malware	Sin virus detectados Sin incidentes de ataque por malware.	-Área de Sistemas de la DGOAE -Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	DGOAE-DSS–2022-04
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —110 de 425—

Medida de seguridad*	Acciones*	Responsable*
Almacenaje	Las bases se encuentran en los equipos de cómputo de la DGOAE y respaldas en un solo contenedor.	*Responsable y Encargados del sistema.*

8. Programa específico de capacitación

8.1.Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-04**		
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Platica informativa sobre la protección de datos.	Impartida por la Dra. Pichardo de la Unidad de Transparencia de la UNAM. el 3 de febrero de 2021	3 horas.	Responsables de Servicio Social de facultades, escuelas, institutos y centros.

8.2.Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-04**		
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementación de aviso de privacidad. Implementación de la carta de confidencialidad.	El aviso de privacidad se muestra al pie de los correos enviados, en la publicación de la convocatoria de registro de Servicio Social. La carta de confidencialidad es solicitada entre los coordinadores y	El aviso es publicado en cada una de las convocatorias y eventos del programa y esta colocado al pie del correo institucional del cual parte la comunicación con los enlaces y prestadores del Servicio Social.	Parcial Está dirigido a los coordinadores, responsables y prestadores del programa de Servicio Social.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —111 de 425—

	responsables del Servicio Social.	En proceso, se está llevando a cabo con los nuevos registros de coordinadores y responsables del Servicio Social para el ciclo 2021-2022	

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-04**		
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Depurar y evaluar los datos solicitados para el programa de Servicio Social.	Revisión de los datos solicitados para el programa de Servicio Social y solo mantener los primordiales para el éxito del programa.	Durante el periodo de la convocatoria. .	El sistema será más factible en ejecución y evaluación de los resultados al contemplar las variables más importantes para las metas del programa.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-04**		
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de Software Comprobación de licencias vigentes. Mantenimiento correctivo y preventivo del	Mantiene en óptimas condiciones el funcionamiento de los equipos de cómputo y se previenen perdidas parciales o totales de los archivos. La comprobación de las licencias vigentes mantendrá	El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo de dos a tres veces	Previene la perdida de datos por malfuncionamiento. El mantenimiento previene que los circuitos no presenten fallas y no se pierdan los

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 112 de 425—

equipo de cómputo.	al día contra amenazas contra virus o software malintencionado. Con la revisión periódica del equipo y con su buen funcionamiento se previenen la pérdida total de la información y se podrán programar respaldos1 de la información.	por año y en caso de demanda son atendidas las solicitudes de dos a tres días dependiendo del recurso solicitado.	archivos contenidos en los discos duros.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-04**	
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**	
Proceso*	**Descripción***	**Responsable***
Concentrar en un solo contenedor el histórico de las bases de datos. Programar respaldos de los archivos.	De esta manera se contempla que los datos no estén en diferentes dispositivos y prevenir la pérdida o mal uso de los datos. Teniendo contemplado un respaldo periódico de los archivos se mitiga la perdida de los archivos por mal funcionamiento de los equipos de cómputo o por un archivo accidental.	Responsable del programa, con apoyo y asesoría del área de Sistemas de la DGOAE.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-04**	
(Nombre del sistema A1)*	**PREMIO AL SERVICIO SOCIAL "Dr. Gustavo Baz Prada"**	
Proceso*	**Descripción***	**Responsable***
Cambio de equipo de cómputo o actualización.	En ocasiones la DGOAE actualiza los equipos de cómputo o se hacen actualizaciones en los dispositivos, para los cuales se hace un respaldo de los archivos y se procede a un	Área de Sistemas de la DGOAE. No se ha necesitado este proceso en la actualidad.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 113 de 425—

	formateo a bajo nivel el cual modifica el disco de almacenamiento para que los datos sean irrecuperables y no sean usados.	

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema.
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
4. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —114 de 425—

- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Portal de Orientación Educativa que se encuentren dentro sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —115 de 425—

Programas Multidisciplinarios

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-05**
(Nombre del sistema A1) *	**Programas Multidisciplinarios**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación - Nombre Completo -Datos de Contacto, número telefónico de domicilio y celular, correo electrónico. Datos académicos - Número de Cuenta UNAM - Facultad y Carrera
Responsable*:	
Nombre*:	**Lic. Griselda G. Gutiérrez Monsalvo**
Cargo*:	**Jefa del Departamento de Programas Multidisciplinarios**
Funciones*:	Responsable de programa, llevar la gestión buen desarrollo del programa, gestión de los recursos materiales, el enlace para las brigadas de atención comunitaria, ante autoridades de las escuelas primarias y con los padres de familia.
Obligaciones*:	Guiar en la operación del programa, llevando a cabo diversas prácticas de intervención comunitaria con brigadas multidisciplinarias de servicio social. Evaluando el impacto y dando seguimiento a cada acción de desarrollo local y de las mismas brigadas interdisciplinarias de servicio social comunitario.
	Encargados:
(Nombre del Encargado 1*)	**Lic. Claudia Navarrete García**
Cargo*:	**Directora de Servicio Social**
Funciones*:	Evaluar las actividades a desarrollar en el tratamiento de los datos personales, validar y ponderar los datos que se soliciten para los fines primordiales del Programa de Servicio Social.
Obligaciones*:	Dirigir, evaluar y delegar funciones a los responsables que manejan y llevan a conformidad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 116 de 425—

	los datos que se requerirán de los participantes en el programa, asignando cargos actividades y roles a cada uno de los participantes.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-05**
(Nombre del sistema A1*)	**Programas Multidisciplinarios**
Tipo de soporte:*	**Tipo de Soporte Electrónico y Físico.**
Descripción:*	Base de datos y archivo físico
Características del lugar donde se resguardan los soportes:*	Las Bases de Datos están en alojamiento en PC, propiedad de la UNAM situada en la DGOAE y asignada al área de Servicio Social en el Departamento de Programas Multidisciplinarios. Los expedientes físicos están almacenados y catalogados de acuerdo con los Instrumentos de Control y Consulta Archivística de la UNAM, en resguardo en un archivero con seguro, en las instalaciones de la Dirección de Social en el área asignada por la Dirección General de Orientación y Atención Educativa.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1) *	**Programas Multidisciplinarios**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —117 de 425—

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1) *	**Programas Multidisciplinarios**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**			
Identificador único*	**DGOAE-DSS–2022-05**		
(Nombre del sistema A1) *	**Programas Multidisciplinarios**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

6. Medidas de seguridad implementadas

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —118 de 425—

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-05**
(Nombre del sistema A1)*	**Programas Multidisciplinarios**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario; Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

   a) **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —119 de 425—

No aplica

b) **Para soportes físicos: Número o clave del expediente utilizado, y**

Los soportes físicos, están clasificados con forme a los Instrumentos de Control y Consulta Archivística por año

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. **Si las bitácoras están en soporte físico o en soporte electrónico**;
Los soportes físicos están debidamente catalogados y almacenados en un cubículo designado por la dependencia con cerrojo en la planta alta de la DGOAE.

3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
Los soportes físicos están a resguardo del encargado en las instalaciones de la DGOAE catalogados según lo estipulado conforme a los Instrumentos de Control y Consulta Archivística

4. **La manera en que asegura la integridad de las bitácoras, y**
Se encuentran en un área de signada en la planta alta de la DGOAE con cerrojo y solo el encargado del programa tiene acceso.

5. **Respecto del análisis de las bitácoras:**

a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
Solo tiene acceso el responsable en caso de necesitar datos de referencia.

b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a. La persona que resolvió el incidente;
   b. La metodología aplicada;
   c. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 120 de 425—

d. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

1) **¿Cómo las identifica?**
Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

2) **¿Cómo las autentifica?**
Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —121 de 425—

canjea al término de su visita.

3) **¿Cómo les autoriza el acceso?**

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):
    1. ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
    2. ¿Es discrecional (matriz de control de acceso)?
    3. ¿Está basado en roles (perfiles) o grupos?
    4. ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
    1. ¿Cuenta con un sistema operativo de red instalado en sus equipos?
    2. ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
    3. ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
    1. ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
    2. ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas
    1. ¿Quién da de alta nuevos perfiles?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 122 de 425—

2. ¿Quién autoriza la creación de nuevos perfiles?
3. ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales
    1. ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
    2. ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
    3. ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
    a. Completos__, diferenciales ___ o incrementales___;
    b. De forma automática ____ o Manual _____,
    c. Periodicidad con que los realiza: _____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
    a. El tipo de sitio (caliente, tibio o frío);
    b. Si el sitio es propio o subcontratado con un tercero;
    c. Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio
    d. Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —123 de 425—

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7..1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1)*	**Programas Multidisciplinarios**	
Recurso*	**Descripción***	**Control***
- Programas de antivirus - Programas de malware	Antivirus Kaspersky Software anti malware, Microsoft Defender	Software proporcionado por la unidad de sistemas de la DGOAE Software, propio del sistema operativo, no se cuenta con el dato de la licencia

7..2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1)*	**Programas Multidisciplinarios**	
Medida de seguridad*	**Procedimiento***	**Responsable***
-Programas de antivirus. -Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	*Indicar:* Área de Sistemas de la DGOAE

7..3. Resultados de la evaluación y pruebas a las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 124 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1)*	**Programas Multidisciplinarios**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Programas de antivirus. Programas de malware	Sin virus detectados Sin incidentes de ataque por malware.	-Área de Sistemas de la DGOAE -Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 125 de 425—

7..4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-05**	
(Nombre del sistema A1)*	**Programas Multidisciplinarios**	
Medida de seguridad*	**Acciones***	**Responsable***
Almacenaje	Las bases se encuentran en los equipos de cómputo de la DGOAE y respaldas en un solo contenedor.	*Responsable y Encargados del sistema.*

8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —126 de 425—

Universitarios por la educación de jóvenes y adultos

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	**DGOAE-DSS–2022-06**
(Nombre del sistema A1) *	**Universitarios por la educación de jóvenes y adultos**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación - Nombre Completo -Datos de Contacto, número telefónico de domicilio y celular, correo electrónico. Datos académicos - Número de Cuenta UNAM - Facultad y Carrera
Responsable*:	
Nombre*:	**Lic. Lorenzo Rossi Hernandez**
Cargo*:	Jefe del Depto. de Modelo Educativos de Programas de Servicio Social
Funciones*:	Responsable de programa, llevar la gestión buen desarrollo del programa, gestión de los recursos materiales.
Obligaciones*:	Implementar métodos de alfabetización y el uso de los materiales educativos aplicando técnicas de motivación y participación, proporcionando acompañamiento y asesoría a los educandos en su proceso educativo.
	Encargados:
(Nombre del Encargado 1*)	**Lic. Claudia Navarrete García**
Cargo*:	**Directora de Servicio Social**
Funciones*:	Evaluar las actividades a desarrollar en el tratamiento de los datos personales, validar y ponderar los datos que se soliciten para los fines primordiales del Programa de Servicio Social.
Obligaciones*:	Dirigir, evaluar y delegar funciones a los responsables que manejan y llevan a conformidad los datos que se requerirán de los participantes en el programa, asignando cargos actividades y roles a

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —127 de 425—

	cada uno de los participantes.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único¨*	DGOAE-DSS–2022-06
(Nombre del sistema A1*)	Universitarios por la educación de jóvenes y adultos
Tipo de soporte:*	Tipo de Soporte Electrónico y Físico.
Descripción:*	Base de datos en Excel
Características del lugar donde se resguardan los soportes:*	Las Bases de Datos están en alojamiento en PC, propiedad de la UNAM situada en la DGOAE y asignada al área de Servicio Social en el Departamento de Modelos Educativos de Programas de Servicio Social. Los expedientes físicos están almacenados y catalogados de acuerdo con los Instrumentos de Control y Consulta Archivística de la UNAM, en resguardo en un archivero con seguro, en las instalaciones de la Dirección de Social en el área asignada por la Dirección General de Orientación y Atención Educativa.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-06	
(Nombre del sistema A1) *	**Universitarios por la educación de jóvenes y adultos**	
Riesgo*	**Impacto***	**Mitigación***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 128 de 425—

[redacted]		

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-06	
(Nombre del sistema A1) *	**Universitarios por la educación de jóvenes y adultos**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-06		
(Nombre del sistema A1) *	**Universitarios por la educación de jóvenes y adultos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 129 de 425—

[redacted]

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —130 de 425—

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	DGOAE-DSS–2022-06
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica.
Transferencias mediante el traslado de soportes electrónicos:	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario. Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

5. Señalar las medidas de seguridad que ha implementado el área

universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.

6. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;

   No aplica

   b) Para soportes físicos: Número o clave del expediente utilizado, y

   Los soportes físicos, están clasificados con forme a los Instrumentos de Control y Consulta Archivística por año

   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Los soportes físicos están debidamente catalogados y almacenados en un cubículo designado por la dependencia con cerrojo en la planta alta de la DGOAE.

3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   Los soportes físicos están a resguardo del encargado en las instalaciones de la DGOAE catalogados según lo estipulado conforme a los Instrumentos de Control y Consulta Archivística

4. La manera en que asegura la integridad de las bitácoras, y
   Se encuentran en un área de signada en un archivero con cerrojo y solo el encargado del programa tiene acceso.

5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Solo tiene acceso el responsable en caso de necesitar datos de referencia.

   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —131 de 425—

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
    a. La persona que resolvió el incidente;
    b. La metodología aplicada;
    c. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
    d. Para soportes electrónicos: Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.
2. Si el registro está en soporte físico o en soporte electrónico;
3. Cómo asegura la integridad de dicho registro, y
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 132 de 425—

horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

- Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

- Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

- En cada una de las entradas está instalado un módulo de vigilancia con control de acceso automatizado, el acceso se brinda únicamente verbalmente.

3. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —133 de 425—

de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas

- Dentro de las instalaciones, las oficinas están habilitadas con puerta con cerradura a llave que solo el personal autorizado tiene, los documentos en el sistema electrónico están contenidos en los equipos de cómputo, al cual se accede por contraseña.

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?

   - Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

2. ¿Cómo las autentifica?

   - Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. ¿Cómo les autoriza el acceso?

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
b) ¿Es discrecional (matriz de control de acceso)?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —134 de 425—

c) ¿Está basado en roles (perfiles) o grupos?
d) ¿Está basado en reglas?

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:
   a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
   b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

4. Administración de perfiles de usuario y contraseñas:
   a) ¿Quién da de alta nuevos perfiles?
   b) ¿Quién autoriza la creación de nuevos perfiles?
   c) ¿Se lleva registro de la creación de nuevos perfiles?

5. Acceso remoto al sistema de tratamiento de datos personales:
   a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
   b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
   c) ¿Cómo se evita el acceso remoto no autorizado?

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos__, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual _____,
   c) Periodicidad con que los realiza: _____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad
3. Cómo y dónde archiva esos medios, y
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 135 de 425—

IX. PLAN DE CONTINGENCIA

4. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
5. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
6. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
   b) Si el sitio es propio o subcontratado con un tercero;
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-06	
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**	
Recurso*	**Descripción***	**Control***
Programas de antivirus Programas de malware	Antivirus Kaspersky Software anti malware, Microsoft Defender	Software proporcionado por la unidad de sistemas de la DGOAE Software, propio del sistema operativo, no se cuenta con el dato de la licencia

7.2. Procedimiento para la revisión de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —136 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-06**	
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**	
Medida de seguridad*	**Procedimiento***	**Responsable***
-Programas de antivirus. -Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	Área de Sistemas de la DGOAE

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**		
Identificador único*	**DGOAE-DSS–2022-06**	
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Programas de antivirus. Programas de malware	Sin virus detectados Sin incidentes de ataque por malware.	-Área de Sistemas de la DGOAE -Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —137 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-06**	
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**	
Medida de seguridad*	**Acciones***	**Responsable***
Almacenaje	Las bases se encuentran en los equipos de cómputo de la DGOAE y respaldas en un solo contenedor.	*Responsable y Encargados del sistema.*

8. Programa específico de capacitación

8.1.Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-06**		
(Nombre del sistema A1)*	**Universitarios por la educación de jóvenes y adultos**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Platica informativa sobre la protección de datos.	Impartida por la Dra. Pichardo de la Unidad de Transparencia de la UNAM. el 3 de febrero de 2021	3 horas.	Responsables de Servicio Social de facultades, escuelas, institutos y centros.

8.2.Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —138 de 425—

Identificador único*	DGOAE-DSS–2022-06		
(Nombre del sistema A1)*	Universitarios por la educación de jóvenes y adultos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementación de aviso de privacidad. Implementación de la carta de confidencialidad.	El aviso de privacidad se muestra al pie de los correos enviados, en la publicación de la convocatoria de registro de Servicio Social. La carta de confidencialidad es solicitada entre los coordinadores y responsables del Servicio Social.	El aviso es publicado en cada una de las convocatorias y eventos del programa y esta colocado al pie del correo institucional del cual parte la comunicación con los enlaces y prestadores del Servicio Social. En proceso, se está llevando a cabo con los nuevos registros de coordinadores y responsables del Servicio Social para el ciclo 2021-2022	Parcial Está dirigido a los coordinadores, responsables y prestadores del programa de Servicio Social.

9. Mejora continua

9.1. **Actualización y mantenimiento de sistemas de información**

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-06		
(Nombre del sistema A1)*	Universitarios por la educación de jóvenes y adultos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Depurar y evaluar los datos solicitados para el programa de Servicio Social.	Revisión de los datos solicitados para el programa de Servicio Social y solo mantener los primordiales para el éxito del programa.	De marzo a mayo de 2022. .	El sistema será más factible en ejecución y evaluación de los resultados al contemplar las variables más importantes para las metas del programa.

9.2. **Actualización y mantenimiento de equipo de cómputo**

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	DGOAE-DSS–2022-06

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —139 de 425—

(Nombre del sistema A1)*	Universitarios por la educación de jóvenes y adultos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de Software Comprobación de licencias vigentes. Mantenimiento correctivo y preventivo del equipo de cómputo.	Mantiene en óptimas condiciones el funcionamiento de los equipos de cómputo y se previenen perdidas parciales o totales de los archivos. La comprobación de las licencias vigentes mantendrá al día contra amenazas contra virus o software malintencionado. Con la revisión periódica del equipo y con su buen funcionamiento se previenen la pérdida total de la información y se podrán programar respaldos1 de la información.	El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo de dos a tres veces por año y en caso de demanda son atendidas las solicitudes de dos a tres días dependiendo del recurso solicitado.	Previene la perdida de datos por malfuncionamiento El mantenimiento previene que los circuitos no presenten fallas y no se pierdan los archivos contenidos en los discos duros.

9.3. **Procesos para la conservación, preservación y respaldos de información**

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-06	
(Nombre del sistema A1)*	Universitarios por la educación de jóvenes y adultos	
Proceso*	**Descripción***	**Responsable***
Concentrar en un solo contenedor el histórico de las bases de datos. Programar respaldos de los archivos.	De esta manera se contempla que los datos no estén en diferentes dispositivos y prevenir la pérdida o mal uso de los datos. Teniendo contemplado un respaldo periódico de los archivos se mitiga la perdida de los archivos por mal funcionamiento de los equipos de cómputo o por un archivo accidental.	Responsable del programa, con apoyo y asesoría del área de Sistemas de la DGOAE.

9.4. **Procesos de borrado seguro y disposición final de equipos y componentes informáticos**

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único*	DGOAE-DSS–2022-06

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —140 de 425—

(Nombre del sistema A1)*	Universitarios por la educación de jóvenes y adultos	
Proceso*	**Descripción***	**Responsable***
Cambio de equipo de cómputo o actualización.	En ocasiones la DGOAE actualiza los equipos de cómputo o se hacen actualizaciones en los dispositivos, para los cuales se hace un respaldo de los archivos y se procede a un formateo a bajo nivel el cual modifica el disco de almacenamiento para que los datos sean irrecuperables y no sean usados.	Área de Sistemas de la DGOAE. No se ha necesitado este proceso en la actualidad.

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

F) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

La cancelación del sistema mediante un escrito donde indique lo siguiente:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

G) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —141 de 425—

4. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

H) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

I) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Portal de Orientación Educativa que se encuentren dentro sistema.

J) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —142 de 425—

Impulso al Desarrollo de Empresas Sociales

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Servicio Social.**	
Identificador único*	DGOAE-DSS-2022-07
(Nombre del sistema A1) *	**Impulso al Desarrollo de Empresas Sociales**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación - Nombre Completo -Datos de Contacto, número telefónico de domicilio y celular, correo electrónico. Datos académicos - Número de Cuenta UNAM - Facultad y Carrera
Responsable*:	
Nombre*:	Lic. María del Carmen Castro Bentura
Cargo*:	Jefe de Unidad
Funciones*:	Responsable de programa, llevar la gestión buen desarrollo del programa.
Obligaciones*:	Selección, capacitación, coordinación y supervisión de prestadores de servicio social y universitarios voluntarios. Gestión de los recursos materiales para la operación del programa. Gestión de visitas a dependencias universitarias u otros recintos culturales.
	Encargados:
(Nombre del Encargado 1*)	Lic. Claudia Navarrete García
Cargo*:	Directora de Servicio Social
Funciones*:	Evaluar las actividades a desarrollar en el tratamiento de los datos personales, validar y ponderar los datos que se soliciten para los fines primordiales del Programa de Servicio Social
Obligaciones*:	Dirigir, evaluar y delegar funciones a los responsables que manejan y llevan a conformidad

ID del Documento: gIPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —143 de 425—

	los datos que se requerirán de los participantes en el programa, asignando cargos actividades y roles a cada uno de los participantes

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.	
Identificador único¨*	DGOAE-DSS–2022-07
(Nombre del sistema A1*)	Impulso al Desarrollo de Empresas Sociales
Tipo de soporte:*	Tipo de Soporte Electrónico
Descripción:*	Base de datos en Excel
Características del lugar donde se resguardan los soportes:*	Las Bases de Datos están en alojamiento en PC, propiedad de la UNAM situada en la DGOAE y asignada al área de Servicio Social en el Departamento de Impulso al Desarrollo de Empresas Sociales. Los expedientes físicos están almacenados y catalogados de acuerdo con los Instrumentos de Control y Consulta Archivística de la UNAM, en resguardo en un archivero con seguro, en las instalaciones de la Dirección de Social en el área asignada por la Dirección General de Orientación y Atención Educativa.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-07	
(Nombre del sistema A1) *	**Impulso al Desarrollo de Empresas Sociales**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —144 de 425—

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	DGOAE-DSS–2022-07	
(Nombre del sistema A1) *	Impulso al Desarrollo de Empresas Sociales	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-07		
(Nombre del sistema A1) *	Impulso al Desarrollo de Empresas Sociales		
Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —145 de 425—

Identificador único*	DGOAE-DSS–2022-07
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No aplica
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	El envío se realiza a través del correo institucional y enviado al correo institucional del destinatario. Solo se mandarán a través de un correo institucional y al correo institucional del solicitante y titular. Se solicita indicar que las transferencias de datos personales se recibieron por el titular del correo institucional al que fue enviado a modo de acuse de recibido.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

III.

IV.

V.

VI.

VII.

VIII.

IX.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —146 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Recurso*	**Descripción***	**Control***
Programas de antivirus Programas de malware	Antivirus Kaspersky Software anti malware, Microsoft Defender	Software proporcionado por la unidad de sistemas de la DGOAE Software, propio del sistema operativo, no se cuenta con el dato de la licencia

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Medida de seguridad*	**Procedimiento***	**Responsable***
-Programas de antivirus. -Programas de malware	Revisión periódica cada semana. La ejecución del malware esta de forma permanente.	Área de Sistemas de la DGOAE

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Programas de antivirus. Programas de malware	Sin virus detectados Sin incidentes de ataque por malware.	-Área de Sistemas de la DGOAE

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —147 de 425—

		-Los programas están configurados para detectar intromisiones o ataques de virus en el momento y una examinación profunda cada 7 días.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Medida de seguridad*	**Acciones***	**Responsable***
Almacenaje	Las bases se encuentran en los equipos de cómputo de la DGOAE y respaldas en un solo contenedor.	*Responsable y Encargados del sistema.*

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-07**		
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Platica informativa sobre la protección de datos.	Impartida por la Dra. Pichardo de la Unidad de Transparencia de la UNAM. el 3 de febrero de 2021	3 horas.	Responsables de Servicio Social de facultades, escuelas, institutos y centros.

8.2. Programa de difusión de la protección a los datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —148 de 425—

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-07		
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementación de aviso de privacidad. Implementación de la carta de confidencialidad.	El aviso de privacidad se muestra al pie de los correos enviados, en la publicación de la convocatoria de registro de Servicio Social. La carta de confidencialidad es solicitada entre los coordinadores y responsables del Servicio Social.	El aviso es publicado en cada una de las convocatorias y eventos del programa y esta colocado al pie del correo institucional del cual parte la comunicación con los enlaces y prestadores del Servicio Social. En proceso, se está llevando a cabo con los nuevos registros de coordinadores y responsables del Servicio Social para el ciclo 2021-2022	Parcial Está dirigido a los coordinadores, responsables y prestadores del programa de Servicio Social.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	DGOAE-DSS–2022-07		
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Depurar y evaluar los datos solicitados para el programa de Servicio Social.	Revisión de los datos solicitados para el programa de Servicio Social y solo mantener los primordiales para el éxito del programa.	Sin periodo de inscripción para este programa, por el momento para 2022. .	El sistema será más factible en ejecución y evaluación de los resultados al contemplar las variables más importantes para las metas del programa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —149 de 425—

9.2. Actualización y mantenimiento de equipo de cómputo

(Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.			
Identificador único*	**DGOAE-DSS–2022-07**		
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de Software Comprobación de licencias vigentes. Mantenimiento correctivo y preventivo del equipo de cómputo.	Mantiene en óptimas condiciones el funcionamiento de los equipos de cómputo y se previenen perdidas parciales o totales de los archivos. La comprobación de las licencias vigentes mantendrá al día contra amenazas contra virus o software malintencionado. Con la revisión periódica del equipo y con su buen funcionamiento se previenen la pérdida total de la información y se podrán programar respaldos1 de la información.	El área de Sistemas de la DGOAE tiene programado el mantenimiento de los equipos de cómputo de dos a tres veces por año y en caso de demanda son atendidas las solicitudes de dos a tres días dependiendo del recurso solicitado.	Previene la perdida de datos por malfuncionamiento. El mantenimiento previene que los circuitos no presenten fallas y no se pierdan los archivos contenidos en los discos duros.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —150 de 425—

Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Proceso*	**Descripción***	**Responsable***
Concentrar en un solo contenedor el histórico de las bases de datos. Programar respaldos de los archivos.	De esta manera se contempla que los datos no estén en diferentes dispositivos y prevenir la pérdida o mal uso de los datos. Teniendo contemplado un respaldo periódico de los archivos se mitiga la perdida de los archivos por mal funcionamiento de los equipos de cómputo o por un archivo accidental.	Responsable del programa, con apoyo y asesoría del área de Sistemas de la DGOAE.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. Dirección de Servicio Social.		
Identificador único*	**DGOAE-DSS–2022-07**	
(Nombre del sistema A1)*	**Impulso al Desarrollo de Empresas Sociales**	
Proceso*	**Descripción***	**Responsable***
Cambio de equipo de cómputo o actualización.	En ocasiones la DGOAE actualiza los equipos de cómputo o se hacen actualizaciones en los dispositivos, para los cuales se hace un respaldo de los archivos y se procede a un formateo a bajo nivel el cual modifica el disco de almacenamiento para que los datos sean irrecuperables y no sean usados.	Área de Sistemas de la DGOAE. No se ha necesitado este proceso en la actualidad.

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —151 de 425—

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
4. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.

ID del Documento: girPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —152 de 425—

- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Portal de Orientación Educativa que se encuentren dentro sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción fisica o desmagnetización.

Voluntariado

1. Inventario de sistemas de tratamiento de datos personales
2. Estructura y descripción de los sistemas de tratamiento de datos personales
3. Análisis de riesgos
4. Análisis de brecha
5. Plan de trabajo
6. Medidas de seguridad implementadas
7. Mecanismos de monitoreo y revisión de las medidas de seguridad
8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —153 de 425—

Dirección de Planeación

Registro de actividades en línea

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	DGOAE-BUT-2020-1
Nombre del sistema*:	Registro de actividades en línea
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales que se le solicitan a las y los universitarios son: Fecha de nacimiento, sexo, teléfono de casa, teléfono celular y correo electrónico. Datos académicos que se le solicitan a las y los universitarios son: Número de cuenta, máximo nivel de estudios en la UNAM, situación académica, semestre (en caso de ser estudiante), año de egreso (en caso de haber concluido sus estudios a cualquier nivel), Escuela/Facultad/Instituto/Centro, carrera/programa dónde realizo sus estudios, promedio, nivel de inglés, idioma y el nivel del idioma. El nombre de las y los universitarios se obtiene de un web service que nos provee DGAE.
	Responsable*:
Nombre*:	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	- Cumplir con las normas de trabajo. - Ejecutar el trabajo en forma y tiempo.
	Encargados:
Nombre del Encargado 1*	- Mtro. Víctor Arturo Morales Díaz
Cargo*:	- Académico

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —154 de 425—

Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Guardar y proteger los datos de los usuarios registrados en el sistema.
	Usuarios
Nombre del Usuario 1*	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 2*	Elizabeth Navarrete Morales
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 3*	Lic. Paola Gabriela Sosa Flores
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 4*	Lic. Miriam Jimenez Ponce
Cargo*:	Profesionista Titulado
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —155 de 425—

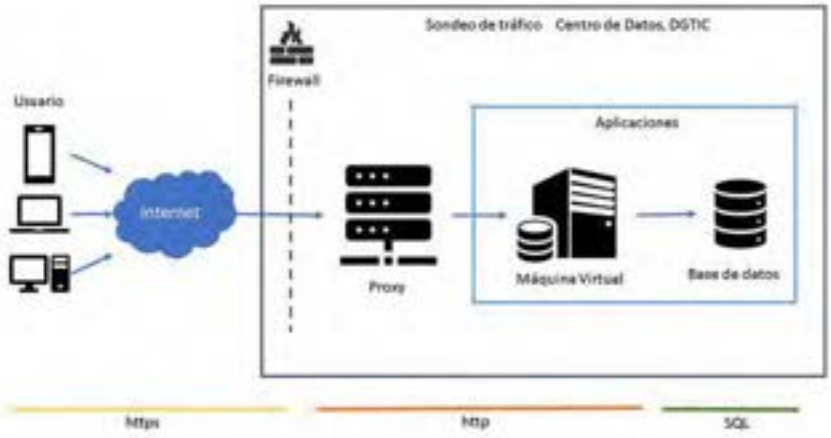
Nombre del Usuario 5*	Lic. Ruth Méndez Hernández
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 6*	Mtra. Susana Chávez Jaramillo
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único*:	DGOAE-BUT-2020-1
Nombre del sistema*:	Registro de actividades en línea
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos relacional en MySQL
Características del lugar donde se resguardan los soportes*:	Alojada en el centro de datos de la DGTIC, que cuenta con seis niveles de seguridad. Nivel 1: Seguridad de acceso físico. • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware. • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido.

ID del Documento: gIrPdH8ZIn1+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —156 de 425—

	• El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP. • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la base de datos. Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. o Responsable del sistema (personal de la BUT), requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la base de datos: • Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol. • Respaldos de la base de datos.

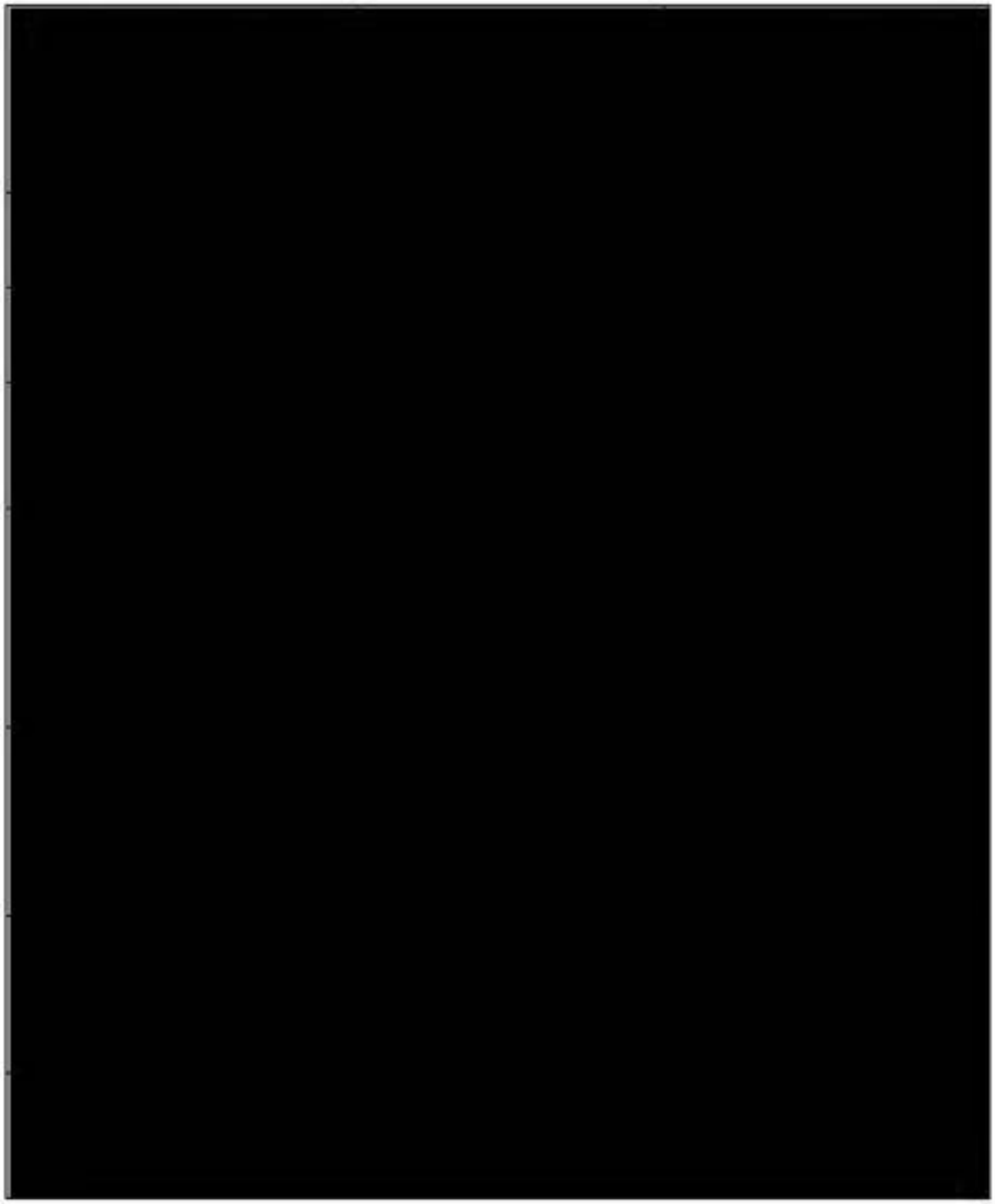


3. Análisis de riesgos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —157 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-1	
Nombre del sistema*:	Registro de actividades en línea	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 158 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —159 de 425—

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-1	
Nombre del sistema*:	Registro de actividades en línea	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —160 de 425—

[redacted]

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*:	DGOAE-BUT-2020-1		
Nombre del sistema*:	Registro de actividades en línea		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —161 de 425—

6. Medidas de seguridad implementadas

I. TRANSFERENCIA DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	DGOAE-BUT-2020-1
Nombre del sistema*:	Registro de actividades en línea
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	No aplica.
Transferencias mediante el traslado de soportes electrónicos	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica. En caso que se envíen documentos, éstos deberán tener contraseña para poder abrirlo.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. No se cuentan con soportes físicos.
2. No se cuenta con soportes físicos.

III. BITÁCORA PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras**
   a) **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida**

   El personal de la BUT accede a consultar los datos del alumnado, egresadas y egresados de la UNAM. Las bitácoras con las que se cuentan son las de apache y MySQL.

   b) **Para soportes físicos: Número o clave del expediente utilizado**

   No se cuenta con expedientes físicos.

   c) **Para soporte electrónico: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos**

   Con los datos del alumnado, egresadas y egresados de la UNAM que se registraron al evento se realizan estadísticas.
2. **Si las bitácoras están en soporte físico o en soporte electrónico**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —162 de 425—

Soporte electrónico

3. **Lugar dónde almacenan las bitácoras y por cuánto tiempo**
   En el servidor dónde se encuentra el sistema, el cual se encuentra en DGTIC.
4. **La manera en que asegura la integridad de las bitácoras**
   - Acceso restringido por usuario, contraseña y dirección IP.
   - Respaldo de la base de datos.
   - Los respaldos se generan en el servidor de DGTIC, posteriormente se copian a una computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro.
5. **Respecto del análisis de las bitácoras**
   a) **Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza**
   Encargado del sistema, cada que se presenta algún incidente o reporte por parte de los usuarios.
   b) **Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.**
   Se utilizan editores de texto, vi, Notepad++, vscode, block de notas.

IV. REGISTRO DE INCIDENTES

5. **Los datos que registra:**
   e) **La persona que resolvió el incidente.** Nombre del encargado o de la persona que resolvió el incidente.
   f) **La metodología aplicada.** Se registra la incidencia, los daños y acciones para prevenir otra.
   g) **Para soportes físicos.** No se cuenta con soportes físicos.
   h) **Para soportes electrónicos.** El respaldo que se hace de la base de datos incluye: tablas, campos y registros de cada una de ellas.
6. **Si el registro está en soporte físico o en soporte electrónico.** El soporte se encuentra en electrónico.
7. **Cómo asegura la integridad de dicho registro.** Reglas de validación, realizando transacciones y por medio de los respaldos.
8. **Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.** El encargado y/o el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior**
   La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —163 de 425—

en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?

   Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. Seguridad perimetral interior

Las oficinas o cubículos de la Bolsa Universitaria de Trabajo son: Oficina 63, cubículo 1, cubículo 4, cubículo 11, cubículo 12, cubículo 16, cubículo 59 y área central, todos se encuentran en la planta baja de la Dirección General de Orientación y Atención Educativa.

Para las personas que acceden a dichos espacios interiores:

1. **¿Cómo las identifica?**

   Las personas a quienes atendemos son: enlaces de entidades académicas, alumnado, egresadas y egresados de la UNAM.

2. **¿Cómo las autentifica?**

   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. **¿Cómo les autoriza el acceso?**

   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —164 de 425—

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para este sistema el alumnado, egresadas y egresados de la UNAM no pueden actualizar sus datos personales y/o académicos.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

5. **Modelo de control de acceso**

   Este sistema se encuentra montado en los servidores de DGTIC

   e) **¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?** Si.

   f) **¿Es discrecional (matriz de control de acceso)?** No.

   g) **¿Está basado en roles (perfiles) o grupos?** Si

   h) **¿Está basado en reglas?** Si

6. **Perfiles de usuario y contraseñas en el sistema operativo de red:**

   d) **¿Cuenta con sistema operativo de red instalado en sus equipos?** Sí, se cuenta con equipos con sistema operativo Windows, algunos tienen Linux y dónde está montado el sistema es un Linux.

   e) **¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?** Sí, los equipos que se encuentran en la DGOAE cuentan con este manejo, así como el equipo de la DGTIC, dónde se encuentra el sistema.

   f) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.

7. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:**

   c) **¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?** Si.

   d) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.

8. **Administración de perfiles de usuario y contraseñas:**

   g) **¿Quién da de alta nuevos perfiles?** El jefe del Departamento de Informática se pone en contacto con DGTIC y hace esta solicitud.
   Para el sistema de registro de actividades en línea, quién realiza esta acción es el jefe del Departamento de Bolsa Universitaria de Trabajo o el encargado del sistema.

   h) **¿Quién autoriza la creación de nuevos perfiles?** La jefa del Departamento de Bolsa Universitaria de Trabajo se pone en contacto con

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —165 de 425—

el jefe del Departamento de Informática, para indicar que necesita un nuevo perfil. Finalmente, esté se pone en contacto con DGTIC para la creación del nuevo perfil.

Para el sistema de registro de actividades en línea, quién realiza esta acción es el jefe del Departamento de Bolsa Universitaria de Trabajo o el encargado del sistema.

9. **Acceso remoto al sistema de tratamiento de datos personales:**
   i) **¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?** No.
   j) **¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?** Si
   k) **¿Cómo se evita el acceso remoto no autorizado?** Las credenciales de acceso solo se dan a personas que están adscritas a la DGOAE, se firma una carta de confidencialidad.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. **Señalar si realiza respaldos**
   a) **Completos** X**, diferenciales o incrementales;**
   b) **De forma automática o manual** X**,**
   c) **Periodicidad con que los realiza:** Cada semana.
2. **El tipo de medios que utiliza para almacenar las copias de seguridad:** Se realizan por medio del comando mysqldump, él cual genera un archivo .sql, el cual se guarda en el servidor, posteriormente se copia a la computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro, finalmente el archivo se borra del servidor.
3. **Cómo y dónde se archiva esos medios:** La computadora se encuentra en la DGOAE.
4. **Quién es el responsable de realizar estas operaciones:** El encargado del sistema.

DGTIC realiza sus propios respaldos.

IX. PLAN DE CONTINGENCIA

4. Plan de contingencia que garantiza la continuidad de la operación del sistema.
   - Tener respaldos de la base de datos y del código.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —166 de 425—

- Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
- Los requerimientos con los que debe contar este espacio son los requeridos por la versión en que se programo el sistema a recuperar.
- El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
- Una ves que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
- Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una ves hecha la conexión se carga el respaldo de la base de datos.
- En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
- Realizar pruebas al sistema de inicio de sesión, cierre de sesión, consulta y registro de las y los universitarios a las actividades.

5. No aplica
6. No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-1	
Nombre del sistema*:	Registro de actividades en línea	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit	Extensión del navegador que esta diseñada para probar vulnerabilidades en el sistema.	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —167 de 425—

Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicarán el tráfico que existen en el servidor.	Se hace manual y solamente será usada cuando se genere un ataque al sistema.
Bitácoras generadas por el servidor	Éstas nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas por la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.

7.2. Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-1	
Nombre del sistema*:	Registro de actividades en línea	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizaciones.	Revisión de páginas oficiales sobre las actualizaciones del lenguaje de programación.	Encargado del sistema.
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones.	Encargado del sistema.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —168 de 425—

Identificador único*	DGOAE-BUT-2020-1	
Nombre del sistema*	Registro de actividades en línea	
Medida de seguridad*	Resultado de evaluación*	Responsable*
Pruebas de vulnerabilidad.	No se encontraron fallas.	Encargado del sistema.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	DGOAE-BUT-2020-1	
Nombre del sistema*	Registro de actividades en línea	
Medida de seguridad*	Acciones*	Responsable*
Pruebas de vulnerabilidad	a) Se corrigieron las partes del código que son vulnerables b) Seguir en constante actualización.	Encargado del sistema

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —169 de 425—

Dirección de Planeación.			
Identificador único*	DGOAE-BUT-2020-1		
Nombre del sistema*	Registro de actividades en línea		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos	Cursos sobre programación en PHP, MySQL, Linux, seguridad informática, creación de certificados SSL, protección a las máquinas virtuales, hacker ético, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único*	DGOAE-BUT-2020-1

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —170 de 425—

Nombre del sistema*	Registro de actividades en línea		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cartas de confidencialidad	Se le hace llegar y firmar una carta de confidencialidad al personal que va a tener acceso al sistema.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Para todo el personal de la BUT, su objetivo es que estén enteradas(os) de que trabajaran con datos del alumnado, egresadas y egresados de la UNAM. Una vez firmada la carta comienza la vigencia y esta se actualiza dependiendo las circunstancias por las que esté pasando la UNAM.
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	La distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Permanente.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

9. Mejora continua

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —171 de 425—

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.			
Identificador único*	DGOAE-BUT-2020-1		
Nombre del sistema*	Registro de actividades en línea		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de mensajes de error, éxito y de información	Actualizar los mensajes del sistema para que no muestre contenido de la base de datos o de la configuración del servidor.	Permanente	Total.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.			
Identificador único*	DGOAE-BUT-2020-1		
Nombre del sistema*	Registro de actividades en línea		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo, lenguaje de programación y de la base de datos.	Es importante tener las versiones más actualizadas para evitar que nuestro equipo o software quedé obsoleto y sin soporte.	Depender de la adquisición del nuevo equipo e instalación del software.	Parcial.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	DGOAE-BUT-2020-1	
Nombre del sistema*	Registro de actividades en línea	
Proceso*	**Descripción***	**Responsable***

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —172 de 425—

Los respaldos se realizan cada semana.	Los respaldos se realizan mediante el comando mysqldump, este comando genera un archivo con toda la información de las tablas que guardan la información de este sistema. Como el espacio que nos brinda DGTIC no es muy grande, los archivos se copian a una máquina que se encuentra en la DGOAE. El nombre del archivo se compone del nombre del sistema (registro_actividades) y de la fecha en que se realizó el respaldo y la extensión del archivo es .sql	Encargado del sistema.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-1	
Nombre del sistema*	Registro de actividades en línea	
Proceso*	**Descripción***	**Responsable***
Borrado	Las y los universitarios pueden borrar su inscripción a alguna de las conferencias si ellos así lo desean. Es lo único que pueden borrar.	Universitarias y universitarios.
Limpieza de la base de datos.	Como cada año se realiza el Encuentro Virtual de Empleabilidad, al termino del evento, se limpia la base, es decir, los datos de las y los universitarios que se registraron al evento se insertan en una tabla histórica al igual que las inscripciones, esto con el motivo de obtener estadísticas por año.	Encargado del sistema.
Proceso de borrado de respaldos en soporte electrónicos	La información se borra de estos dispositivos solamente deberá guardar información del sistema. Formatear mediante borrado de bajo nivel.	Encargado del sistema o bien se le pide apoyo a la Dirección de Apoyo Técnico.

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —173 de 425—

Departamento de Bolsa Universitaria de Trabajo acordará la cancelación del sistema mediante un escrito donde indique lo siguiente:

a) Fecha de cuando deja de dar servicio el sistema.
b) Fecha de cancelación del sistema.
c) Motivo de la cancelación.
d) Si existe un sistema que lo reemplaza, poner la información del nuevo.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso y registro al sistema.
4. Solamente el administrador del sistema podrá ingresar.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Se realizará un último respaldo de la base de datos que el sistema utiliza para almacenar la información, está se guardará por si en un futuro se requiere realizar algún tipo de consulta, en un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por la BUT para su resguardo y acceso a la información de los datos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —174 de 425—

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Una vez que hayan pasado los días establecidos del bloqueo, se realizara lo siguiente:

1. Se retira del servidor el sistema Registro de actividades en línea.
2. Respaldo del código del sistema y de la base de datos.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA Y TRATAMIENTO DE DATOS PERSONALES.

Una vez que se tenga el respaldo de las tablas, solo se eliminaran de manera física estas tablas, ya que estas se encuentran en una base de datos que tiene más tablas y estás son usadas por diferentes sistemas.

Encuentro Virtual de Empleabilidad

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	DGOAE-BUT-2020-2
Nombre del sistema*:	Encuentro Virtual de Empleabilidad
Datos personales (sensibles o no) contenidos en el sistema*:	Universitarios: El nombre de las y los universitarios se obtiene de un web service que nos provee DGAE. • Datos personales que se le solicitan a las y los universitarios son: Correo electrónico, fecha de nacimiento, sexo, teléfono de casa y teléfono celular. • Datos académicos que se le solicitan a las y los universitarios son: Número de cuenta, máximo nivel de estudios en la UNAM, situación académica, semestre (en caso de ser estudiante), año de egreso (en caso de haber concluido sus estudios a cualquier nivel), Escuela/Facultad/Instituto/Centro, carrera/programa dónde realizo sus estudios, promedio, nivel de inglés, nivel de conversación del idioma inglés, certificación, vigente, nombre de la certificación y puntaje. Ponentes:

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 175 de 425—

	• Datos: nombre, correo electrónico, cargo, teléfono oficina, extensión, teléfono celular, foto, semblanza y nombre de la empresa/institución a la que pertenecen.
Responsable*:	
Nombre*:	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	- Cumplir con las normas de trabajo. - Ejecutar el trabajo en forma y tiempo.
	Encargados:
Nombre del Encargado 1*	Mtro. Víctor Arturo Morales Díaz
Cargo*:	Académico
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Guardar y proteger los datos de los usuarios registrados en el sistema.
	Usuarios
Nombre del Usuario 1*	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.
Nombre del Usuario 2*	Elizabeth Navarrete Morales
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —176 de 425—

	inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.
Nombre del Usuario 3*	Lic. Paola Gabriela Sosa Flores
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.
Nombre del Usuario 4*	Lic. Miriam Jimenez Ponce
Cargo*:	Profesionista Titulado
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.
Nombre del Usuario 5*	Lic. Ruth Méndez Hernández
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.
Nombre del Usuario 6*	Mtra. Susana Chávez Jaramillo
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: secciones, empresas, ponentes, conferencias y generar constancias de participación.

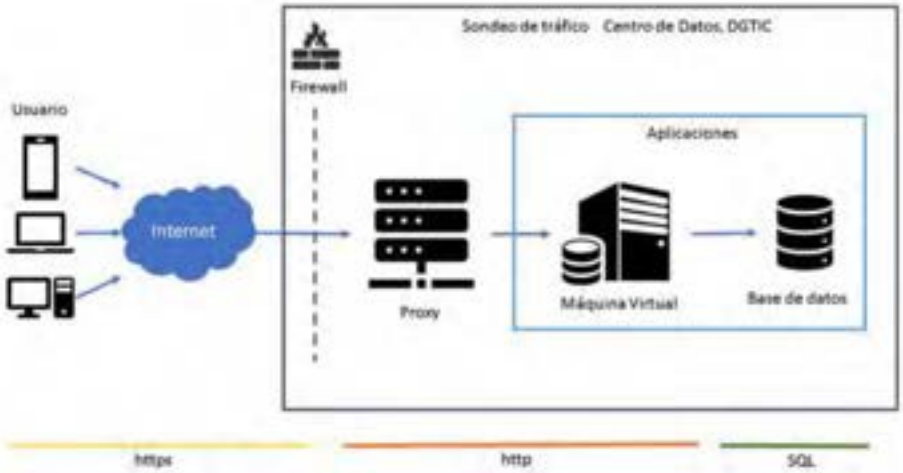
2. Estructura y descripción de los sistemas de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —177 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	DGOAE-BUT-2020-2
Nombre del sistema*:	Encuentro Virtual de Empleabilidad
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos relacional en MySQL
Características del lugar donde se resguardan los soportes*:	Alojada en el centro de datos de la DGTIC, que cuenta con seis niveles de seguridad. Nivel 1: Seguridad de acceso físico. • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware. • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP. • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la base de datos. Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. o Responsable del sistema (personal de la BUT), requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la base de datos:

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —178 de 425—

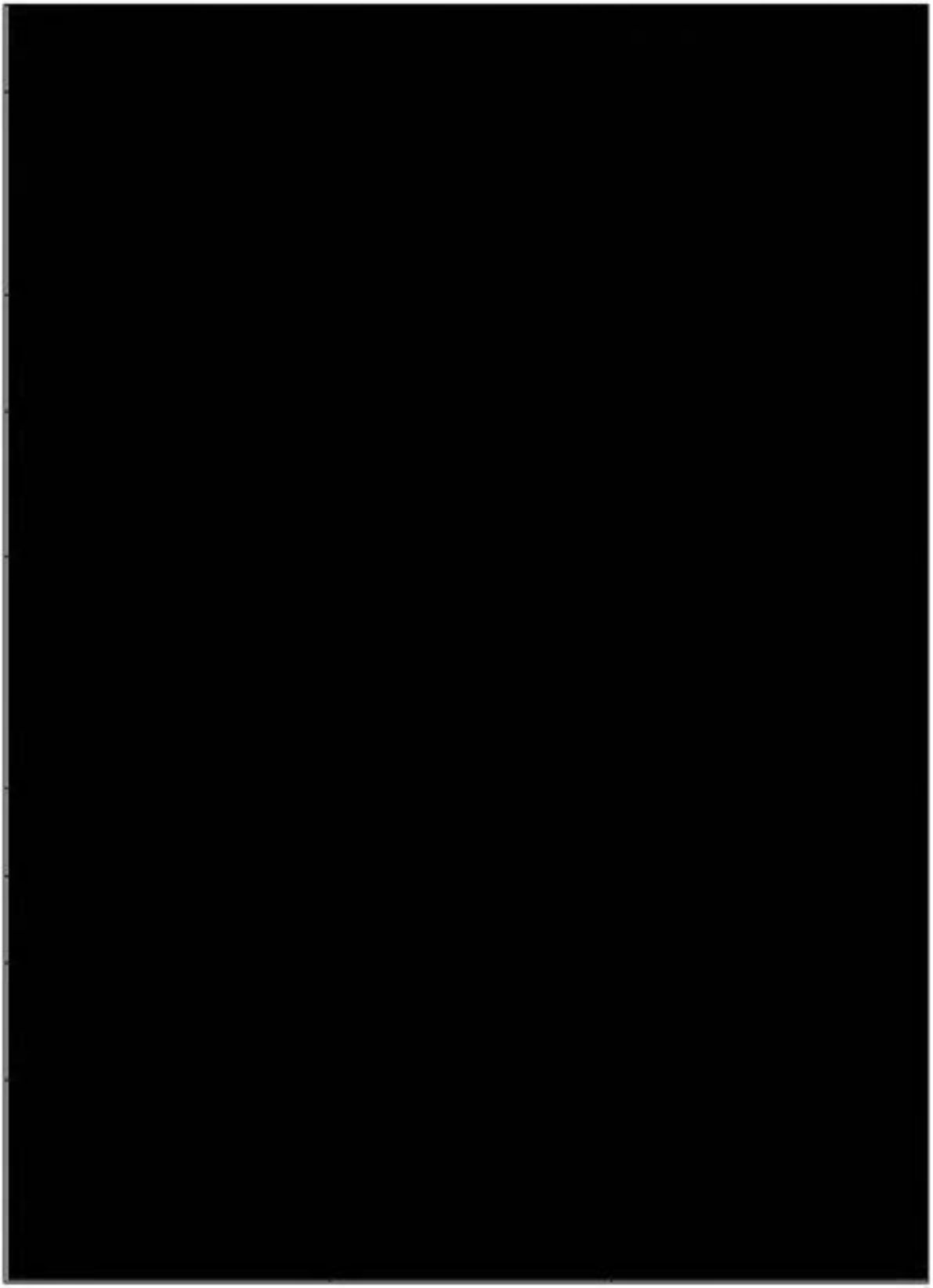
	• Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol. • Respaldos de la base de datos.



3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*:	DGOAE-BUT-2020-2	
Nombre del sistema*:	Encuentro Virtual de Empleabilidad	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —179 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 180 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-2	
Nombre del sistema*:	Encuentro Virtual de Empleabilidad	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —181 de 425—



5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*:	DGOAE-BUT-2020-2		
Nombre del sistema*:	Encuentro Virtual de Empleabilidad		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Implementar captcha.	Identificar en el sistema las páginas que tienen algún formulario y si éste cuenta con una página de inicio de sesión, para evitar accesos no autorizados.	Durante el periodo de uso del sistema (dos meses al año).	Total.
Validación de los datos ingresados.	Identificar las partes del código vulnerables.	Durante el desarrollo/mantenimeinto del sistema y el periodo de uso del mismo (dos meses al año).	Total.
Incorporación del aviso de privacidad.	El usuario este de acuerdo con el aviso de privacidad, puede hacer uso del sistema.	Durante el periodo de uso del sistema (dos meses al año).	Total.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 182 de 425—

Encriptación de la contraseña de los usuarios.	El framework de laravel utiliza bycrypt para encriptar la contraseña.	Durante el periodo de uso del sistema (dos meses al año).	Total.
Respaldar la información de la base de datos.	Contar con un respaldo de la información de la base de datos.	Durante el periodo de uso del sistema (dos meses al año).	Total.
Envío de documentos con contraseña.	Todos los documentos que contengan información de datos personales deberán tener contraseña.	Durante el periodo de uso del sistema (dos meses al año).	Total.

6. Medidas de seguridad implementadas

I. TRANSFERENCIA DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	DGOAE-BUT-2020-2
Nombre del sistema*:	Encuentro Virtual de Empleabilidad
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos	No aplica.
Transferencias mediante el traslado de soportes electrónicos	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	El enlace de bolsa de trabajo de cada facultad, por correo solicita la información de las y los universitarios que se registraron en el evento. La información se descarga en un archivo de Excel y es enviada por correo electrónico como respuesta a la solicitud. Los datos personales y académicos que se envían son los que se mencionan en el punto 1 Inventarios de sistemas de tratamiento de datos personales. Todos los documentos deberán tener contraseña para poder abrirlo.

ID del Documento: gIPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —183 de 425—

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. No se cuentan con soportes físicos.
2. No se cuenta con soportes físicos.

III. BITÁCORA PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras**
   a) **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida**

      El personal de la BUT accede a consultar los datos del alumnado, egresadas y egresados de la UNAM, conferencias, empresa y ponentes. Las bitácoras con las que se cuentan son las de apache, MySQL y la del framework laravel. En la base de datos se registra fecha y hora en la que se realiza el acceso.
   b) **Para soportes físicos: Número o clave del expediente utilizado**

      No se cuenta con expedientes físicos.
   c) **Para soporte electrónico: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos**

      Con los datos del del alumnado, egresadas y egresados de la UNAM que se registraron al evento se realizan estadísticas.
2. **Si las bitácoras están en soporte físico o en soporte electrónico**

   Soporte electrónico
3. **Lugar dónde almacenan las bitácoras y por cuánto tiempo**

   En el servidor dónde se encuentra el sistema, el cual se encuentra en DGTIC.
4. **La manera en que asegura la integridad de las bitácoras**
   - Acceso restringido por usuario, contraseña y dirección IP.
   - Respaldo de la base de datos.
   - Los respaldos se generan en el servidor de DGTIC, posteriormente se copian a una computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro.
5. **Respecto del análisis de las bitácoras**
   a) **Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza**

      Encargado del sistema, cada que se presenta algún incidente o reporte por parte de los usuarios.
   b) **Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.**

      Se utilizan editores de texto, vi, Notepad++, vscode, block de notas.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —184 de 425—

IV. REGISTRO DE INCIDENTES

1. **Los datos que registra:**
   a) **La persona que resolvió el incidente.**
   Nombre del encargado o de la persona que resolvió el incidente.
   b) **La metodología aplicada.**
   Se registra la incidencia, los daños y acciones para prevenir otra.
   c) **Para soportes físicos.**
   No se cuenta con soportes físicos.
   d) **Para soportes electrónicos.**
   El respaldo que se hace de la base de datos incluye: tablas, campos y registros de cada una de ellas.
2. **Si el registro está en soporte físico o en soporte electrónico.**
   El soporte se encuentra en electrónico.
3. **Cómo asegura la integridad de dicho registro.**
   Reglas de validación, realizando transacciones y por medio de los respaldos.
4. **Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.**
   El encargado y/o el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior**

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 185 de 425—

Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. **Seguridad perimetral interior**

Para las personas que acceden a dichos espacios interiores:

Las oficinas o cubículos de la Bolsa Universitaria de Trabajo son: Oficina 63, cubículo 1, cubículo 4, cubículo 11, cubículo 12, cubículo 16, cubículo 59 y área central, todos se encuentran en la planta baja de la Dirección General de Orientación y Atención Educativa.

1. **¿Cómo las identifica?**

   Las personas a quienes atendemos son: enlaces de entidades académicas, alumnado, egresadas y egresados de la UNAM.

2. **¿Cómo las autentifica?**

   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. **¿Cómo les autoriza el acceso?**

   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para este sistema el alumnado, egresadas y egresados de la UNAM no pueden actualizar sus datos personales y/o académicos. Los datos de los ponentes se actualizan en caso de que estos vuelvan a impartir una conferencia y si ellos lo piden. El personal de la BUT es el encargado de realizar dicha actualización.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. **Modelo de control de acceso**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 186 de 425—

Este sistema se encuentra montado en los servidores de DGTIC

a) **¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?** Si
b) **¿Es discrecional (matriz de control de acceso)?** No
c) **¿Está basado en roles (perfiles) o grupos?** Si
d) **¿Está basado en reglas?** Si

2. **Perfiles de usuario y contraseñas en el sistema operativo de red:**
   a) **¿Cuenta con sistema operativo de red instalado en sus equipos?** Sí, se cuenta con equipos con sistema operativo Windows, algunos tienen Linux y dónde esta montado el sistema es un Linux.
   b) **¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?** Sí, los equipos que se encuentran en la DGOAE cuentan con este manejo, así como el equipo de la DGTIC, dónde se encuentra el sistema.
   c) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.
3. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:**
   a) **¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?** Si.
   b) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.
4. **Administración de perfiles de usuario y contraseñas:**
   a) **¿Quién da de alta nuevos perfiles?** El jefe del Departamento de Informática se pone en contacto con DGTIC y hace esta solicitud.
   Para el sistema de Encuentro Virtual de Empleabilidad, quién realiza esta acción es el jefe del Departamento de Bolsa Universitaria de Trabajo o el encargado del sistema.
   b) **¿Quién autoriza la creación de nuevos perfiles?** La jefa del Departamento de Bolsa Universitaria de Trabajo se pone en contacto con el jefe del Departamento de Informática, para indicar que necesita un nuevo perfil. Finalmente, esté se pone en contacto con DGTIC para la creación del nuevo perfil.
   Para el sistema de Encuentro Virtual de Empleabilidad, quién realiza esta acción es el jefe del Departamento de Bolsa Universitaria de Trabajo o el encargado del sistema.
5. **Acceso remoto al sistema de tratamiento de datos personales:**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —187 de 425—

a) **¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?** No.
b) **¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?** Si
c) **¿Cómo se evita el acceso remoto no autorizado?** Las credenciales de acceso solo se dan a personas que están adscritas a la DGOAE, se firma una carta de confidencialidad.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

DGOAE

1. **Señalar si realiza respaldos**
   d) **Completos** X**, diferenciales o incrementales;**
   e) **De forma automática o manual** X**,**
   f) **Periodicidad con que los realiza:** Cada día desde que comienza el registro hasta el último día del evento.
2. **El tipo de medios que utiliza para almacenar las copias de seguridad:**
   Los respaldos se realizan mediante el software de administración de base de datos, el cual genera un archivo con toda la información de las tablas que guardan la información de este sistema. Como el espacio que nos brinda DGTIC no es muy grande, los archivos se copian a una máquina que se encuentra en la DGOAE y en un disco duro.
3. **Cómo y dónde se archiva esos medios:** La computadora se encuentra en la DGOAE.
4. **Quién es el responsable de realizar estas operaciones:** El encargado del sistema.

DGTIC realiza sus propios respaldos.

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.
   - Tener respaldos de la base de datos y del código.
   - Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 188 de 425—

- Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
- El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
- Una ves que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
- Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una ves hecha la conexión se carga el respaldo de la base de datos.
- En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
- Realizar pruebas al sistema de inicio de sesión, cierre de sesión, registro de universitarias y universitarios, consulta del programa del Encuentro Virtual de Empleabilidad, inscripción y baja a las diferentes actividades que ofrece éste.

2. Este plan fue implementado por primera vez en el 2020, ya que el sitio se tuvo que migrar a un espacio donde DGTIC pudiera ponerle más recursos dependiendo de la demanda, esto ocurrió porque los días del evento el sitio tardaba mucho en responder las peticiones.
   El tiempo que se demoro DGTIC en darnos el nuevo espacio fue de un día, ya que se le explico que era de carácter urgente.
3. No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 189 de 425—

Dirección de Planeación.		
Identificador único*:	DGOAE-BUT-2020-2	
Nombre del sistema*:	Encuentro Virtual de Empleabilidad	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit	Extensión del navegador que esta diseñada para probar vulnerabilidades en el sistema.	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular.
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicarán el tráfico que existen en el servidor.	Se hace manual y solamente será usada cuando se genere un ataque al sistema.
Bitácoras generadas por el servidor	Éstas nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas por la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-2	
Nombre del sistema*:	Encuentro Virtual de Empleabilidad	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizaciones.	Revisión de páginas oficiales sobre las actualizaciones del lenguaje de programación.	Encargado del sistema.
Prueba de seguridad por parte de DGTIC	Se realiza una solicitud a DGTIC para que realice pruebas de seguridad y	DGTIC.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —190 de 425—

	encuentre vulnerabilidades, DGTIC envía un documento con las vulnerabilidades que encontró para que éstas sean corregigas.	
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones.	Encargado del sistema.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	DGOAE-BUT-2020-2	
Nombre del sistema*	Encuentro Virtual de Empleabilidad	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad.	No se encontraron fallas.	Encargado del sistema.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	DGOAE-BUT-2020-2	
Nombre del sistema*	Encuentro Virtual de Empleabilidad	
Medida de seguridad*	**Acciones***	**Responsable***
Pruebas de vulnerabilidad	a) Se corrigieron las partes del código que son vulnerables b) Seguir en constante actualización.	Encargado del sistema

8. Programa específico de capacitación

8.1 Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.			
Identificador único*	DGOAE-BUT-2020-2		
Nombre del sistema*	Encuentro Virtual de Empleabilidad		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —191 de 425—

Cursos	Cursos sobre programación en PHP, MySQL, Linux, seguridad informática, creación de certificados SSL, protección a las máquinas virtuales, hacker ético, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.

8.2 Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-2		
Nombre del sistema*	Encuentro Virtual de Empleabilidad		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cartas de confidencialidad	Se le hace llegar y firmar una carta de confidencialidad al personal que va a tener acceso al sistema.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Para todo el personal de la BUT, su objetivo es que estén enteradas(os) de que trabajaran con datos del alumnado, egresadas y egresados de la UNAM. Una vez firmada la carta comienza la vigencia y esta se actualiza dependiendo las circunstancias por las que esté pasando la UNAM.
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los	La distribución podrá ser mediante	Permanente.	Usuario titular de los datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 192 de 425—

datos personales de los titulares están resguardados en el sistema.	las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.		Cada vez que se haga algún cambio para la protección de los datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —193 de 425—

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-2		
Nombre del sistema*	Encuentro Virtual de Empleabilidad		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de mensajes de error, éxito y de información	Actualizar los mensajes del sistema para que no muestre contenido de la base de datos o de la configuración del servidor.	Permanente.	Total.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-2		
Nombre del sistema*	Encuentro Virtual de Empleabilidad		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo, lenguaje de programación y de la base de datos.	Es importante tener las versiones más actualizadas para evitar que nuestro equipo o software quedé obsoleto y sin soporte.	Depender de la adquisición del nuevo equipo e instalación del software.	Parcial.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-2	
Nombre del sistema*	Encuentro Virtual de Empleabilidad	
Proceso*	**Descripción***	**Responsable***
Los respaldos se realizan cada semana durante el evento.	Realizar respaldos de la base de datos, se genera un archivo con toda la información de las tablas que guardan la información de este sistema. Como el espacio que nos brinda DGTIC no es muy grande, los archivos se copian a una máquina que se encuentra en la DGOAE y en un disco duro.	Encargado del sistema.

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-2	
Nombre del sistema*	Encuentro Virtual de Empleabilidad	
Proceso*	**Descripción***	**Responsable***
Borrado	Las y los universitarios pueden borrar su inscripción a alguna de las conferencias	Universitarias y universitarios.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 194 de 425—

	si ellos así lo desean. Es lo único que pueden borrar.	
Limpieza de la base de datos.	Como cada año se realiza el Encuentro Virtual de Empleabilidad, al termino del evento, se limpia la base, es decir, los datos de las y los universitarios que se registraron al evento se insertan en una tabla histórica al igual que las inscripciones, esto con el motivo de obtener estadísticas por año.	Encargado del sistema.
Proceso de borrado de respaldos en soporte electrónicos	La información se borra de estos dispositivos solamente deberá guardar información del sistema. Formatear mediante borrado de bajo nivel.	Encargado del sistema o bien se le pide apoyo a la Dirección de Apoyo Técnico.

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO

Departamento de Bolsa Universitaria de Trabajo acordará la cancelación del sistema mediante un escrito donde indique lo siguiente:

a) Fecha de cuando deja de dar servicio el sistema.
b) Fecha de cancelación del sistema.
c) Motivo de la cancelación.
d) Si existe un sistema que lo reemplaza, poner la información del nuevo.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso y registro al sistema.
4. Solamente el administrador del sistema podrá ingresar.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 195 de 425—

7. Bajar del servidor el sistema para que no pueda ser visto por red.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Se realizará un último respaldo de la base de datos que el sistema utiliza para almacenar la información, está se guardará por si en un futuro se requiere realizar algún tipo de consulta, en un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por la BUT para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Una vez que hayan pasado las fechas establecidas para el bloqueo, se realizara lo siguiente:

1. Se retira del servidor el sistema Encuentro Virtual de Empleabilidad.
2. Respaldo del código del sistema y de la base de datos.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA Y TRATAMIENTO DE DATOS PERSONALES.

Una vez que se tenga el respaldo de la base de datos, solo se eliminará el sistema (código) del servidor de manera física, la base de datos se dejará en el servidor si así se decide, en caso contrario se procederá a borrar la misma, en ambos casos se tendrán los respaldos correspondientes.

Sistema de Información Automatizada de Prácticas Profesionales

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	**DGOAE-BUT-2020-3**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 196 de 425—

Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales
Datos personales (sensibles o no) contenidos en el sistema*:	Datos que se solicitan para el registro de una Instancia Receptora, coordinador y responsable del programa. • Instancia Responsable: RFC, nombre de la institución, razón social, sector al que pertenece la institución, giro y página web. • Coordinador y responsable del programa: Nombre, apellido paterno, apellido materno, cargo, profesión, entidad federativa, alcaldía/municipio, colonia/localidad, calle, número exterior, número interior, código postal, teléfono, extensión, teléfono celular, correo electrónico y responsable de la evaluación. Datos que se solicitan para el registro de un administrador del sistema y para un enlace de entidad académica. • Administrador del sistema: nombre, apellido paterno, apellido materno, cargo, teléfono y correo electrónico. Enlace de entidad académica: nombre, apellido paterno, apellido materno, cargo, teléfono, correo electrónico, sistema, entidad académica y carrera(s).
Responsable*:	
Nombre*:	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	- Cumplir con las normas de trabajo. - Ejecutar el trabajo en forma y tiempo.
	Encargados:
Nombre del Encargado 1*	Mtro. Víctor Arturo Morales Díaz
Cargo*:	Académico
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —197 de 425—

	inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Guardar y proteger los datos de los usuarios registrados en el sistema.
Nombre del Encargado 2*	Ing. Brian Alfonso Sánchez Vázquez
Cargo*:	Técnico Académico
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Guardar y proteger los datos de los usuarios registrados en el sistema.
Nombre del Encargado 3*	Ing. Mayra Erika Flores Pacheco
Cargo*:	Técnico Académico
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Guardar y proteger los datos de los usuarios registrados en el sistema.
	Usuarios
Nombre del Usuario 1*	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 2*	Elizabeth Navarrete Morales
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —198 de 425—

Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 3*	Lic. Paola Gabriela Sosa Flores
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 4*	Lic. Miriam Jimenez Ponce
Cargo*:	Profesionista Titulado
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 5*	Lic. Ruth Méndez Hernández
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 6*	Mtra. Susana Chávez Jaramillo
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —199 de 425—

Nombre del Usuario 7*	Lic. Laura Patricia Montoya Jiménez
Cargo*:	Directora de Planeación
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 8*	Lic. Claudia Navarrete García
Cargo*:	Directora de Servicio Social
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 9*	Lic. Lorenzo Rossi Hernandez
Cargo*:	Jefe del Departamento de modelos educativos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 10*	Biól. Alejandra Hernández Valdivia
Cargo*:	Jefa del Departamento de Registro y Seguimiento
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 11*	Lic. Griselda G. Gutiérrez Monsalvo
Cargo*:	Jefa del Departamento de Programas Multidisciplinarios de Servicio Social

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —200 de 425—

Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 12*	Lic. Celeste Cruz Avilés
Cargo*:	Jefa del Departamento de voluntariado
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Administrar: Usuarios DGOAE, usuarios de enlace, usuarios de instancia receptora, programas de prácticas profesional y practicantes.
Nombre del Usuario 13*	Dr. Germán Alvarez Díaz de León
Cargo*:	Director General
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Generar y firmar las cartas de término de práctica profesional.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	DGOAE-BUT-2020-3
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos relacional en MariaDB
Características del lugar donde se resguardan los soportes*:	El centro de datos de la CUAIEED cuenta con seis niveles de seguridad Nivel 1: SEGURIDAD DE ACCESO FÍSICO: • El personal registra fecha y hora de entrada/salida.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —201 de 425—

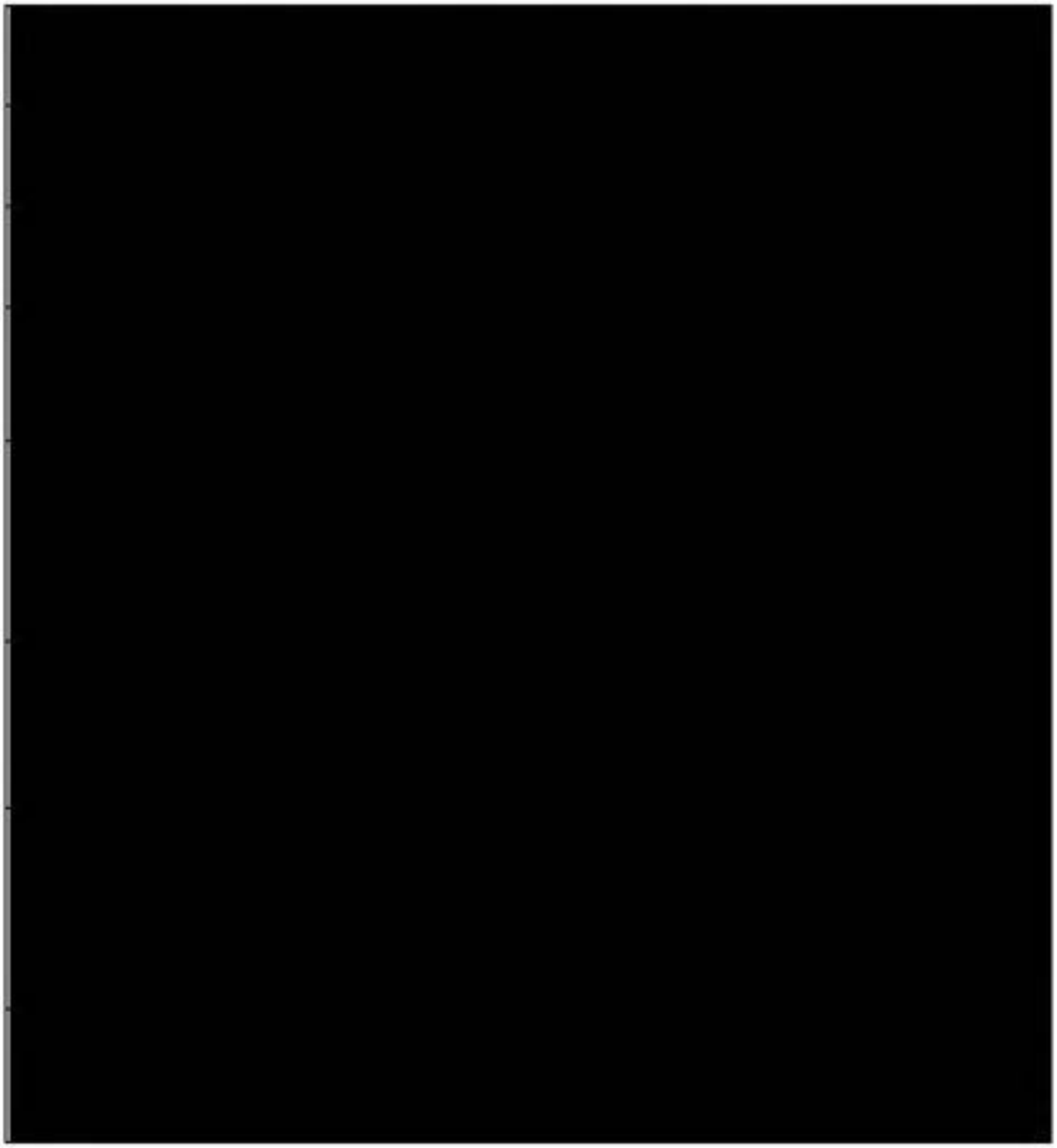
	• Se tiene personal de vigilancia que da el acceso a la dependencia. • El acceso con automóvil es con tarjeta autorizada y entregada por la Secretaría Administrativa. Nivel 2: SEGURIDAD EN LA INFRAESTRUCTURA DEL HARDWARE • Los servidores se encuentran en un área restringida con un espacio de 19.2 m2. • Cuenta con aire acondicionado manteniendo una temperatura de 17 ° Con humedad relativa de 40%. • Sistema de respaldo de energía eléctrica ininterrumpida (UPS). Tiempo de respaldo aproximado de 30 min. (ingreso de planta de energía). • Cámaras de vigilancia. • Sistema automático contra incendios. • Control de acceso al site (sistema por medio de huella digital y/o claves). • Planta de energía eléctrica. Nivel 3: SEGURIDAD EN LA INFRAESTRUCTURA DEL SOFTWARE: • Sistema de monitoreo a nivel software. • Restricción en los puertos de entrada/salida. • Configuración de Firewall. Nivel 4: SEGURIDAD DEL SISTEMA OPERATIVO • Autenticación al sistema a través de llaves privada utilizando Secure Shell. • Restricción de acceso por medio de contraseñas y roles. • Actualizaciones de seguridad continuas al sistema. Nivel 5: SEGURIDAD EN LA APLICACIÓN: • Certificado de seguridad SSL. • Control de acceso a usuarios dependiendo el rol asignado. • Restricción de acceso con usuario y contraseña. • Respaldo de la aplicación. Nivel 6: SEGURIDAD EN LA BASE DE DATOS: • Acceso restringido con usuario y contraseña. • Acceso restringido solo conexión local. • Permisos de restricción en los usuarios. • Respaldo de la base de datos.

3. Análisis de riesgos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 202 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-3	
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 203 de 425—



4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*:	DGOAE-BUT-2020-3
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 204 de 425—

Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único*:	DGOAE-BUT-2020-3
Nombre del sistema*:	Encuentro Virtual de Empleabilidad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —205 de 425—

Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

6. Medidas de seguridad implementadas

I. TRANSFERENCIA DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único*	DGOAE-BUT-2020-3
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales
TRANSFERENCIAS DE DATOS PERSONALES	

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 206 de 425—

Transferencias mediante el traslado de soportes físicos	No aplica.
Transferencias mediante el traslado de soportes electrónicos	No aplica.
Transferencias mediante el traslado sobre redes electrónicas:	No aplica. En caso que se envíen documentos, éstos deberán tener contraseña para poder abrirlo.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1) No se cuentan con soportes físicos
2) No se cuentan con soportes físicos

III. BITÁCORA PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras**

   a) **Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida**

   Las bitácoras con las que se cuentan son las de apache, MySQL y la del framework laravel. En la base de datos se registra fecha y hora en la que se realiza el acceso.
   El personal de la BUT (administradores) accede a consultar los siguientes datos:

   - Alumnado de la UNAM que se registraron a una práctica profesional.
   - Instancias receptoras, su coordinador, responsables y de los programas.
   - Enlaces de las entidades académicas.

   Los enlaces de entidades académicas acceden a consultar los siguientes datos:

   - Alumnado de la UNAM que se registraron a una práctica profesional.
   - Instancias receptoras, su coordinador, responsables y de los programas.

   Los coordinadores y/o responsables de una instancia receptora acceden consultar los siguientes datos:

   - Programas que registraron.

   b) **Para soportes físicos: Número o clave del expediente utilizado**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —207 de 425—

No se cuenta con expedientes físicos.

c) **Para soporte electrónico: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos**

Con los datos del alumnado de la UNAM que se registró a una práctica profesional, de las instancias receptoras y de los programas, se realizan reportes y estadísticas. A las instancias receptoras se les aplica una encuesta con los datos de esta se generan estadísticas.

2. **Si las bitácoras están en soporte físico o en soporte electrónico**

Soporte electrónico

3. **Lugar dónde almacenan las bitácoras y por cuánto tiempo**

En el servidor dónde se encuentra el sistema, el cual se encuentra en la CUAIIED.

4. **La manera en que asegura la integridad de las bitácoras**
   - Acceso restringido por usuario, contraseña y dirección IP.
   - Respaldo de la base de datos.
5. **Respecto del análisis de las bitácoras**

a) **Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza**

Encargado del sistema, cada que se presenta algún incidente o reporte por parte de los usuarios.

b) **Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.**

Se utilizan editores de texto, vi, Notepad++, vscode, block de notas.

IV. REGISTRO DE INCIDENTES

1. **Los datos que registra:**

a) **La persona que resolvió el incidente.** Nombre del encargado o de la persona que resolvió el incidente.

b) **La metodología aplicada.** Se registra la incidencia, los daños y acciones para prevenir otra.

c) **Para soportes físicos.** No se cuenta con soportes físicos.

d) **Para soportes electrónicos.** El respaldo que se hace de la base de datos incluye: tablas, campos y registros de cada una de ellas.

2. **Si el registro está en soporte físico o en soporte electrónico.** El soporte se encuentra en electrónico.
3. **Cómo asegura la integridad de dicho registro.** Reglas de validación, realizando transacciones y por medio de los respaldos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —208 de 425—

4. **Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.** El encargado y/o el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior**

   La CUAIEED se encuentre limitada con reja en toda el área perimetral. Existen dos accesos vehiculares y un acceso peatonal todos restringidos. En la puerta principal se cuenta con personal de vigilancia que autoriza el acceso. Además de contar con CCTV

2. **Seguridad perimetral interior**

   Contamos con un centro de datos ubicado en el edificio B planta baja. Se tienen cámaras de vigilancia fuera y dentro del centro de datos. El acceso se realiza a través de un sistema de control de acceso a base de huella digital o por medio de contraseña.

Para las personas que acceden a dichos espacios interiores:

1. **¿Cómo las identifica?**

   Para el acceso a la Dependencia es requisito indispensable contar con una identificación oficial y nombre de la persona que visitará, así como el motivo. Es necesario registrarse en un libro de bitácoras de entrada y salida para su acceso.

2. **¿Cómo las autentifica?**

   Por medio de su identificación oficial. Cabe señalar que, si la visita desea entrar con vehículo, el área que recibirá la visita debe generar un oficio con los datos del automóvil y de la persona o personas que ingresarán, el cual se debe entregar a la Secretaría Administrativa máximo un día antes del ingreso.

3. **¿Cómo les autoriza el acceso?**

   Si es horario laborable con su identificación y nombre de quien visita se le da el acceso, cuando son horarios de comida los vigilantes verifican que se encuentre la persona a quien hacen la visita.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para este sistema el personal de la BUT (administradores) son los únicos que pueden actualizar datos personales de los enlaces de entidades académicas, de la instancia receptora, de sus coordinadores y responsables.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —209 de 425—

1. **Modelo de control de acceso**

   Este sistema se encuentra montado en el servidor de CUAIIED

   a) **¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?** Si.

   b) **¿Es discrecional (matriz de control de acceso)?** Para el acceso al servidor de CUAIEED, es a través de una llave ssh, la cual se genero y fue enviada al personal de la CUAIEED para que la colocaran en su servidor y permitiera el acceso.

   c) **¿Está basado en roles (perfiles) o grupos?** Si

   d) **¿Está basado en reglas?** Si

2. **Perfiles de usuario y contraseñas en el sistema operativo de red:**

   g) **¿Cuenta con sistema operativo de red instalado en sus equipos?** Si, se cuenta con equipos con sistema operativo Windows, algunos tienen Linux y dónde está montado el sistema es un Linux.

   h) **¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?** Sí, los equipos que se encuentran en la DGOAE cuentan con este manejo, así como el equipo de la CUAIEED, dónde se encuentra el sistema.

   i) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.

3. **Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:**

   a) **¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?** Si.

   b) **¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?** Sí.

4. **Administración de perfiles de usuario y contraseñas:**

¿Quién da de alta nuevos perfiles? La CUAIEED.

   a) **¿Quién autoriza la creación de nuevos perfiles?** La jefa del Departamento de Bolsa Universitaria de Trabajo.

5. **Acceso remoto al sistema de tratamiento de datos personales:**

   a) **¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?** No.

   b) **¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?** Si

   c) **¿Cómo se evita el acceso remoto no autorizado?** La llave ssh es personal y no se comparte, se firma una carta de confidencialidad.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —210 de 425—

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Se realizan dos respaldos, uno por parte de CUAIEED y otro por parte de la Bolsa Universitaria de Trabajo de la DGOAE.

CUAIEED

1. **Señalar si realiza respaldos**
   a) **Completos** X, **diferenciales_ o incrementales_;**
   b) **De forma automática** X **o manual _.** A través de un script y un cron.
   c) **Periodicidad con que los realiza:** Todos los miércoles y domingos a las 12:00 am
2. **El tipo de medios que utiliza para almacenar las copias de seguridad:** Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.
3. **Cómo y dónde se archiva esos medios:** El servidor de respaldos se encuentra en el centro de datos, posteriormente se respalda en cintas magnéticas identificadas y etiquetadas. Se resguardan en la oficina del departamento de Seguridad y Operación de Servidores.
4. **Quién es el responsable de realizar estas operaciones:** El jefe de departamento Mtro. Enrique Pérez Campos) y jefe de área (Lic. Alan López de Jesús) ambos del Departamento de Seguridad y Operación de Servidores.

Bolsa Universitaria de Trabajo de la DGOAE

1. **Señalar si realiza respaldos**
   a) **Completos** X, **diferenciales o incrementales.**
   b) **De forma automática o manual** X.
   c) **Periodicidad con los que los realiza:** Cada semana.
2. **El tipo de medios que utiliza para almacenar las copias de seguridad:** Se realizan por medio del comando mysqldump, él cual genera un archivo .sql, éste se guarda en la computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro.
3. **Cómo y dónde se archiva esos medios:** La computadora se encuentra en la DGOAE y en un disco duro.
4. **Quién es el responsable de realizar estas operaciones:** El encargado del sistema.

IX. PLAN DE CONTINGENCIA

CUAIEED cuenta con su propio plan de contingencia.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —211 de 425—

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-3	
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit	Extensión del navegador que esta diseñada para probar vulnerabilidades en el sistema.	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular.
Bitácoras generadas por CUAIEED	Las bitácoras generadas por CUAIEED nos indicarán el tráfico que existen en el servidor.	Se tendrán que pedir las bitácoras a CUAIEED.
Bitácoras generadas por el servidor	Éstas nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas por la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.

7.2. Procedimiento para la revisión de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —212 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*:	DGOAE-BUT-2020-3	
Nombre del sistema*:	Sistema de Información Automatizada de Prácticas Profesionales	
Medida de seguridad*	**Procedimiento***	**Responsable***
Actualizaciones.	Revisión de páginas oficiales sobre las actualizaciones del lenguaje de programación.	Encargado del sistema.
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones.	Encargado del sistema.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-3	
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Pruebas de vulnerabilidad.	No se encontraron fallas.	Encargado del sistema y CUAIEED.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 213 de 425—

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-3	
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales	
Medida de seguridad*	**Acciones***	**Responsable***
Pruebas de vulnerabilidad	a) Se corrigieron las partes del código que son vulnerables b) Seguir en constante actualización.	Encargado del sistema y CUAIEED.

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-3		
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos	Cursos sobre programación en PHP, MySQL, Linux, seguridad informática, creación de certificados SSL, protección a las máquinas virtuales, hacker ético, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	La duración depende del curso.	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 214 de 425—

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-3		
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cartas de confidencialidad	Se le hace llegar y firmar una carta de confidencialidad al personal que va a tener acceso al sistema.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Para todo el personal de la BUT, su objetivo es que estén enteradas(os) de que trabajaran con datos del alumnado, egresadas y egresados de la UNAM. Una vez firmada la carta comienza la vigencia y esta se actualiza dependiendo las circunstancias por las que esté pasando la UNAM.
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	La distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Permanente.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —215 de 425—

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-3		
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de mensajes de error, éxito y de información	Actualizar los mensajes del sistema para que no muestre contenido de la base de datos o de la configuración del servidor.	Permanente	Total.

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**			
Identificador único*	DGOAE-BUT-2020-3		
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo, lenguaje de programación y de la base de datos.	Es importante tener las versiones más actualizadas para evitar que nuestro equipo o software quedé obsoleto y sin soporte.	Depender de la adquisición del nuevo equipo e instalación del software.	Parcial.

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-3	
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales	
Proceso*	**Descripción***	**Responsable***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 216 de 425—

Generación de respaldos	Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.	Responsable en CUAIIED
Generación de respaldos	Se realizan en un archivo .sql, el cual se genera en la computadora que se encuentra en las instalaciones de la DGOAE y en un disco duro.	Encargado del sistema en DGOAE

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	DGOAE-BUT-2020-3	
Nombre del sistema*	Sistema de Información Automatizada de Prácticas Profesionales	
Proceso*	**Descripción***	**Responsable***
Borrado	Las y los universitarios pueden borrar su inscripción a alguna de las conferencias si ellos así lo desean. Es lo único que pueden borrar.	Universitarias y universitarios.
Limpieza de la base de datos.	Como cada año se realiza el Encuentro Virtual de Empleabilidad, al termino del evento, se limpia la base, es decir, los datos de las y los universitarios que se registraron al evento se insertan en una tabla histórica al igual que las inscripciones, esto con el motivo de obtener estadísticas por año.	Encargado del sistema.
Proceso de borrado de respaldos en soporte electrónicos	La información se borra de estos dispositivos solamente deberá guardar información del sistema. Formatear mediante borrado de bajo nivel.	Encargado del sistema o bien se le pide apoyo a la Dirección de Apoyo Técnico.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 217 de 425—

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO

Departamento de Bolsa Universitaria de Trabajo acordará la cancelación del sistema mediante un escrito donde indique lo siguiente:

a) Fecha de cuando deja de dar servicio el sistema.
b) Fecha de cancelación del sistema.
c) Motivo de la cancelación.
d) Si existe un sistema que lo reemplaza, poner la información del nuevo.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en CUAIEED que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso y registro al sistema.
4. Solamente el administrador del sistema podrá ingresar.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Se realizará un último respaldo de la base de datos que el sistema utiliza para almacenar la información, está se guardará por si en un futuro se requiere realizar algún tipo de consulta, en un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu8s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —218 de 425—

- El tiempo será definido por la BUT para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES.

Una vez que hayan pasado los días establecidos del bloqueo, se realizara lo siguiente:

1. Se retira del servidor el sistema SIAPP.
2. Respaldo del código del sistema y de la base de datos.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA Y TRATAMIENTO DE DATOS PERSONALES.

Una vez que se tenga el respaldo de la base de datos, solo se eliminará el sistema (código) del servidor de manera física, la base de datos se dejará en el servidor si así se decide, en caso contrario se procederá a borrar la misma, en ambos casos se tendrán los respaldos correspondientes.

Estrategias de vinculación e inserción laboral

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador únic	**502 62 06**
(Nombre del siste A1) *	**Estrategias de vinculación e inserción laboral**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —219 de 425—

Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales que se le solicitan a las y los universitarios son: Fecha de nacimiento, sexo, teléfono de casa, teléfono celular y correo electrónico. Datos académicos que se le solicitan a las y los universitarios son: Número de cuenta, máximo nivel de estudios en la UNAM, situación académica, semestre (en caso de ser estudiante), año de egreso (en caso de haber concluido sus estudios a cualquier nivel), Escuela/Facultad/Instituto/Centro, carrera/programa dónde realizo sus estudios, promedio, nivel de inglés, idioma y el nivel del idioma. El nombre de las y los universitarios se obtiene de un web service que nos provee DGAE.
Responsable*:	
Nombre*:	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de a Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE
Obligaciones*:	• Cumplir con las normas de trabajo. • Ejecutar el trabajo en forma y tiempo
	Encargados:
(Nombre del Encargado 1*)	Ing. Pedro Benitez Mejía
Cargo*:	Jefe del Departamento de Informática
Funciones*:	Estandarización de Datos y Coordinación de Proyecto
Obligaciones*:	Realizar el piloteo y aseguramiento de implementación de medidas de seguridad. Supervisión de datos generados por Google Analytics. Implementar medidas necesarias para evitar posibles ataques DDoS o cualquier ataque que pueda representar un problema en la continuidad del servicio. Considerar la limpieza de información previa a la inserción de datos en la Base de Datos con los lineamientos necesarios para evitar posibles inyecciones de SQL. Forzar el peso y formato de los documentos proporcionados a las necesidades del servidor utilizado. Encriptar documentos proporcionados, tanto en nombre de archivo como en integridad física del mismo. Agregar controles básicos para evitar ataques de bots (captcha). Implementar herramienta de Google Analitycs en los puntos vulnerables del sistema.

Usuarios

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 220 de 425—

Nombre del Usuario 1*	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 2*	Elizabeth Navarrete Morales
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 3*	Lic. Paola Gabriela Sosa Flores
Cargo*:	Asistente de procesos
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 4*	Lic. Miriam Jimenez Ponce
Cargo*:	Profesionista Titulado
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 5*	Lic. Ruth Méndez Hernández
Cargo*:	Técnica académica

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —221 de 425—

Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.
Nombre del Usuario 6*	Mtra. Susana Chávez Jaramillo
Cargo*:	Técnica académica
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE.
Obligaciones*:	Consultar a las y los universitarios que se inscribieron a las diferentes actividades y quitar las actividades que ya se hayan impartido o bien ya no haya cupo.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —222 de 425—

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único*"	502_62_06
(Nombre del sistema A1*)	Estrategias de vinculación e inserción laboral
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos. Se tienen 1 sola de base de datos con el registro de la información del universitario y de la actividad que va a realizar.
Características del lugar donde se resguardan los soportes:*	bolsadetrabajo.unam.mx --- Acceso por consola: IP: 132.248.10.143 Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico: • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video.

	Nivel 2: Seguridad en la infraestructura del hardware: • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. ✓ Estudiantes requiere usuario y contraseña. ✓ Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la Base de Datos: • Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol • Respaldos de Base de Datos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —223 de 425—

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	502_62_06	
(Nombre del sistema A1) *	**Estrategias de vinculación e inserción laboral**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —224 de 425—



4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 06	
(Nombre del sistema A1) *	Estrategias de vinculación e inserción laboral	
Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]		

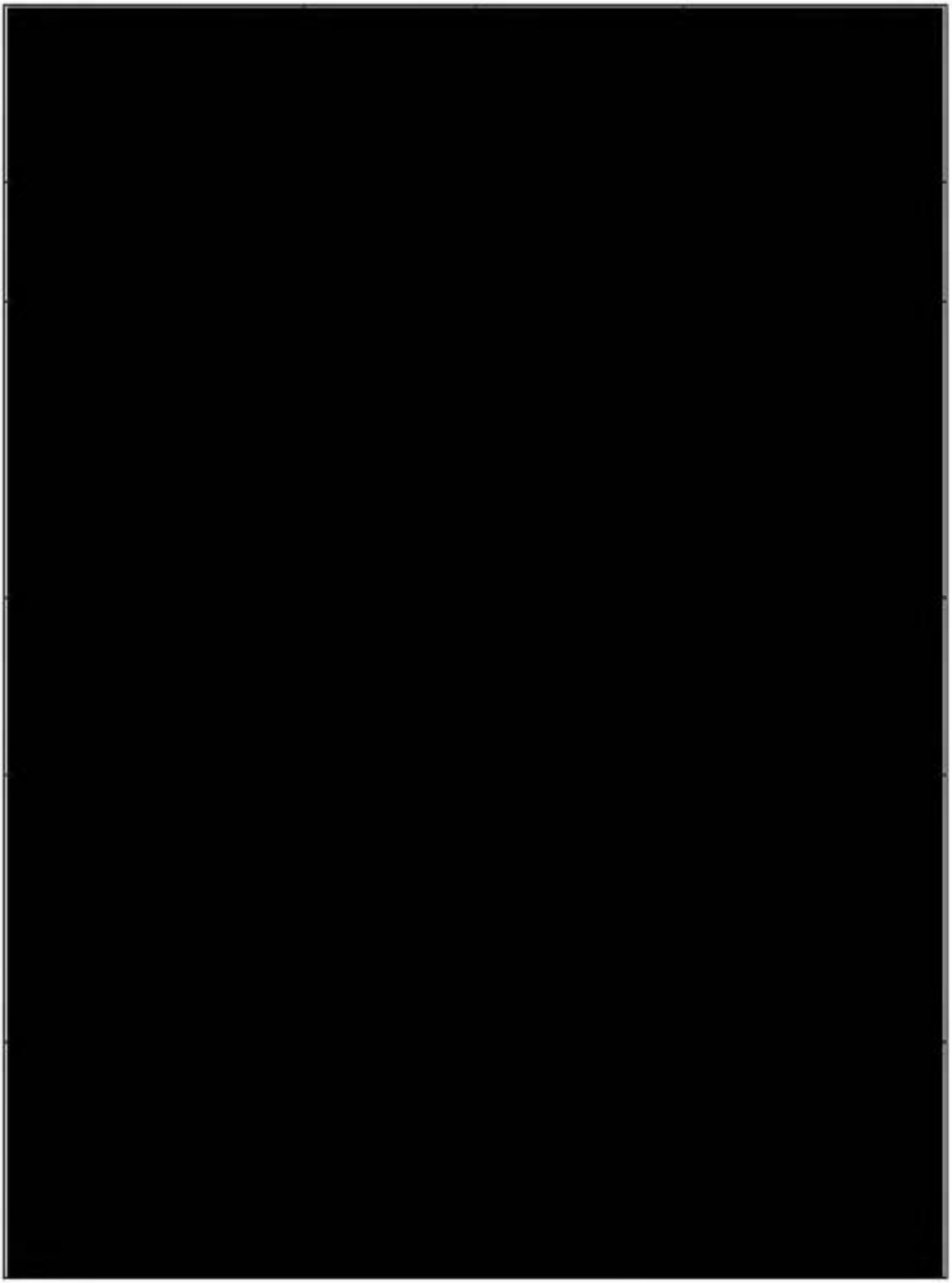
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 225 de 425—



5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.			
Identificador único*	502 62 06		
(Nombre del sistema A1) *	Estrategias de vinculación e inserción laboral		
Actividad*	Descripción*	Duración*	Cobertura*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 226 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —227 de 425—

[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —228 de 425—

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	502 62 06
(Nombre del sistema A1) *	**Estrategias de vinculación e inserción laboral**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NO APLICA
Transferencias mediante el traslado de soportes electrónicos:	a) La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos

	personales.
Transferencias mediante el traslado sobre redes electrónicas:	La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales. El acceso al sistema se realiza por medio de un usuario previamente registrado y con sesión activa.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
   - Se cuentan con contraseñas robustas.
   - Debe de darse de alta una dirección IP específica dentro de la red UNAM.
   - Existe un puerto en el servidor dedicado a la transferencia de información.
   - Es asignado un espacio específico para la carga de proyectos.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
   - Nombre: Mtro. Pedro Benítez Mejía
     Cargo: Jefe de Departamento de Informática
     Funciones: Coordinación y Aprobación de Requisitos del Sistema. Diseño, desarrollo y programación de Sistema. Diseño, modelado e implementación de Base de Datos del Sistema.
     Obligaciones: Garantizar el mejor manejo de los datos personales de los usuarios involucrados.
     Garantizar que se cumplan con las necesidades estructurales y funcionales del sistema y el trato de los datos personales

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 229 de 425—

c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
Se lleva una bitácora de soporte técnico asociado a una base que se registra en red.

- Nombre de usuario
- Cargo
- Fecha de entrada
- Hora de entrada
- Fecha de salida
- Hora de salida
- Datos modificados

2. Si las bitácoras están en soporte físico o en soporte electrónico;
Soporte electrónico y físico (por semestre).
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
Semestral, asociado al equipo de trabajo generado en comunidad UNAM.
4. La manera en que asegura la integridad de las bitácoras, y
Se imprime Semestralmente.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
      Nombre: Mtro. Pedro Benítez Mejía
      Cargo: Jefe de Departamento de Informática
      Periodicidad: Semestralmente
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   Bitácora en red, autogestionada.

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 230 de 425—

1. Los datos que registra:
   a. La persona que resolvió el incidente;
      Nombre, cargo, incidente, acción, descripción breve, fecha del incidente, sistema afectado, URL del sistema.
   b. La metodología aplicada;
      Se recopila la información con la información del registro donde se debe incluir la fecha del incidente, cual fue el incidente, una descripción breve de la solución ejecutada, los datos afectados, datos recuperados, de ser el caso el Sistema afectado y su dirección URL.
   c. Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
      Carpeta con bitácora de incidentes por semestre
   d. Para soportes electrónicos:
      Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
   ambos
3. Cómo asegura la integridad de dicho registro, y
   En la oficina del Director de Apoyo Técnico, y una copia en la oficina del Jefe de Departamento de Informática.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
   Jefe de Departamento de Informática

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):
   ¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.
   La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales así como los días de asueto.
   Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDSzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —231 de 425—

Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:
a) ¿Cómo las identifica?
Es necesario presentar una credencial oficial vigente, bien sea de la Dirección General de Orientación y Atención Educativa, o de alguna entidad autorizada de la UNAM. Y en caso de no contar con ella, un previo registro en el acceso con alguna credencial de identificación con fotografía que será resguardada por el personal de vigilancia, para ser devuelta con el registro de hora de salida.
b) ¿Cómo las autentifica?
Solamente debe proporcionarse el acceso a las instalaciones con alguna identificación oficial para los siguientes casos:

- Personal de la Dirección General de Orientación y Atención Educativa. En caso de ser trabajadores contratados, deben contar con la identificación que acredita la pertenencia a esta dependencia. En caso de no contar con una credencial oficial, contar con algún gafete o documento expedido por el área para la cual está prestando sus servicios.
- En caso de visita de personal externo a la Dirección General de Orientación y Atención Educativa, debe presentar alguno de los siguientes documentos:
    - Credencial UNAM, en caso de pertenecer a alguna dependencia, sea el caso de tratarse de un alumno o trabajador de la Universidad Nacional Autónoma de México.
    - Credencial INE, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
    - Pasaporte, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
    - Cartilla militar, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.

c) ¿Cómo les autoriza el acceso?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —232 de 425—

Para el caso del personal que labora en la dependencia, se realiza presentando la credencial o gafete que acredita labora en la Dirección General de Orientación y Atención Educativa.
Para el caso de personal ajeno a la dependencia, es necesario presentar los documentos oficiales declarados en el punto anterior y registrar sus datos tales como:

- Nombre completo, Institución a la que representa, hora de entrada, fecha de entrada, área a visitar, motivo de la visita, hora de salida, firma.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.
Se cuenta con doble cerradura, al interior de la Dirección:

- Cerradura Tubular
- Cerradura Empotrada

Por la parte externa se cuenta con dos cerraduras externas y otras dos cerraduras el interior

- 2 Cerraduras Empotradas
- Cerradura Multipunto
- Cerradura Tubular

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Una vez registrado en el acceso principal, debe contar con las llaves para ingresar al área de Servidores. Y sólo el personal autorizado cuenta con las llaves del espacio y acceso al área.
2. ¿Cómo las autentifica?
   Es necesario ser personal autorizado para acceder al área. Por tal motivo debe contar con las llaves del inmueble y la credencial que acredite su vigencia en la plantilla del Departamento de Informática.
3. ¿Cómo les autoriza el acceso?
   Es necesario forzosamente ser personal del Departamento de Informática adscrito a la Dirección General de Orientación y Atención Educativa y tener las credenciales que acrediten ello.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDSzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —233 de 425—

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.
Es necesario cada año renovar el Aviso de Privacidad, y los métodos de guardado y almacenado para los datos personales. A demás, de tratarse de una convocatoria anual, esta debe renovarse si así lo amerita en los aspectos de seguridad actuales.
Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
1. Modelo de control de acceso (alguno de los siguientes):
   a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
   Si, debe ser una IP perteneciente a la red UNAM y haber sido dada de alta al departamento encargado de administrar el servidor. Así mismo, contar con las credenciales y los parámetros de conexión.
   b) ¿Es discrecional (matriz de control de acceso)?
   No, pero debe asentarse en la bitácora de conexión el acceso para cada usuario autorizado.
   c) ¿Está basado en roles (perfiles) o grupos?
   Roles
   d) ¿Está basado en reglas?
   Si, son proporcionadas por el administrador del servicio.
2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   No, pero se cuenta con EGOSECURE que nos ayuda a monitorear la actividad de toda la red, y el uso de los equipos.
   b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
   No, cada equipo cuenta con una contraseña generada por el Departamento de Informática, con los lineamientos establecidos por DGTIC, y una cuenta administrador-creada exclusivamente al personal del autorizado.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —234 de 425—

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No, en dado caso de ser necesario, debe crearse un nuevo usuario y contraseña individualmente por cada equipo dentro de la red.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?

No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

Alguno de los integrantes del Departamento de Informática de la Dirección General de Orientación y Atención Educativa.

b) ¿Quién autoriza la creación de nuevos perfiles?

El Director de Apoyo Técnico y el Jefe del Departamento de Informática.

c) ¿Se lleva registro de la creación de nuevos perfiles?

Si, en una Bitácora de usuarios, pero sin el dato de contraseña, sólo datos generales.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

Si

c) ¿Cómo se evita el acceso remoto no autorizado?

Se cuentan con llaves privadas de conexión y configuración de firewall, para el acceso único de los equipos autorizados, dichos equipos se encuentran en servidores de la DGTIC.

En el caso de la DGTIC

1. Señalar si realiza respaldos
   a) Completos X, diferenciales_ o incrementales_;
      Se realizan respaldos completos
   b) De forma automática X o manual _,
      A través de un script y un cron
   c) Periodicidad con que los realiza:
      Todos los miércoles y domingos a las 12:00 am

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —235 de 425—

2. El tipo de medios que utiliza para almacenar las copias de seguridad:

   Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.
3. Cómo y dónde se archiva esos medios:

   El servidor de respaldos se encuentra en el centro de datos, posteriormente se respalda en cintas magnéticas identificadas y etiquetadas. Se resguardan en la oficina del departamento de Seguridad y Operación de Servidores.
4. Quién es el responsable de realizar estas operaciones:

   El jefe de departamento Mtro. Enrique Pérez Campos) y jefe de área (Lic. Alan López de Jesús) ambos del Departamento de Seguridad y Operación de Servidores.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   1. Completos_X_, diferenciales ___ o incrementales___;
   2. De forma automática ____ o Manual __X__,
   3. Periodicidad con que los realiza: _Semestral_
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Disco Duro, Nube de equipo de trabajo y USB si es posible.
3. Cómo y dónde archiva esos medios, y
   En las instalaciones del Departamento de Informática.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El Departamento de Informática

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Plan de Contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   Si se ha aplicado. No se han realizado pruebas de eficiencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —236 de 425—

No

b) Si el sitio es propio o subcontratado con un tercero;
No

c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
No

d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	502 62 06	
(Nombre del sistema A1) *	**Estrategias de vinculación e inserción laboral**	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit (PTK)	Se trata de una extensión del navegador que esta diseñada para probar la posible vulnerabilidad en el sistema	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular. Versión 6.1.5
Google Analytics	Te permite hacer un seguimiento de sitios web, blogs y redes sociales. Además, pone a tu disposición informes predeterminados y personalizables.	Podemos analizar el tráfico que esta generando nuestro sistema y que secciones están generando mayor impacto, así como diferentes estadísticas que van desde la recopilación del dispositivo de conexión, hasta el tiempo de conexión en nuestro sitio.
JMeter	Es una herramienta de carga para llevar a cabo simulaciones sobre	Inicialmente diseñada para pruebas de estrés en aplicaciones web, hoy en día, su arquitectura ha evolucionado no sólo para

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —237 de 425—

	cualquier recurso de Software.	llevar a cabo pruebas en componentes habilitados en Internet (HTTP), sino además en Bases de Datos, programas en Perl requisiciones FTP y prácticamente cualquier otro medio.

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 06	
(Nombre del sistema A1)*	**Estrategias de vinculación e inserción laboral**	
Medida de seguridad*	**Procedimiento***	**Responsable***
DDoS.	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Inyección SQL	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Jmeter	Pedro Benítez Mejía, 1 día.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 06	
(Nombre del sistema A1)*	**Estrategias de vinculación e inserción laboral**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
DDoS.	Cumple con los requisitos.	Pedro Benítez Mejía, 1 día.
Inyección SQL	Cumple con los requisitos	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Probado para 500 peticiones durante 1 hora, permanece estable.	Pedro Benítez Mejía, 1 día.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —238 de 425—

Dirección de Planeación.		
Identificador único*	502 62 06	
(Nombre del sistema A1) *	**Estrategias de vinculación e inserción laboral**	
Medida de seguridad*	**Acciones***	**Responsable***
Realizar pruebas de estrés en el sistema	Revisar cuantos usuarios pueden interactuar en el sistema.	Pedro Benítez Mejía, 2 días
Realizar pruebas de escalabilidad	Que mejoras pueden implementarse al sistema	Pedro Benítez Mejía, 1 semana
Realizar test de resistencia	Se realizan simulaciones de peticiones, relacionando la cantidad de peticiones con las localidades de posible impacto.	Pedro Benítez Mejía, 1 semana

8. Programa específico de capacitación
   - **8.1. Programa de capacitación a los responsables de seguridad de datos personales**
   - **8.2. Ass**
   - **8.3. Asd**
   - **8.4. addf**
9. Mejora continua
   - 9.1. A
   - 9.2. B
   - 9.3. C
   - 9.4. D
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —239 de 425—

Feria del empleo

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	502 62 05
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**
Datos personales (sensibles o no) contenidos en el sistema*:	• Número de cuenta • Fecha de nacimiento • Apellido paterno • Apellido materno • Nombre • Edad • Sexo • Teléfono de casa • Correo electrónico • Correo electrónico adicional • Escuela / facultad de procedencia • Carrera • Nivel máximo de estudios • Situación académica • Área (especialidad / posgrado) • Promedio • ¿Cuántos idiomas habla además del español? • Idioma • Conversación • Certificación • Vigente • Nombre de la certificación • Puntaje • ¿Eres o has sido becario? • De que programa • Lugar del programa • País / Estado • Sueldo deseado • ¿Trabajas actualmente? • ¿En qué sector trabajas?

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 240 de 425—

	• Sueldo • Horario • Tu trabajo tiene que ver con tu profesión • ¿Por qué medio conseguiste tu último empleo? • ¿Por qué no trabajas? • Fecha de tu último trabajo • Tienes alguna discapacidad • Tipo de discapacidad • Asistencia a la Feria • ¿Cómo te enteraste a la Feria? • Has asistido a otras ferias del Empleo UNAM • ¿Cuales? • Señala los talleres que has cursado para apoyar tu búsqueda de empleo • Has tenido asesoría para elaborar tu curriculum • ¿En dónde? • Has tenido asesoría para preparar tus entrevistas • ¿En dónde? • Selección de día y hora de asistencia a la feria
Responsable*:	
Nombre*:	Lic. Yazmin Barrales Zarza
Cargo*:	Jefa del Departamento de a Bolsa Universitaria de Trabajo
Funciones*:	Apoyar en las estrategias para vincular al alumnado, las y los egresados con empresas e instituciones, con la finalidad de favorecer el desarrollo profesional e inserción laboral, así como en las actividades de la DGOAE
Obligaciones*:	• Cumplir con las normas de trabajo. • Ejecutar el trabajo en forma y tiempo.
	Encargados:
(Nombre del Encargado 1*)	Ing. Pedro Benitez Mejía

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —241 de 425—

Cargo*:	Jefe del Departamento de Informática
Funciones*:	Estandarización de Datos y Coordinación de Proyecto
Obligaciones*:	Realizar el piloteo y aseguramiento de implementación de medidas de seguridad. Supervisión de datos generados por Google Analytics. Implementar medidas necesarias para evitar posibles ataques DDoS o cualquier ataque que pueda representar un problema en la continuidad del servicio. Considerar la limpieza de información previa a la inserción de datos en la Base de Datos con los lineamientos necesarios para evitar posibles inyecciones de SQL. Forzar el peso y formato de los documentos proporcionados a las necesidades del servidor utilizado. Encriptar documentos proporcionados, tanto en nombre de archivo como en integridad física del mismo. Agregar controles básicos para evitar ataques de bots (captcha). Implementar herramienta de Google Analityes en los puntos vulnerables del sistema.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.	
Identificador único* (Nombre del sistema A1*)	S02_62_05 Feria del Empleo UNAM. Registro CV
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos. Se tienen 2 bases de datos con diseño de entidad relación y llave primaria asociada al curriculum del universitario y a al día y hora de asistencia a la Feria
Características del lugar donde se resguardan los soportes:*	feriadelempleo.unam.mx --- Acceso por consola: IP: 132.248.10.149 Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico: • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución.

ID del Documento: gIPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 242 de 425—

	• Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware: • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. ✓ Estudiantes requiere usuario y contraseña. ✓ Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la Base de Datos: • Acceso restringido por usuario y dirección IP de acceso local.

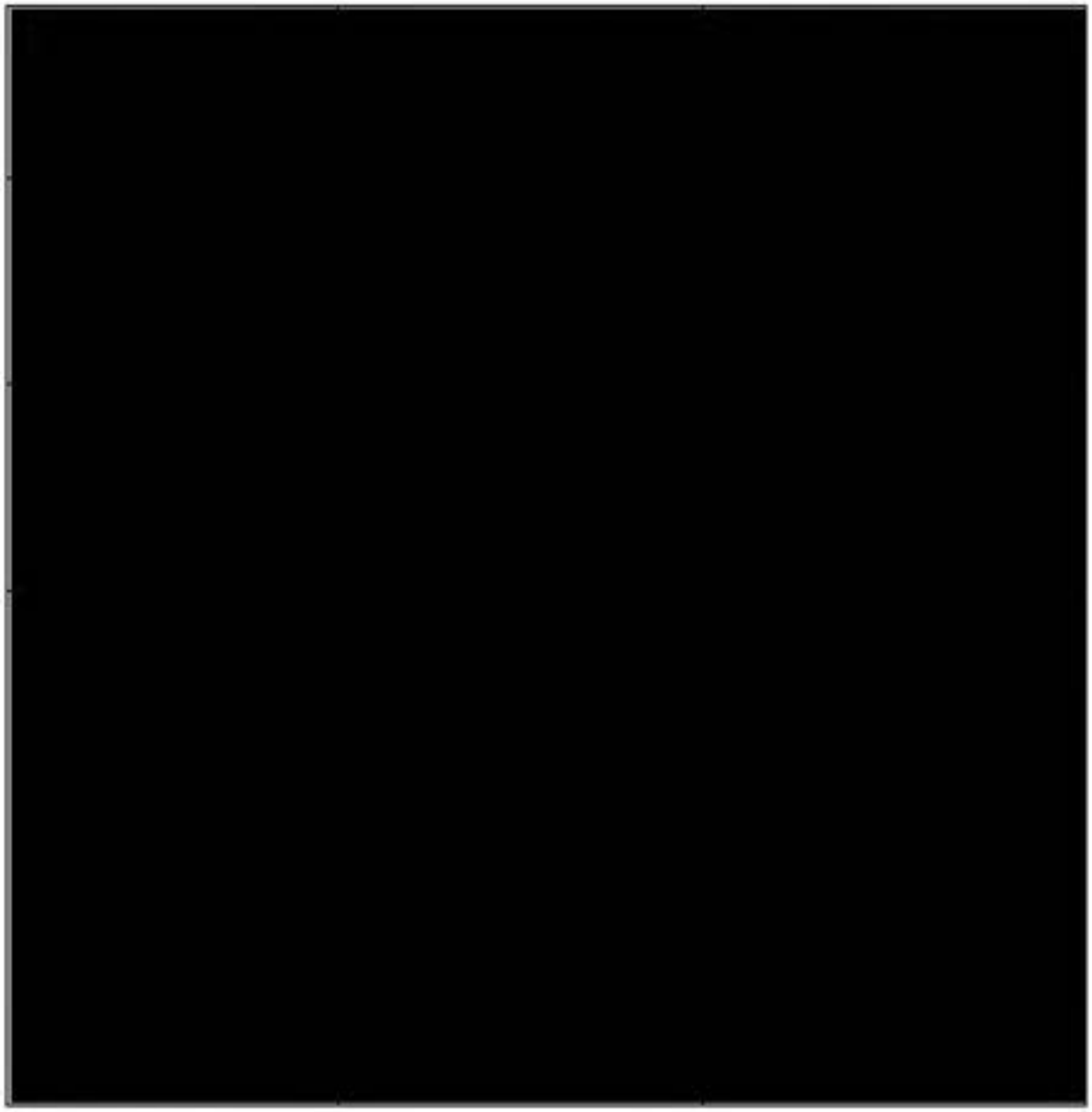
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 243 de 425—

	• Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol • Respaldos de Base de Datos

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 05	
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

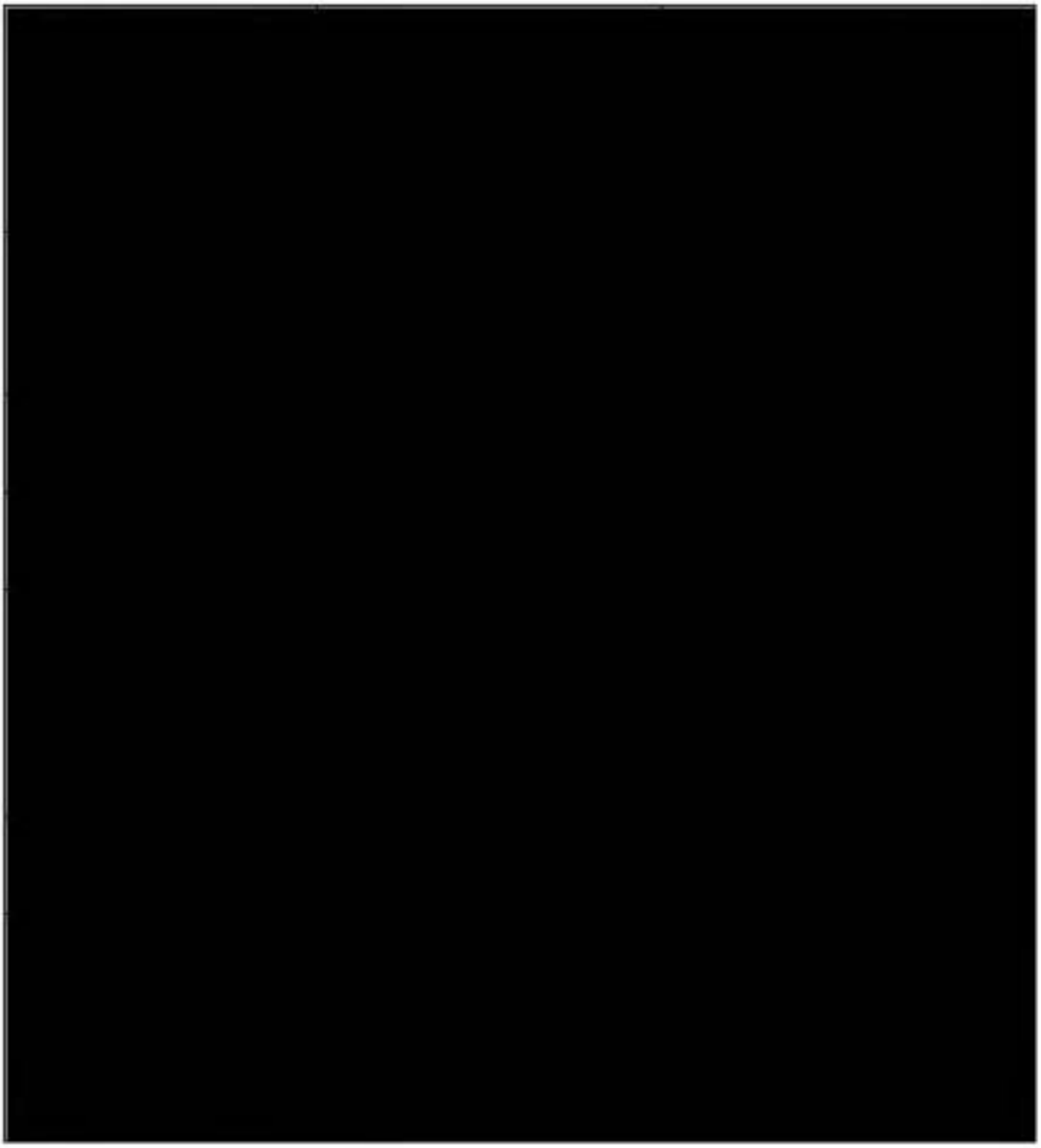
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 244 de 425—



4. Análisis de brecha

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 05	
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 245 de 425—



5. Plan de trabajo

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	502 62 05
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 246 de 425—

Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 247 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 248 de 425—

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	502 62 05
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NO APLICA
Transferencias mediante el traslado de soportes electrónicos:	a) La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos

	personales.
Transferencias mediante el traslado sobre redes electrónicas:	La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales. El acceso al sistema se realiza por medio de un usuario previamente registrado y con sesión activa.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
   - Se cuentan con contraseñas robustas.
   - Debe de darse de alta una dirección IP específica dentro de la red UNAM.
   - Existe un puerto en el servidor dedicado a la transferencia de información.
   - Es asignado un espacio específico para la carga de proyectos.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
   - Nombre: Mtro. Pedro Benítez Mejía
     Cargo: Jefe de Departamento de Informática
     Funciones: Coordinación y Aprobación de Requisitos del Sistema. Diseño, desarrollo y programación de Sistema. Diseño, modelado e implementación de Base de Datos del Sistema.
     Obligaciones: Garantizar el mejor manejo de los datos personales de los usuarios involucrados.
     Garantizar que se cumplan con las necesidades estructurales y funcionales del sistema y el trato de los datos personales

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 249 de 425—

como fecha y hora de salida;

b) Para soportes físicos: Número o clave del expediente utilizado, y
c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
Se lleva una bitácora de soporte técnico asociado a una base que se registra en red.
   - Nombre de usuario
   - Cargo
   - Fecha de entrada
   - Hora de entrada
   - Fecha de salida
   - Hora de salida
   - Datos modificados

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Soporte electrónico y físico (por semestre).
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   Semestral, asociado al equipo de trabajo generado en comunidad UNAM.
4. La manera en que asegura la integridad de las bitácoras, y
   Se imprime Semestralmente.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
      Nombre: Mtro. Pedro Benítez Mejía
      Cargo: Jefe de Departamento de Informática
      Periodicidad: Semestralmente
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
      Bitácora en red, autogestionada.

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 250 de 425—

a) La persona que resolvió el incidente;
Nombre, cargo, incidente, acción, descripción breve, fecha del incidente, sistema afectado, URL del sistema.

b) La metodología aplicada;
Se recopila la información con la información del registro donde se debe incluir la fecha del incidente, cual fue el incidente, una descripción breve de la solución ejecutada, los datos afectados, datos recuperados, de ser el caso el Sistema afectado y su dirección URL.

c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
Carpeta con bitácora de incidentes por semestre

d) Para soportes electrónicos:
Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
ambos
3. Cómo asegura la integridad de dicho registro, y
En la oficina del Director de Apoyo Técnico, y una copia en la oficina del Jefe de Departamento de Informática.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
Jefe de Departamento de Informática

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior (las instalaciones del área universitaria):
¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales así como los días de asueto.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —251 de 425—

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.
Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Es necesario presentar una credencial oficial vigente, bien sea de la Dirección General de Orientación y Atención Educativa, o de alguna entidad autorizada de la UNAM. Y en caso de no contar con ella, un previo registro en el acceso con alguna credencial de identificación con fotografía que será resguardada por el personal de vigilancia, para ser devuelta con el registro de hora de salida.

b) ¿Cómo las autentifica?

Solamente debe proporcionarse el acceso a las instalaciones con alguna identificación oficial para los siguientes casos:

- Personal de la Dirección General de Orientación y Atención Educativa. En caso de ser trabajadores contratados, deben contar con la identificación que acredita la pertenencia a esta dependencia. En caso de no contar con una credencial oficial, contar con algún gafete o documento expedido por el área para la cual está prestando sus servicios.
- En caso de visita de personal externo a la Dirección General de Orientación y Atención Educativa, debe presentar alguno de los siguientes documentos:
  - Credencial UNAM, en caso de pertenecer a alguna dependencia, sea el caso de tratarse de un alumno o trabajador de la Universidad Nacional Autónoma de México.
  - Credencial INE, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
  - Pasaporte, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
  - Cartilla militar, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —252 de 425—

c) ¿Cómo les autoriza el acceso?

Para el caso del personal que labora en la dependencia, se realiza presentando la credencial o gafete que acredita labora en la Dirección General de Orientación y Atención Educativa.
Para el caso de personal ajeno a la dependencia, es necesario presentar los documentos oficiales declarados en el punto anterior y registrar sus datos tales como:

- Nombre completo, Institución a la que representa, hora de entrada, fecha de entrada, área a visitar, motivo de la visita, hora de salida, firma.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.
Se cuenta con doble cerradura, al interior de la Dirección:

- Cerradura Tubular
- Cerradura Empotrada

Por la parte externa se cuenta con dos cerraduras externas y otras dos cerraduras el interior

- 2 Cerraduras Empotradas
- Cerradura Multipunto
- Cerradura Tubular

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Una vez registrado en el acceso principal, debe contar con las llaves para ingresar al área de Servidores. Y sólo el personal autorizado cuenta con las llaves del espacio y acceso al área.

2. ¿Cómo las autentifica?
   Es necesario ser personal autorizado para acceder al área. Por tal motivo debe contar con las llaves del inmueble y la credencial que acredite su vigencia en la plantilla del Departamento de Informática.

3. ¿Cómo les autoriza el acceso?
   Es necesario forzosamente ser personal del Departamento de Informática adscrito a la Dirección General de Orientación y Atención Educativa y tener las credenciales que acrediten ello.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —253 de 425—

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.
Es necesario cada año renovar el Aviso de Privacidad, y los métodos de guardado y almacenado para los datos personales. A demás, de tratarse de una convocatoria anual, esta debe renovarse si así lo amerita en los aspectos de seguridad actuales.
Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
1. Modelo de control de acceso (alguno de los siguientes):
   a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
   Si, debe ser una IP perteneciente a la red UNAM y haber sido dada de alta al departamento encargado de administrar el servidor. Así mismo, contar con las credenciales y los parámetros de conexión.
   b) ¿Es discrecional (matriz de control de acceso)?
   No, pero debe asentarse en la bitácora de conexión el acceso para cada usuario autorizado.
   c) ¿Está basado en roles (perfiles) o grupos?
   Roles
   d) ¿Está basado en reglas?
   Si, son proporcionadas por el administrador del servicio.
2. Perfiles de usuario y contraseñas en el sistema operativo de red:
   a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
   No, pero se cuenta con EGOSECURE que nos ayuda a monitorear la actividad de toda la red, y el uso de los equipos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 254 de 425—

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?

No, cada equipo cuenta con una contraseña generada por el Departamento de Informática, con los lineamientos establecidos por DGTIC, y una cuenta administrador creada exclusivamente al personal del autorizado.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No, en dado caso de ser necesario, debe crearse un nuevo usuario y contraseña individualmente por cada equipo dentro de la red.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?

No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

Alguno de los integrantes del Departamento de Informática de la Dirección General de Orientación y Atención Educativa.

b) ¿Quién autoriza la creación de nuevos perfiles?

El Director de Apoyo Técnico y el Jefe del Departamento de Informática.

c) ¿Se lleva registro de la creación de nuevos perfiles?

Si, en una Bitácora de usuarios, pero sin el dato de contraseña, sólo datos generales.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

Si

c) ¿Cómo se evita el acceso remoto no autorizado?

Se cuentan con llaves privadas de conexión y configuración de firewall, para el acceso único de los equipos autorizados, dichos equipos se encuentran en servidores de la DGTIC.

En el caso de la DGTIC

1. Señalar si realiza respaldos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —255 de 425—

a) Completos X, diferenciales_ o incrementales_;
Se realizan respaldos completos
b) De forma automática X o manual _,
A través de un script y un cron
c) Periodicidad con que los realiza:
Todos los miércoles y domingos a las 12:00 am

2. El tipo de medios que utiliza para almacenar las copias de seguridad:
Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.
3. Cómo y dónde se archiva esos medios:
El servidor de respaldos se encuentra en el centro de datos, posteriormente se respalda en cintas magnéticas identificadas y etiquetadas. Se resguardan en la oficina del departamento de Seguridad y Operación de Servidores.
4. Quién es el responsable de realizar estas operaciones:
El jefe de departamento Mtro. Enrique Pérez Campos) y jefe de área (Lic. Alan López de Jesús) ambos del Departamento de Seguridad y Operación de Servidores.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X__,
   c) Periodicidad con que los realiza: _Semestral_
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
Disco Duro, Nube de equipo de trabajo y USB si es posible.
3. Cómo y dónde archiva esos medios, y
En las instalaciones del Departamento de Informática.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
El Departamento de Informática

IX. PLAN DE CONTINGENCIA

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —256 de 425—

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Plan de Contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   Si se ha aplicado. No se han realizado pruebas de eficiencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
      No
   b) Si el sitio es propio o subcontratado con un tercero;
      No
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio y
      No
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
      No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**		
Identificador único*	502 62 05	
(Nombre del sistema A1) *	**Feria del Empleo UNAM. Registro CV**	
Recurso*	**Descripción***	**Control***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —257 de 425—

Penetration Testin Kit (PTK)	Se trata de una extensión del navegador que esta diseñada para probar la posible vulnerabilidad en el sistema	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular. Versión 6.1.5
Google Analytics	Te permite hacer un seguimiento de sitios web, blogs y redes sociales. Además, pone a tu disposición informes predeterminados y personalizables.	Podemos analizar el tráfico que esta generando nuestro sistema y que secciones están generando mayor impacto, así como diferentes estadísticas que van desde la recopilación del dispositivo de conexión, hasta el tiempo de conexión en nuestro sitio.
JMeter	Es una herramienta de carga para llevar a cabo simulaciones sobre cualquier recurso de Software.	Inicialmente diseñada para pruebas de estrés en aplicaciones web, hoy en día, su arquitectura ha evolucionado no sólo para llevar a cabo pruebas en componentes habilitados en Internet (HTTP), sino además en Bases de Datos, programas en Perl requisiciones FTP y prácticamente cualquier otro medio.

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. **Dirección de Planeación.**	
Identificador único*	502 62 05

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 258 de 425—

(Nombre del sistema A1)*	Feria del Empleo UNAM. Registro CV	
Medida de seguridad*	**Procedimiento***	**Responsable***
DDoS.	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Inyección SQL	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Jmeter	Pedro Benítez Mejía, 1 día.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 05	
(Nombre del sistema A1)*	**Feria del Empleo UNAM. Registro CV**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
DDoS.	Cumple con los requisitos.	Pedro Benítez Mejía, 1 día.
Inyección SQL	Cumple con los requisitos	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Probado para 500 peticiones durante 1 hora, permanece estable.	Pedro Benítez Mejía, 1 día.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa. Dirección de Planeación.		
Identificador único*	502 62 05	
(Nombre del sistema A1)*	**Feria del Empleo UNAM. Registro CV**	
Medida de seguridad*	**Acciones***	**Responsable***
Realizar pruebas de estrés en el sistema	Revisar cuantos usuarios pueden interactuar en el sistema.	Pedro Benítez Mejía, 2 días
Realizar pruebas de escalabilidad	Que mejoras pueden implementarse al sistema	Pedro Benítez Mejía, 1 semana
Realizar test de resistencia	Se realizan simulaciones de peticiones, relacionando la cantidad de peticiones con las localidades de posible impacto.	Pedro Benítez Mejía, 1 semana

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —259 de 425—

8. Programa específico de capacitación
   8.1. Programa de capacitación a los responsables de seguridad de datos personales
   8.2. Ass
9. Mejora continua
   9.1. A
   9.2. B
   9.3. C
   9.4. d
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

Dirección de Apoyo Técnico

Programa Registro del Premio al Talento Bachiller Universitario

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	502 62 01
(Nombre del sistema A1) *	**Registro del Premio al Talento Bachiller Universitario**
Datos personales (sensibles o no) contenidos en el sistema*:	Número de cuenta, Nombre, Apellido Paterno, Apellido Materno, Sexo, Fecha de Nacimiento, Calle, Número Interior, Número Exterior, Colonia, Alcaldía, Código Postal, Estado, Teléfono, Celular, Email, Plantel de Bachillerato, Año / semestre, Turno, Propuesto por y Rubro de participación. Expediente electrónico: 1. Carta de postulación, 2. Carta de declaración de conocimiento y conformidad , 3. Currículum vitae, 4. Historial académico, 5. Publicaciones: Primaria / Secundaria / Bachillerato.
Responsable*:	
Nombre*:	Lic. José Antonio Sánchez Yllañez
Cargo*:	Director de Apoyo Técnico
Funciones*:	Elaboración de la convocatoria, Integrar el Jurado Calificador del Premio Conocer y Autorizar la protección de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 260 de 425—

Obligaciones*:	Fomentar la protección de datos personales al interior de la Dirección Dar trámite a las solicitudes de los titulares de datos personales, para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)
	Encargados:
(Nombre del Encargado 1*)	Ing. Pedro Benitez Mejía
Cargo*:	Jefe del Departamento de Informática
Funciones*:	Estandarización de Datos y Coordinación de Proyecto
Obligaciones*:	Realizar el piloteo y aseguramiento de implementación de medidas de seguridad. Supervisión de datos generados por Google Analytics. Implementar medidas necesarias para evitar posibles ataques DDoS o cualquier ataque que pueda representar un problema en la continuidad del servicio. Considerar la limpieza de información previa a la inserción de datos en la Base de Datos con los lineamientos necesarios para evitar posibles inyecciones de SQL. Forzar el peso y formato de los documentos proporcionados a las necesidades del servidor utilizado. Encriptar documentos proporcionados, tanto en nombre de archivo como en integridad física del mismo. Agregar controles básicos para evitar ataques de bots (captcha). Implementar herramienta de Google Analitycs en los puntos vulnerables del sistema.
	Usuarios:
(Nombre del Usuario 1*)	Incorporar al Jurado del Premio: por cada usuario 1. Un representante de la Secretaría General; 2. Un representante de la Dirección General de la ENP; 3. Un representante de la Dirección General del CCH; 4. Una o un profesor designado por el Consejo Técnico de la ENP; 5. Una o un profesor designado por el Consejo Técnico del CCH; 6. Una o un alumno designado por el Consejo

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —261 de 425—

	Técnico de la ENP; 7. Una o un alumno designado por el Consejo Técnico del CCH; 8. Un representante de la Dirección General del Deporte Universitario, y 9. Un representante de la Dirección General de Orientación y Atención Educativa. Funciones: Definir los criterios generales de evaluación de los trabajos (expedientes digitales) y los mecanismos específicos para la adjudicación del premio en cada uno de los rubros o actividades de interés de la convocatoria. Obligaciones: Comprometerse a revisar a través del sistema cada uno de los expedientes digitales no resguardar la información proporcionada, y utilizar dicha información sólo para los fines de sus funciones asignadas, es decir dar su fallo a un ganador.
Cargo*:	Usuario universitario general
Funciones*:	Proveer de datos y documentos que serán evaluados por un miembro del comité evaluador.
Obligaciones*:	Cargar los datos solicitados, sólo los obligatorios de ser el caso. Cargar los documentos con los lineamientos solicitados, en peso y formato.
(Nombre del Usuario 2*)	Cuatro Representantes
Cargo*:	Comité Evaluador. (2 integrantes de la Escuela Nacional Colegio de Ciencias y Humanidades y 2 integrantes de la Escuela Nacional Preparatoria)
Funciones*:	Revisar y Calificar los alumnos aprobados para ser acreedores al premio.
Obligaciones*:	Comprometerse a resguardar la información proporcionada por el cuerpo estudiantil, y utilizarlo sólo para los fines de sus funciones asignadas.
Sistema (Nombre del A2)*:	**Seguimiento de Evaluación del Registro del Premio al Talento Bachiller Universitario**
Datos personales contenidos en el sistema*:	Número de cuenta, Nombre, Apellido Paterno, Apellido Materno, Sexo, Fecha de Nacimiento, Calle, Número Interior, Número Exterior, Colonia, Alcaldía, Código Postal, Estado, Teléfono, Celular, Email, Plantel de Bachillerato, Año / semestre, Turno, Propuesto por y Rubro de participación.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —262 de 425—

	Expediente electrónico: 1. Carta de postulación, 2. Carta de declaración de conocimiento y conformidad, 3. Curriculum vitae, 4. Historial académico, 5. Publicaciones: Primaria / Secundaria / Bachillerato.
Responsable:	
Nombre*:	Lic. José Antonio Sánchez Yllañez
Cargo*:	Director de Apoyo Técnico
Funciones*:	Conocer y Autorizar la protección de datos personales
Obligaciones*:	Fomentar la protección de datos personales al interior de la Dirección Dar trámite a las solicitudes de los titulares de datos personales, para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)
Encargados:	
(Nombre del Encargado 1*)	Ing. Pedro Benitez Mejía
Cargo*:	Jefe del Departamento de Informática
Funciones*:	Estandarización de Datos y Coordinación de Proyecto. Diseño, desarrollo y programación de sistema, orientado a una plantilla específica de calificaciones. Diseño y modelado de Base de Datos, para almacenar las calificaciones individuales de cada integrante del comité evaluador por cada integrante del cuerpo estudiantil calificado.
Obligaciones*:	Pilotar y Asegurar que Supervisión de datos generados por Google Analytics. Diseñar los campos específicos y estandarizados a criterios matemáticos que corresponden a una correcta evaluación con los parámetros solicitados.
	Usuarios:
(Nombre del Usuario 1*)	Comité evaluador. Cuatro representantes (Dos de la Escuela Nacional de Ciencias y Humanidades y dos de la Escuela Nacional Preparatoria)
Cargo*:	Dos integrantes de la Escuela Nacional Colegio de Ciencias y Humanidades y dos integrantes de la Escuela Nacional Preparatoria
Funciones*:	Cotejar y evaluar los datos y documentos proporcionados por el integrante del cuerpo estudiantil seleccionado y asentar su calificación en el sistema

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —263 de 425—

Obligaciones*:	utilizar la información proporcionada por el integrante del cuerpo estudiantil solo con los fines necesarios que este sistema solicita

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	S02_62_01
(Nombre del sistema A1*)	Registro del Premio al Talento Bachiller Universitario
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos. Se tienen 2 bases de datos con diseño de entidad relación y llave primaria asociada al integrante del cuerpo estudiantil en número de cuenta. La primera orientada a los datos generales tales como: nombre apellido paterno apellido materno dirección plantel turno y área Perteneciente. La segunda es una relación entre los datos generales y la calificación que le fue asignada al alumno
Características del lugar donde se resguardan los soportes:*	dgoae.servicios.unam.mx/ IP: 132.247.28.92 Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico: • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware: Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —264 de 425—

	• Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. ✓ Estudiantes requiere usuario y contraseña. ✓ Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la Base de Datos: • Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol • Respaldos de Base de Datos
(Nombre del sistema A2*)	**Seguimiento del Premio al Talento al Bachiller Universitario**
Tipo de soporte*:	Soporte electrónico
Descripción*:	Se tienen dos bases de datos con diseño entidad relación y llave primaria asociada al integrante del cuerpo estudiantil el número de cuenta. La primera cuenta con los elementos que generan la calificación final asociada a cada integrante del comité evaluador. La segunda es una relación entre los datos generales y la calificación que le fue asignada al alumno.
Características del lugar donde se resguardan los soportes*:	dgoae.servicios.unam.mx/ IP: 132.247.28.92 Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 265 de 425—

	• El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware: • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación: • Control de accesos a usuarios dependiendo del tipo de rol asignado. ✓ Estudiantes requiere usuario y contraseña. ✓ Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida. Nivel 6: Seguridad en la Base de Datos:

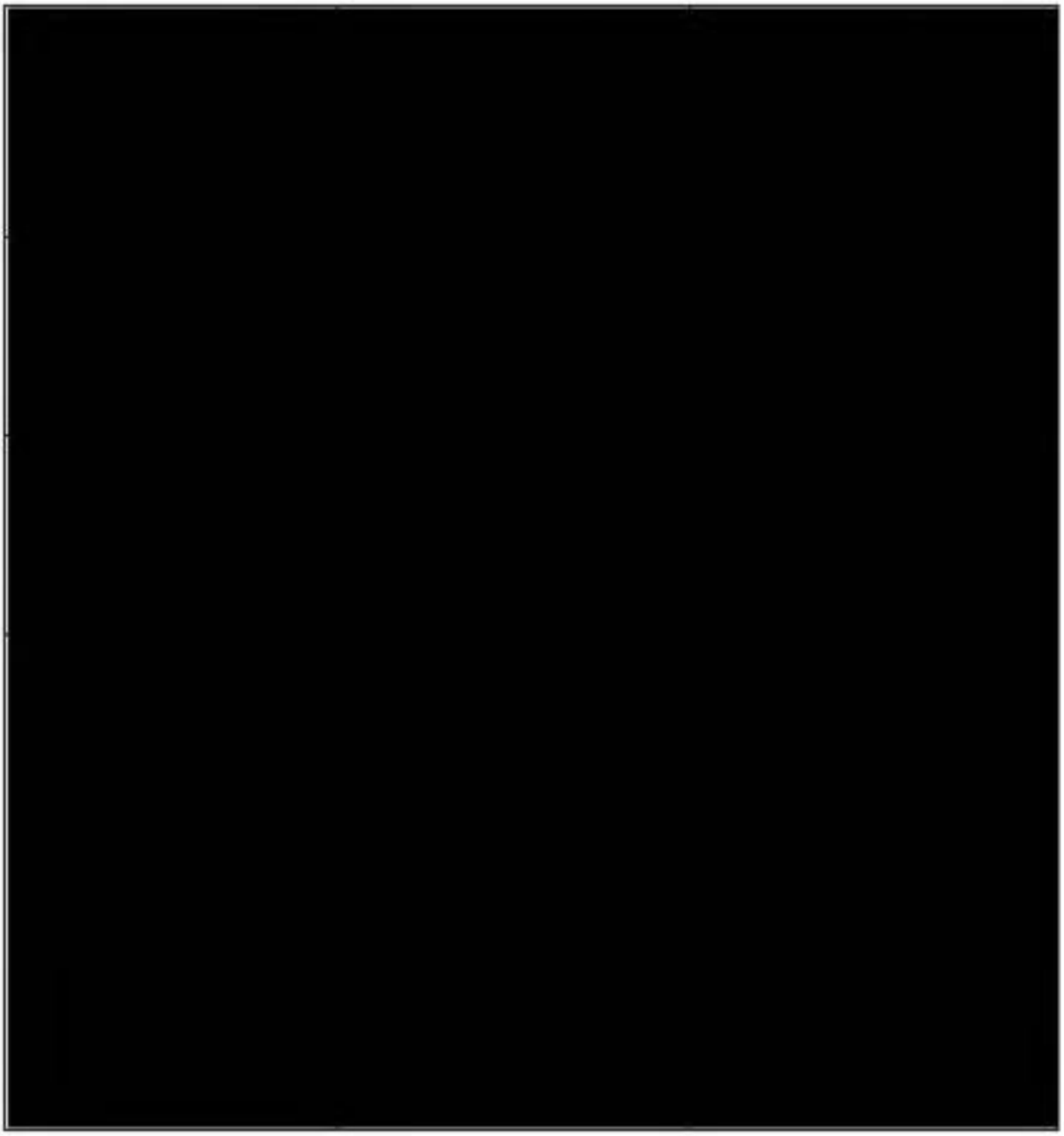
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 266 de 425—

	• Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol • Respaldos de Base de Datos

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	**502 62 01**	
(Nombre del sistema A1) *	**Registro del Premio al Talento del Bachiller Universitario**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 267 de 425—



4. Análisis de brecha

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	502 62 01
(Nombre del sistema A1) *	Registro del Premio al Talento Bachiller Universitario

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 268 de 425—

Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]		

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	502 62 01

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 269 de 425—

(Nombre del sistema A1) *	Registro del Premio al Talento Bachiller Universitario		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 270 de 425—



6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	502_62_01
(Nombre del sistema A1) *	**Registro del Premio al Talento Bachiller Universitario**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NO APLICA
Transferencias mediante el traslado de soportes electrónicos:	a) La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —271 de 425—

Transferencias mediante el traslado sobre redes electrónicas:	La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales. El acceso al sistema se realiza por medio de un usuario previamente registrado y con sesión activa.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

5. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
    - Se cuentan con contraseñas robustas.
    - Debe de darse de alta una dirección IP específica dentro de la red UNAM.
    - Existe un puerto en el servidor dedicado a la transferencia de información.
    - Es asignado un espacio específico para la carga de proyectos.

6. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
    - Nombre: Mtro. Pedro Benítez Mejía
    - Cargo: Jefe de Departamento de Informática
    - Funciones: Coordinación y Aprobación de Requisitos del Sistema. Diseño, desarrollo y programación de Sistema. Diseño, modelado e implementación de Base de Datos del Sistema.
    - Obligaciones: Garantizar el mejor manejo de los datos personales de los usuarios involucrados.
    - Garantizar que se cumplan con las necesidades estructurales y funcionales del sistema y el trato de los datos personales

    - Nombre: Martha Verónica Rojas Hernández
    - Cargo: Jefa de Área.
    - Funciones: Generación de Constancias y Menciones Honoríficas, revisión de documentación envío y comunicación a través de correo electrónico.
    - Obligaciones: Probar posible mal funcionamiento del

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 272 de 425—

Sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.

   Se lleva una bitácora de soporte técnico asociado a una base que se registra en red.

   - Nombre de usuario
   - Cargo
   - Fecha de entrada
   - Hora de entrada
   - Fecha de salida
   - Hora de salida
   - Datos modificados

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Soporte electrónico y físico (por semestre).
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   Semestral, asociado al equipo de trabajo generado en comunidad UNAM.
4. La manera en que asegura la integridad de las bitácoras, y
   Se imprime Semestralmente.
5. Respecto del análisis de las bitácoras:
   a) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
      Nombre: Mtro. Pedro Benítez Mejía
      Cargo: Jefe de Departamento de Informática
      Periodicidad: Semestralmente
   b) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
      Bitácora en red, autogestionada.

IV. REGISTRO DE INCIDENTES

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —273 de 425—

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:

   a) La persona que resolvió el incidente;
   Nombre, cargo, incidente, acción, descripción breve, fecha del incidente, sistema afectado, URL del sistema.

   b) La metodología aplicada;

   Se recopila la información con la información del registro donde se debe incluir la fecha del incidente, cual fue el incidente, una descripción breve de la solución ejecutada, los datos afectados, datos recuperados, de ser el caso el Sistema afectado y su dirección URL.

   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   Carpeta con bitácora de incidentes por semestre

   d) Para soportes electrónicos:
   Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
   Ambos

3. Cómo asegura la integridad de dicho registro, y
   En la oficina del Director de Apoyo Técnico, y una copia en la oficina del Jefe de Departamento de Informática.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
   Jefe de Departamento de Informática

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —274 de 425—

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas, si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.
Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Es necesario presentar una credencial oficial vigente, bien sea de la Dirección General de Orientación y Atención Educativa, o de alguna entidad autorizada de la UNAM. Y en caso de no contar con ella, un previo registro en el acceso con alguna credencial de identificación con fotografía que será resguardada por el personal de vigilancia, para ser devuelta con el registro de hora de salida.

b) ¿Cómo las autentifica?

Solamente debe proporcionarse el acceso a las instalaciones con alguna identificación oficial para los siguientes casos:

- Personal de la Dirección General de Orientación y Atención Educativa. En caso de ser trabajadores contratados, deben contar con la identificación que acredita la pertenencia a esta dependencia. En caso de no contar con una credencial oficial, contar con algún gafete o documento expedido por el área para la cual está prestando sus servicios.
- En caso de visita de personal externo a la Dirección General de Orientación y Atención Educativa, debe presentar alguno de los siguientes documentos:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —275 de 425—

- Credencial UNAM, en caso de pertenecer a alguna dependencia, sea el caso de tratarse de un alumno o trabajador de la Universidad Nacional Autónoma de México.
- Credencial INE, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
- Pasaporte, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
- Cartilla militar, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.

c) ¿Cómo les autoriza el acceso?

Para el caso del personal que labora en la dependencia, se realiza presentando la credencial o gafete que acredita labora en la Dirección General de Orientación y Atención Educativa.

Para el caso de personal ajeno a la dependencia, es necesario presentar los documentos oficiales declarados en el punto anterior y registrar sus datos tales como:

- Nombre completo, Institución a la que representa, hora de entrada, fecha de entrada, área a visitar, motivo de la visita, hora de salida, firma.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.

Se cuenta con doble cerradura, al interior de la Dirección:

- Cerradura Tubular
- Cerradura Empotrada

Por la parte externa se cuenta con dos cerraduras externas y otras dos cerraduras el interior

- 2 Cerraduras Empotradas
- Cerradura Multipunto
- Cerradura Tubular

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?

   Una vez registrado en el acceso principal, debe contar con las llaves para ingresar al área de Servidores. Y sólo el personal autorizado cuenta con las llaves del espacio y acceso al área.

2. ¿Cómo las autentifica?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —276 de 425—

Es necesario ser personal autorizado para acceder al área. Por tal motivo debe contar con las llaves del inmueble y la credencial que acredite su vigencia en la plantilla del Departamento de Informática.

3. ¿Cómo les autoriza el acceso?
Es necesario forzosamente ser personal del Departamento de Informática adscrito a la Dirección General de Orientación y Atención Educativa y tener las credenciales que acrediten ello.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.
Es necesario cada año renovar el Aviso de Privacidad, y los métodos de guardado y almacenado para los datos personales. A demás, de tratarse de una convocatoria anual, esta debe renovarse si así lo amerita en los aspectos de seguridad actuales.
Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Si, debe ser una IP perteneciente a la red UNAM y haber sido dada de alta al departamento encargado de administrar el servidor. Así mismo, contar con las credenciales y los parámetros de conexión.

b) ¿Es discrecional (matriz de control de acceso)?
No, pero debe asentarse en la bitácora de conexión el acceso para cada usuario autorizado.

c) ¿Está basado en roles (perfiles) o grupos?
Roles

d) ¿Está basado en reglas?
Si, son proporcionadas por el administrador del servicio.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No, pero se cuenta con EGOSECURE que nos ayuda a monitorear la actividad de toda la red, y el uso de los equipos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —277 de 425—

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?

No, cada equipo cuenta con una contraseña generada por el Departamento de Informática, con los lineamientos establecidos por DGTIC, y una cuenta administrador creada exclusivamente al personal del autorizado.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No, en dado caso de ser necesario, debe crearse un nuevo usuario y contraseña individualmente por cada equipo dentro de la red.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?

No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?

No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?

Alguno de los integrantes del Departamento de Informática de la Dirección General de Orientación y Atención Educativa.

b) ¿Quién autoriza la creación de nuevos perfiles?

El Director de Apoyo Técnico y el Jefe del Departamento de Informática.

c) ¿Se lleva registro de la creación de nuevos perfiles?

Si, en una Bitácora de usuarios, pero sin el dato de contraseña, sólo datos generales.

5. Acceso remoto al sistema de tratamiento de datos personales:

d) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?

No

e) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?

Si

f) ¿Cómo se evita el acceso remoto no autorizado?

Se cuentan con llaves privadas de conexión y configuración de firewall, para el acceso único de los equipos autorizados, dichos equipos se encuentran en servidores de la DGTIC.

En el caso de la DGTIC

1. **Señalar si realiza respaldos**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —278 de 425—

a) **Completos X, diferenciales_ o incrementales_;**
Se realizan respaldos completos
b) **De forma automática X o manual _,**
A través de un script y un cron
c) **Periodicidad con que los realiza:**
Todos los miércoles y domingos a las 12:00 am

2. **El tipo de medios que utiliza para almacenar las copias de seguridad:**
Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.
3. **Cómo y dónde se archiva esos medios:**
El servidor de respaldos se encuentra en el centro de datos, posteriormente se respalda en cintas magnéticas identificadas y etiquetadas. Se resguardan en la oficina del departamento de Seguridad y Operación de Servidores.
4. **Quién es el responsable de realizar estas operaciones:**
El jefe de departamento Mtro. Enrique Pérez Campos) y jefe de área (Lic. Alan López de Jesús) ambos del Departamento de Seguridad y Operación de Servidores.

En el caso de la DGOAE

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a. Completos **X** , diferenciales ___ o incrementales___;
   b. De forma automática ____ o Manual **X** ,
   c. Periodicidad con que los realiza: **Semestral**
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Disco Duro, Nube de equipo de trabajo y USB si es posible.
3. Cómo y dónde archiva esos medios, y
   En las instalaciones del Departamento de Informática.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El Departamento de Informática

IX. PLAN DE CONTINGENCIA

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —279 de 425—

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Plan de Contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.
   Si se ha aplicado. No se han realizado pruebas de eficiencia.
3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a) El tipo de sitio (caliente, tibio o frío);
      No
   b) Si el sitio es propio o subcontratado con un tercero;
      No
   c) Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio
      No
   d) Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
      No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502_62_01	
Nombre del sistema*	**Registro del Premio al Talento Bachiller Universitario**	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit (PTK)	Se trata de una extensión del navegador que esta diseñada para probar la posible vulnerabilidad en el sistema	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular. Versión 6.1.5
Google Analytics	Te permite hacer un seguimiento de sitios web, blogs y redes sociales. Además, pone a tu disposición	Podemos analizar el tráfico que esta generando nuestro sistema y que secciones están generando mayor impacto, así como diferentes estadísticas que van desde la recopilación del

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 280 de 425—

	informes predeterminados y personalizables.	dispositivo de conexión, hasta el tiempo de conexión en nuestro sitio.
JMeter	Es una herramienta de carga para llevar a cabo simulaciones sobre cualquier recurso de Software.	Inicialmente diseñada para pruebas de estrés en aplicaciones web, hoy en día, su arquitectura ha evolucionado no sólo para llevar a cabo pruebas en componentes habilitados en Internet (HTTP), sino además en Bases de Datos, programas en Perl requisiciones FTP y prácticamente cualquier otro medio.

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 01	
(Nombre del sistema A1)*	**Registro del Premio al Talento Bachiller Universitario**	
Medida de seguridad*	**Procedimiento***	**Responsable***
DDoS.	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Inyección SQL	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Jmeter	Pedro Benítez Mejía, 1 día.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 01	
(Nombre del sistema A1)*	**Registro del Premio al Talento Bachiller Universitario**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
DDoS.	Cumple con los requisitos.	Pedro Benítez Mejía, 1 día.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDSzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 281 de 425—

Inyección SQL	Cumple con los requisitos	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Probado para 500 peticiones durante 1 hora, permanece estable.	Pedro Benítez Mejía, 1 día.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 01	
(Nombre del sistema A1) *	**Registro del Premio al Talento Bachiller Universitario**	
Medida de seguridad*	**Acciones***	**Responsable***
Realizar pruebas de estrés en el sistema	Revisar cuantos usuarios pueden interactuar en el sistema.	Pedro Benítez Mejía, 2 días
Realizar pruebas de escalabilidad	Que mejoras pueden implementarse al sistema	Pedro Benítez Mejía, 1 semana
Realizar test de resistencia	Se realizan simulaciones de peticiones, relacionando la cantidad de peticiones con las localidades de posible impacto.	Pedro Benítez Mejía, 1 semana

8. Programa específico de capacitación
9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 282 de 425—

Programa Registro de la Presea Bernardo Quintana Arrioja

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único*	502 62 02
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**
Datos personales (sensibles o no) contenidos en el sistema*:	Número de cuenta, Nombre, Apellido Paterno, Apellido Materno, Sexo, Estado civil, Fecha de Nacimiento, Nacionalidad, Lugar de nacimiento, Calle, Número Interior, Número Exterior, Colonia, Alcaldía, Código Postal, Estado, Teléfono, Celular, Email, Plantel de Bachillerato, promedio, Categoría de participación y Expediente electrónico: Curriculum vitae, carta de exposición de motivos, acta de nacimiento, credencial de alumno, constancia de estudios y autobiografía.
Responsable*:	
Nombre*:	Lic. José Antonio Sánchez Yllañez
Cargo*:	Director de Apoyo Técnico
Funciones*:	Elaboración de la convocatoria, Integrar el Jurado Calificador de la Presea Conocer y Autorizar la protección de datos personales
Obligaciones*:	Fomentar la protección de datos personales al interior de la Dirección Dar trámite a las solicitudes de los titulares de datos personales, para el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)
	Encargados:
(Nombre del Encargado 1*)	Ing. Pedro Benitez Mejía
Cargo*:	Jefe del Departamento de Informática
Funciones*:	Estandarización de Datos y Coordinación de Proyecto
Obligaciones*:	Realizar el piloteo y aseguramiento de implementación de medidas de seguridad. Supervisión de datos generados por Google Analytics. Implementar medidas necesarias para evitar posibles ataques DDoS o cualquier ataque que pueda representar un problema en la continuidad del servicio. Considerar la limpieza de información previa a la inserción de datos en la Base de Datos con los lineamientos necesarios para evitar posibles inyecciones de SQL. Forzar el peso y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 283 de 425—

	formato de los documentos proporcionados a las necesidades del servidor utilizado. Encriptar documentos proporcionados, tanto en nombre de archivo como en integridad física del mismo. Agregar controles básicos para evitar ataques de bots (captcha). Implementar herramienta de Google Analitycs en los puntos vulnerables del sistema
	Usuarios:
(Nombre del Usuario 1*)	Jurado Calificador de la Presea: ▪ Un representante de la Secretaría General; ▪ Un representante de la Dirección General de Orientación y Atención Educativa. ▪ Dos representantes de la Dirección General de la ENP; ▪ Dos representantes de la Dirección General del CCH; ▪ Un miembro de la Fundación de Apoyo a la Juventud IAP; ▪ Un ex ganador de la presea; ▪ Un representante de organización juvenil y ▪ Un académico en materia de juventud Funciones: Definir los criterios generales de evaluación de los trabajos (expedientes digitales) y los mecanismos específicos para la adjudicación de la presea en cada uno de los rubros o actividades de interés de la convocatoria. Obligaciones: Comprometerse a revisar a través del sistema cada uno de los expedientes digitales no resguardar la información proporcionada, y utilizar dicha información sólo para los fines de sus funciones asignadas, es decir dar su fallo a un ganador.
Cargo*:	Usuario universitario general
Funciones*:	Proveer de datos y documentos que serán evaluados por un miembro del Jurado Calificador.
Obligaciones*:	Cargar los datos solicitados, sólo los obligatorios de ser el caso. Cargar los documentos con los lineamientos solicitados, en peso y formato.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico	
Identificador único**	502_62_02

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 284 de 425—

(Nombre del sistema A1*)	Registro de la Presea Bernardo Quintana Arrioja
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos. Se tienen 2 bases de datos con diseño de entidad relación y llave primaria asociada al integrante del cuerpo estudiantil en número de cuenta. La primera orientada a los datos generales tales como: nombre apellido paterno apellido materno dirección plantel turno y área Perteneciente. La segunda es una relación entre los datos generales y la evaluación del estudiante
Características del lugar donde se resguardan los soportes:*	dgoae.servicios.unam.mx/ IP: 132.247.28.92 Alojamiento en el centro de datos de DGTIC por lo que se cuenta con seis niveles de seguridad Nivel 1: Seguridad de acceso físico: • El personal registra fecha y hora de entrada/salida. • Registra equipo de cómputo externo. • El acceso es con credencial de la institución. • Existe vigilancia de personal autorizado y cámaras de video. Nivel 2: Seguridad en la infraestructura del hardware: • Los servidores se encuentran resguardados dentro de un aula informática de acceso restringido. • El lugar tiene la temperatura adecuada para el correcto funcionamiento de los servidores. • Etiquetado en los cables de conexión. Nivel 3: Seguridad en la infraestructura del software: • Instalación de programas que permiten la detección y eliminación de programas maliciosos y spyware. • Configuración de firewall proxy para evitar conexiones directas desde el exterior de la red. • Restricción en los puertos de entrada/salida por dirección IP • Configuración de puertos disponibles a ciertas direcciones IPs para el acceso a la Base de Datos del Sistema Integra. Nivel 4: Seguridad del sistema operativo: • Autenticación al sistema ingresando usuario y contraseña de una cuenta de administrador. Nivel 5: Seguridad en la aplicación:

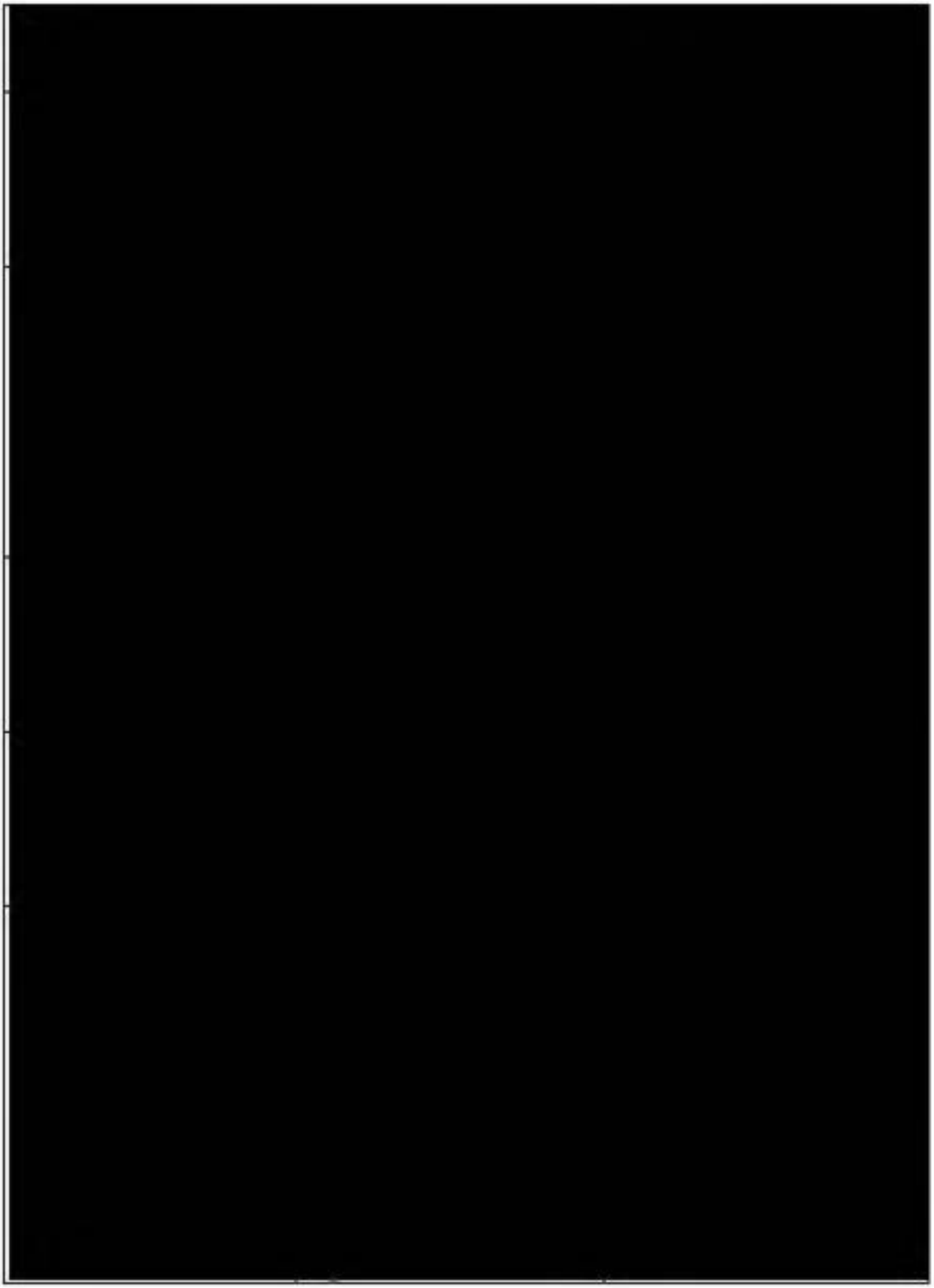
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 285 de 425—

	• Control de accesos a usuarios dependiendo del tipo de rol asignado. ✓ Estudiantes requiere usuario y contraseña. ✓ Personal de la DGOAE requiere usuario, contraseña y dirección IP permitida. • Desarrollo e implementación del módulo que administra auditorías por usuario, nombre de módulo y dirección IP. Nivel 6: Seguridad en la Base de Datos: • Acceso restringido por usuario y dirección IP de acceso local. • Privilegios de lectura, escritura, modificación, ejecución y eliminación dependiendo del rol que tiene los desarrolladores. • Respaldos de Base de Datos

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 286 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 287 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

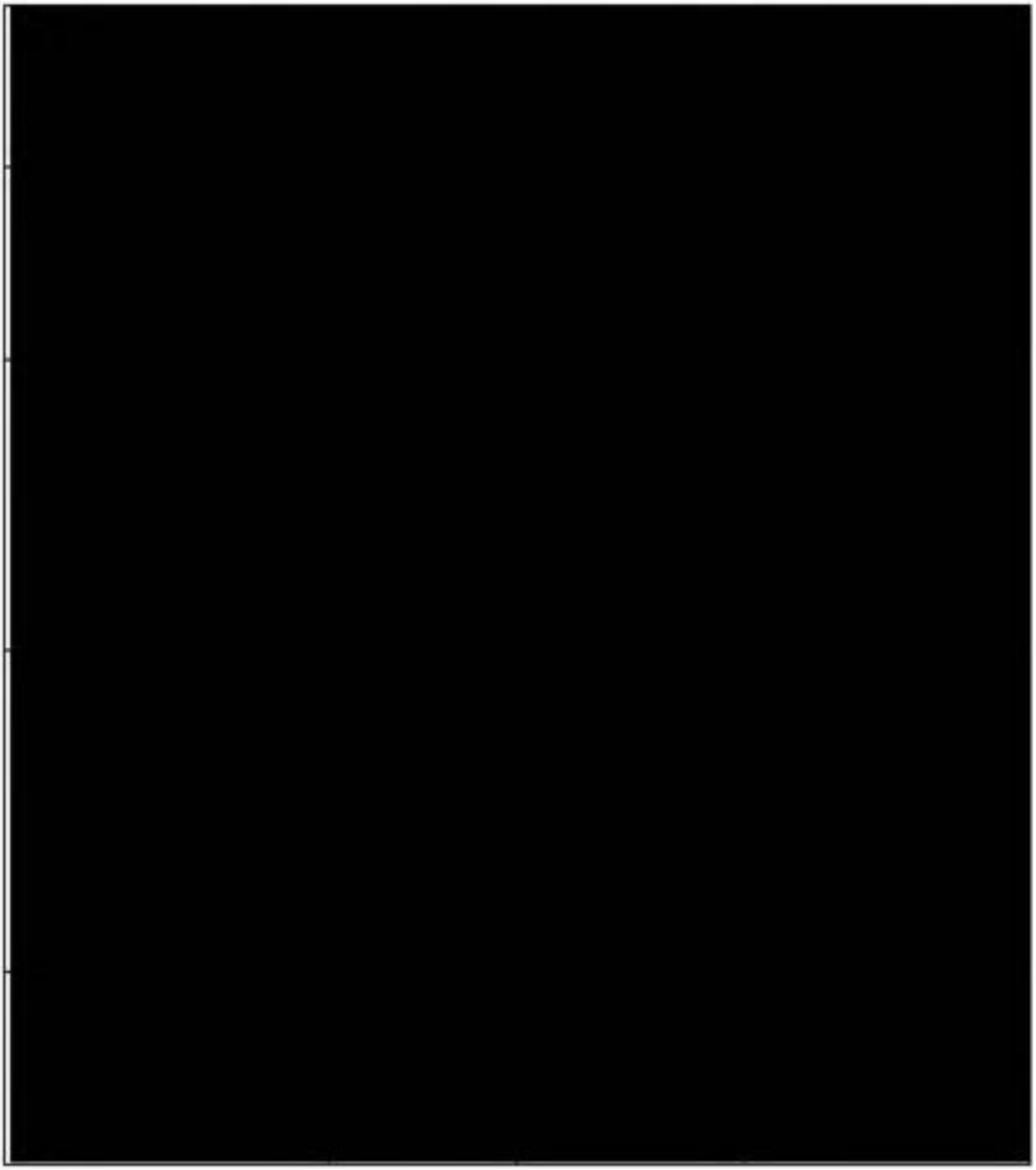
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 288 de 425—

[redacted]

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico			
Identificador único*	502 62 02		
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
[redacted]			

ID del Documento: gIrPdH8ZIhi+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 289 de 425—



6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa,

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 290 de 425—

Dirección de Apoyo Técnico	
Identificador único*	502 62 02
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	NO APLICA
Transferencias mediante el traslado de soportes electrónicos:	a) La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales.
Transferencias mediante el traslado sobre redes electrónicas:	La información se encuentra en los servidores que se encuentran bajo el resguardo de la DGOAE, y debe ser consultada directamente en la fuente proporcionada. El acceso a este sistema debe ser autorizado por el personal responsable, y firmar el acuerdo de confidencialidad y protección de datos personales. El acceso al sistema se realiza por medio de un usuario previamente registrado y con sesión activa.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
    - Se cuentan con contraseñas robustas.
    - Debe de darse de alta una dirección IP específica dentro de la red UNAM.
    - Existe un puerto en el servidor dedicado a la transferencia de información.
    - Es asignado un espacio específico para la carga de proyectos.

2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.
    - Nombre: Mtro. Pedro Benítez Mejía

    Cargo: Jefe de Departamento de Informática
    Funciones: Coordinación y Aprobación de Requisitos del Sistema. Diseño, desarrollo y programación de Sistema. Diseño, modelado e implementación de Base de Datos del Sistema.
    Obligaciones: Garantizar el mejor manejo de los datos personales de los usuarios involucrados.
    Garantizar que se cumplan con las necesidades estructurales y funcionales del

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —291 de 425—

sistema y el trato de los datos personales

- Nombre: Martha Verónica Rojas Hernández
  Cargo: Jefa de Área.
  Funciones: Generación de Constancias y Menciones Honoríficas, revisión de documentación envío y comunicación a través de correo electrónico.
  Obligaciones: Probar posible mal funcionamiento del Sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:
   a) Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
   b) Para soportes físicos: Número o clave del expediente utilizado, y
   c) Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
   Se lleva una bitácora de soporte técnico asociado a una base que se registra en red.
      - Nombre de usuario
      - Cargo
      - Fecha de entrada
      - Hora de entrada
      - Fecha de salida
      - Hora de salida
      - Datos modificados

2. Si las bitácoras están en soporte físico o en soporte electrónico;
   Soporte electrónico y físico (por semestre).
3. Lugar dónde almacena las bitácoras y por cuánto tiempo;
   Semestral, asociado al equipo de trabajo generado en comunidad UNAM.
4. La manera en que asegura la integridad de las bitácoras, y
   Se imprime Semestralmente.
5. Respecto del análisis de las bitácoras:
   c) Quién es el responsable de analizarlas (si es el área universitaria o si es un tercero) y cada cuándo las analiza, y
   Nombre: Mtro. Pedro Benítez Mejía
   Cargo: Jefe de Departamento de Informática
   Periodicidad: Semestralmente
   d) Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.
   Bitácora en red, autogestionada.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 292 de 425—

IV. REGISTRO DE INCIDENTES

Describir el procedimiento de atención de incidentes que tiene implementado el área universitaria y especificar si lleva registro de los incidentes relativos a soportes físicos, como lo son la pérdida o alteración no autorizada de expedientes, y para el caso de soportes electrónicos, ofrecer detalles sobre el registro de incidentes en el cual consigne los procedimientos realizados para la recuperación de los datos o para permitir la disponibilidad del proceso.

1. Los datos que registra:
   a) La persona que resolvió el incidente;
   Nombre, cargo, incidente, acción, descripción breve, fecha del incidente, sistema afectado, URL del sistema.
   b) La metodología aplicada;
   Se recopila la información con la información del registro donde se debe incluir la fecha del incidente, cual fue el incidente, una descripción breve de la solución ejecutada, los datos afectados, datos recuperados, de ser el caso el Sistema afectado y su dirección URL.
   c) Para soportes físicos: Los oficios, documentos, expedientes, estantes o archiveros, tanto los dañados como los recuperados, y
   Carpeta con bitácora de incidentes por semestre
   d) Para soportes electrónicos:
   Los campos, registros, tablas, bases de datos o archivos electrónicos, tanto dañados como recuperados, el nombre de los sistemas y la infraestructura afectada, indicar si el incidente afectó el servidor principal y los servidores de respaldo, etc.

2. Si el registro está en soporte físico o en soporte electrónico;
   Ambos

3. Cómo asegura la integridad de dicho registro, y
   En la oficina del Director de Apoyo Técnico, y una copia en la oficina del Jefe de Departamento de Informática.
4. Para el caso de soportes electrónicos, quién autoriza la recuperación de datos.
   Jefe de Departamento de Informática

V. ACCESO A LAS INSTALACIONES

En el caso de la DGOAE

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):
   ¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones? Por ejemplo, se espera que describa si cuenta con uno o más puntos de control de acceso y quienes los operan, si tiene vigilancia las 24 horas,

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —293 de 425—

si ha levantado bardas o cercas, si existe un sistema de tratamiento de datos personales de videovigilancia, entre otras posibles medidas.

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Esta dependencia universitaria está en proceso de implementar un sistema de tratamiento de datos personales de videovigilancia.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones:

a) ¿Cómo las identifica?

Es necesario presentar una credencial oficial vigente, bien sea de la Dirección General de Orientación y Atención Educativa, o de alguna entidad autorizada de la UNAM. Y en caso de no contar con ella, un previo registro en el acceso con alguna credencial de identificación con fotografía que será resguardada por el personal de vigilancia, para ser devuelta con el registro de hora de salida.

b) ¿Cómo las autentifica?

Solamente debe proporcionarse el acceso a las instalaciones con alguna identificación oficial para los siguientes casos:

- Personal de la Dirección General de Orientación y Atención Educativa. En caso de ser trabajadores contratados, deben contar con la identificación que acredita la pertenencia a esta dependencia. En caso de no contar con una credencial oficial, contar con algún gafete o documento expedido por el área para la cual está prestando sus servicios.
- En caso de visita de personal externo a la Dirección General de Orientación y Atención Educativa, debe presentar alguno de los siguientes documentos:
    - Credencial UNAM, en caso de pertenecer a alguna dependencia, sea el caso de tratarse de un alumno o trabajador de la Universidad Nacional Autónoma de México.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —294 de 425—

- Credencial INE, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
- Pasaporte, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.
- Cartilla militar, es necesario que tenga vigencia y coincida con las características fisonómicas de la credencial presentada.

c) ¿Cómo les autoriza el acceso?
Para el caso del personal que labora en la dependencia, se realiza presentando la credencial o gafete que acredita labora en la Dirección General de Orientación y Atención Educativa.
Para el caso de personal ajeno a la dependencia, es necesario presentar los documentos oficiales declarados en el punto anterior y registrar sus datos tales como:

- Nombre completo, Institución a la que representa, hora de entrada, fecha de entrada, área a visitar, motivo de la visita, hora de salida, firma.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

¿Qué medidas de seguridad ha implementado para controlar el acceso a los espacios donde almacena los soportes físicos o electrónicos del sistema? Por ejemplo, se espera que precise el tipo de puertas y cerraduras instaladas, si tiene instalados controles biométricos, si administra la asignación de llaves y/o claves de acceso para abrir puertas y/o estantería, si cuenta con vigilancia las 24 horas, si hay un sistema de tratamiento de datos personales de videovigilancia, entre otras medidas.
Se cuenta con doble cerradura, al interior de la Dirección:

- Cerradura Tubular
- Cerradura Empotrada

Por la parte externa se cuenta con dos cerraduras externas y otras dos cerraduras el interior

- 2 Cerraduras Empotradas
- Cerradura Multipunto
- Cerradura Tubular

Para las personas que acceden a dichos espacios interiores:

1. ¿Cómo las identifica?
   Una vez registrado en el acceso principal, debe contar con las llaves para ingresar al área de Servidores. Y sólo el personal autorizado cuenta con las llaves del espacio y acceso al área.
2. ¿Cómo las autentifica?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 295 de 425—

Es necesario ser personal autorizado para acceder al área. Por tal motivo debe contar con las llaves del inmueble y la credencial que acredite su vigencia en la plantilla del Departamento de Informática.

3. ¿Cómo les autoriza el acceso?
   Es necesario forzosamente ser personal del Departamento de Informática adscrito a la Dirección General de Orientación y Atención Educativa y tener las credenciales que acrediten ello.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.
Es necesario cada año renovar el Aviso de Privacidad, y los métodos de guardado y almacenado para los datos personales. A demás, de tratarse de una convocatoria anual, esta debe renovarse si así lo amerita en los aspectos de seguridad actuales.
Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)?
Si, debe ser una IP perteneciente a la red UNAM y haber sido dada de alta al departamento encargado de administrar el servidor. Así mismo, contar con las credenciales y los parámetros de conexión.

b) ¿Es discrecional (matriz de control de acceso)?
No, pero debe asentarse en la bitácora de conexión el acceso para cada usuario autorizado.

c) ¿Está basado en roles (perfiles) o grupos?
Roles

d) ¿Está basado en reglas?
Si, son proporcionadas por el administrador del servicio.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos?
No, pero se cuenta con EGOSECURE que nos ayuda a monitorear la actividad de toda la red, y el uso de los equipos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 296 de 425—

b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas?
No, cada equipo cuenta con una contraseña generada por el Departamento de Informática, con los lineamientos establecidos por DGTIC, y una cuenta administrador creada exclusivamente al personal del autorizado.

c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No, en dado caso de ser necesario, debe crearse un nuevo usuario y contraseña individualmente por cada equipo dentro de la red.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas?
No

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena?
No

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles?
Alguno de los integrantes del Departamento de Informática de la Dirección General de Orientación y Atención Educativa.

b) ¿Quién autoriza la creación de nuevos perfiles?
El Director de Apoyo Técnico y el Jefe del Departamento de Informática.

c) ¿Se lleva registro de la creación de nuevos perfiles?
Si, en una Bitácora de usuarios, pero sin el dato de contraseña, sólo datos generales.

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema?
No

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento?
Si

c) ¿Cómo se evita el acceso remoto no autorizado?
Se cuentan con llaves privadas de conexión y configuración de firewall, para el acceso único de los equipos autorizados, dichos equipos se encuentran en servidores de la DGTIC.

En el caso de la DGTIC

1. **Señalar si realiza respaldos**
   a) **Completos X, diferenciales_ o incrementales_;**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 297 de 425—

Se realizan respaldos completos

b) **De forma automática** X **o manual _,**

A través de un script y un cron

c) **Periodicidad con que los realiza:**

Todos los miércoles y domingos a las 12:00 am

2. **El tipo de medios que utiliza para almacenar las copias de seguridad:**

Se realiza el respaldo en un servidor dedicado a almacenar respaldos y después de un mes se guardan en cintas magnéticas.

3. **Cómo y dónde se archiva esos medios:**

El servidor de respaldos se encuentra en el centro de datos, posteriormente se respalda en cintas magnéticas identificadas y etiquetadas. Se resguardan en la oficina del departamento de Seguridad y Operación de Servidores.

4. **Quién es el responsable de realizar estas operaciones:**

El jefe de departamento Mtro. Enrique Pérez Campos) y jefe de área (Lic. Alan López de Jesús) ambos del Departamento de Seguridad y Operación de Servidores.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_X_, diferenciales ___ o incrementales___;
   b) De forma automática ____ o Manual __X__,
   c) Periodicidad con que los realiza: _Semestral_
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Disco Duro, Nube de equipo de trabajo y USB si es posible.
3. Cómo y dónde archiva esos medios, y
   En las instalaciones del Departamento de Informática.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero).
   El Departamento de Informática

IX. PLAN DE CONTINGENCIA

1. Presentar el plan de contingencia con el cual garantiza la continuidad de la operación del sistema o informar si no lo tiene, pero se encuentra desarrollándolo.
   Plan de Contingencia.
2. Si cuenta con plan de contingencia y lo ha implementado, deberá indicar si realiza pruebas de eficiencia de este.

Si se ha aplicado. No se han realizado pruebas de eficiencia.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud5=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 298 de 425—

3. Informar si cuenta con un sitio redundante (alterno) y señalar lo siguiente:
   a. El tipo de sitio (caliente, tibio o frío);
      No
   b. Si el sitio es propio o subcontratado con un tercero;
      No
   c. Los procedimientos, el equipo y el personal que designa para poner en marcha tal sitio
      No
   d. Tiempo que le lleva poner en marcha el sitio, según las pruebas de eficiencia.
      No aplica

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**	
Recurso*	**Descripción***	**Control***
Penetration Testin Kit (PTK)	Se trata de una extensión del navegador que esta diseñada para probar la posible vulnerabilidad en el sistema	Genera un registro de tráfico detallado permite repetir una solicitud en el R-Builder o enviarla para atacar al R-Attacker y ejecutar inyecciones de comandos XSS, SQL o OS en cualquier solicitud en particular. Versión 6.1.5
Google Analytics	Te permite hacer un seguimiento de sitios web, blogs y redes sociales. Además, pone a tu disposición informes predeterminados y personalizables.	Podemos analizar el tráfico que esta generando nuestro sistema y que secciones están generando mayor impacto, así como diferentes estadísticas que van desde la recopilación del dispositivo de conexión, hasta el tiempo de conexión en nuestro sitio.

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 299 de 425—

JMeter	Es una herramienta de carga para llevar a cabo simulaciones sobre cualquier recurso de Software.	Inicialmente diseñada para pruebas de estrés en aplicaciones web, hoy en día, su arquitectura ha evolucionado no sólo para llevar a cabo pruebas en componentes habilitados en Internet (HTTP), sino además en Bases de Datos, programas en Perl , requisiciones FTP y prácticamente cualquier otro medio.

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1)*	**Registro de la Presea Bernardo Quintana Arrioja**	
Medida de seguridad*	**Procedimiento***	**Responsable***
DDoS.	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Inyección SQL	Realizar prueba con PKT	Pedro Benítez Mejía, 1 día.
Prueba de Carga	Jmeter	Pedro Benítez Mejía, 1 día.

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1)*	**Registro de la Presea Bernardo Quintana Arrioja**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
DDoS.	Cumple con los requisitos.	Pedro Benítez Mejía, 1 día.
Inyección SQL	Cumple con los requisitos	Pedro Benítez Mejía, 1 día.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —300 de 425—

Prueba de Carga	Probado para 500 peticiones durante 1 hora, permanece estable.	Pedro Benítez Mejía, 1 día.

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa, Dirección de Apoyo Técnico		
Identificador único*	502 62 02	
(Nombre del sistema A1) *	**Registro de la Presea Bernardo Quintana Arrioja**	
Medida de seguridad*	**Acciones***	**Responsable***
Realizar pruebas de estrés en el sistema	Revisar cuantos usuarios pueden interactuar en el sistema.	Pedro Benítez Mejía, 2 días
Realizar pruebas de escalabilidad	Que mejoras pueden implementarse al sistema	Pedro Benítez Mejía, 1 semana
Realizar test de resistencia	Se realizan simulaciones de peticiones, relacionando la cantidad de peticiones con las localidades de posible impacto.	Pedro Benítez Mejía, 1 semana

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

8.2. Ass

8.3. Asd

8.4. addf

9. Mejora continua
10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales
11. Aprobación del documento de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —301 de 425—

Centro de Orientación Educativa (COE)

Instrumento Manual de Evaluación Psicológica en línea MEPSI.

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE DAT MEPSI 01**
(Nombre del sistema A1) *	**MEPSI en Línea**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de Identificación** • Nombre • Correo electrónico • Fecha de nacimiento • Nacionalidad • Sexo **Datos de Académicos** • Trayectoria educativa • Número de cuenta
Responsable*:	DGTIC, Departamento de Instrumentos, DGOAE y Dirección de Apoyo técnico, DGOAE
Nombre*:	**Lic. José Antonio Sánchez Yllanez**
Cargo*:	**Director de Apoyo Técnico de la DGOAE**
Funciones*:	Responsable del cuidado de datos personales en los sistemas desarrollados por su área de trabajo.
Obligaciones*:	Verificar y ver que se cumplan los protocolos para el cumplimiento de los derechos ARCOP en los sistemas desarrollados en la Dirección de Apoyo Técnico.
	Encargados[2]:
(Nombre del Encargado 1*)	**M. en C. Pedro Xavier Contla Romero**
Cargo*:	**Técnico Académico Titular "A"**
Funciones*:	Desarrollo y automatización de sistemas web para la DGOAE
Obligaciones*:	Diseño, Desarrollo, Implementación, mantenimiento y Actualización de Sistemas web en la DGOAE.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —302 de 425—

(Nombre del Encargado 2*)	**Lic. Alejandro Garrido Hernández**
Cargo*:	**Jefe de Departamento de Instrumentos de Orientación, DGOAE**
Funciones*:	Coordinar la aplicación de instrumentos.
Obligaciones*:	Coordinar la aplicación de instrumentos de orientación vocacional a alumnos de bachillerato UNAM y de escuelas incorporadas. Coordinar y aplicar pruebas psicológicas a aspirantes de posgrado de la UNAM evaluación de ferias y exposiciones organizadas por la DGOAE. Actualizar los instrumentos.
	Usuarios:
(Nombre del Usuario 1*)	Lic. Alejandro Garrido Hernández
Cargo*:	Jefe de Departamento de Instrumentos de Orientación, DGOAE
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de alumnos, Envío de información,
(Nombre del Usuario 2*)	M. en C. Pedro Xavier Contla Romero
Cargo*:	Técnico Académico Titular "A"
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de usuarios y alumnos, envío de información, actualización de datos personales, académicos.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único*	DGOAE_DAT_MEPSI_01
(Nombre del sistema A1*)	MEPSI en Línea
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de datos relacional, hojas de cálculo
Características del lugar donde se resguardan los soportes: *	• El alojamiento del sistema Portal de Orientación Educativa se encuentra en los servidores de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Toda comunicación con el sitio web está asegurado por el protocolo HTTPS para que la información viaje encriptada en la red. • Los datos se encuentran resguardados en bases de datos de MySQL que solamente tiene acceso el encargado M. en C. Xavier Contla. • La conexión a al servidor se realiza mediante SSH y un conjunto de llaves privada y pública (SSH Public Key Authentication). • El acceso a estas bases de datos es por medio de un usuario y contraseña.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —303 de 425—

	• Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área. • Para el acceso al sistema es por un nombre de usuario y contraseña, las cuales se generan para cada alumno usuario del sistema.

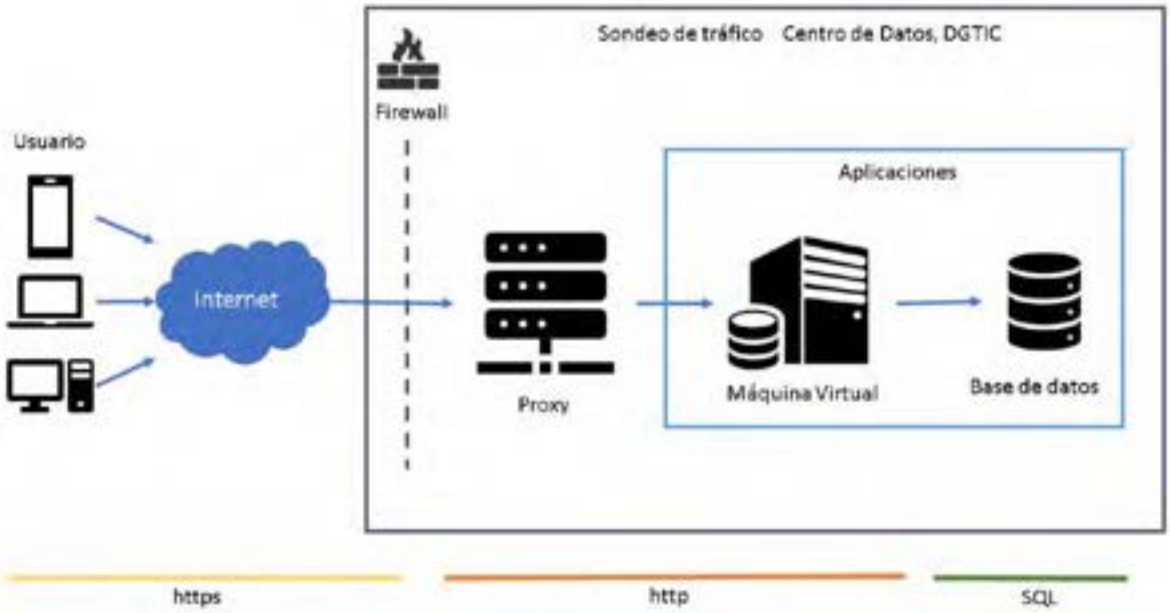


Ilustración 2 Diagrama de Seguridad

La Ilustración 1 muestra como es el acceso a la información dentro del sistema que se encuentra alojado en los servidores del Centro de Datos de DGTIC. Se tienen varios niveles de seguridad:

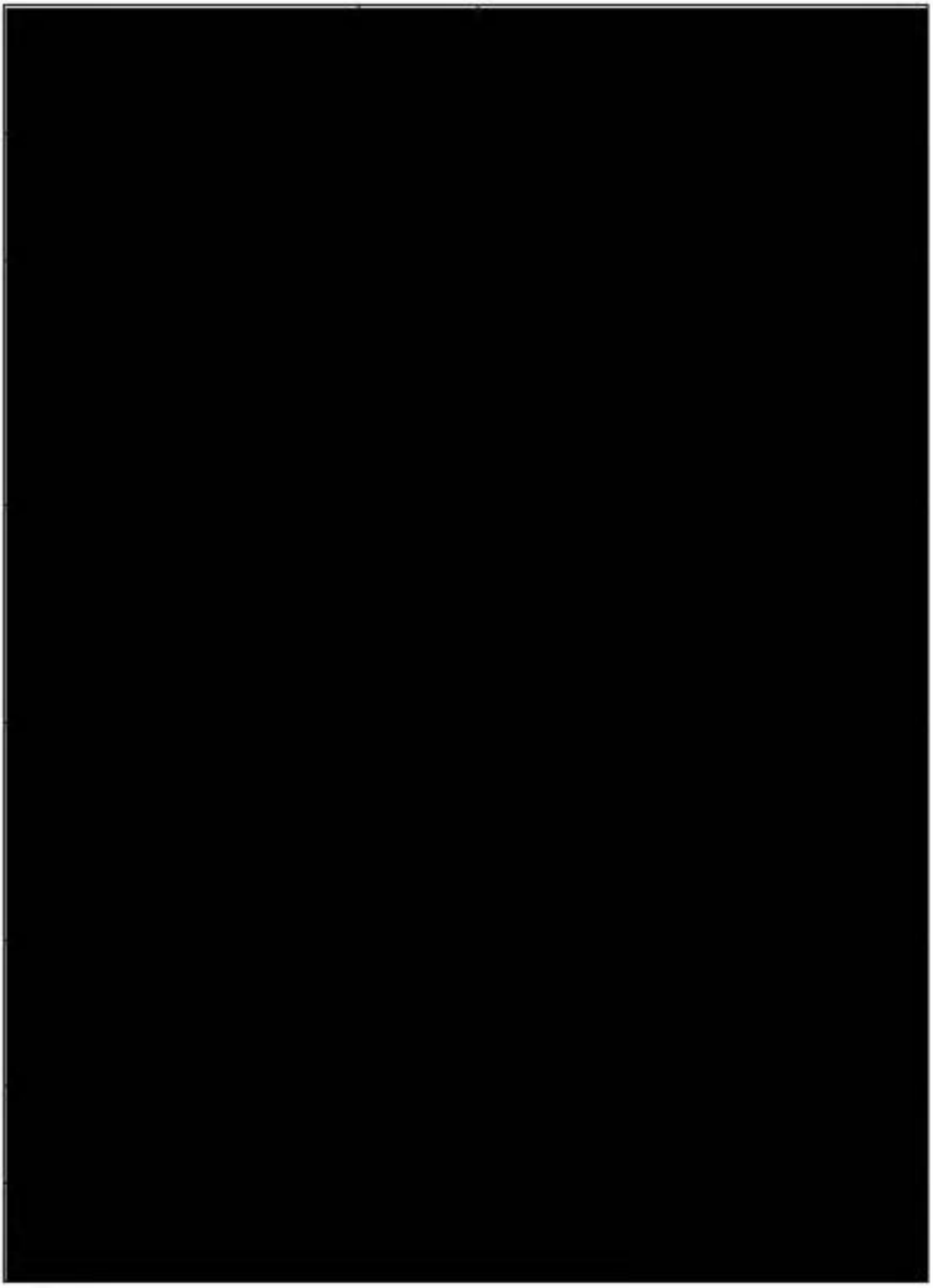
- La comunicación de un usuario con el sistema se hace mediante internet usando el protocolo de seguridad https, el cual cifra los datos que viajan en internet y solamente los puede leer el sistema.
- Dentro del Centro de datos, existe in firewall para monitorear la red entrante y saliente y decide su permite o bloquea el tráfico en función de un conjunto definido de reglas.
- Si los datos son seguros pasa a través de un proxy el cual, no solo realiza la tarea de balancear la carga a los servidores si no, es el punto de inicio a la conexión de la aplicación.
- El usuario que quiere usar la aplicación tiene un nombre de usuario y contraseña para poder acceder al aplicativo.
- Cada usuario tiene un perfil el cual tiene permisos específicos para acceder a la información de datos personales.
- Al pedir alguna información que se encuentra dentro de la base de datos, el sistema tiene un usuario y contraseña único para acceder a la información.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —304 de 425—

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT MEPSI 01**	
(Nombre del sistema A1) *	**MEPSI en Línea**	
Riesgo*	**Impacto ***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 305 de 425—



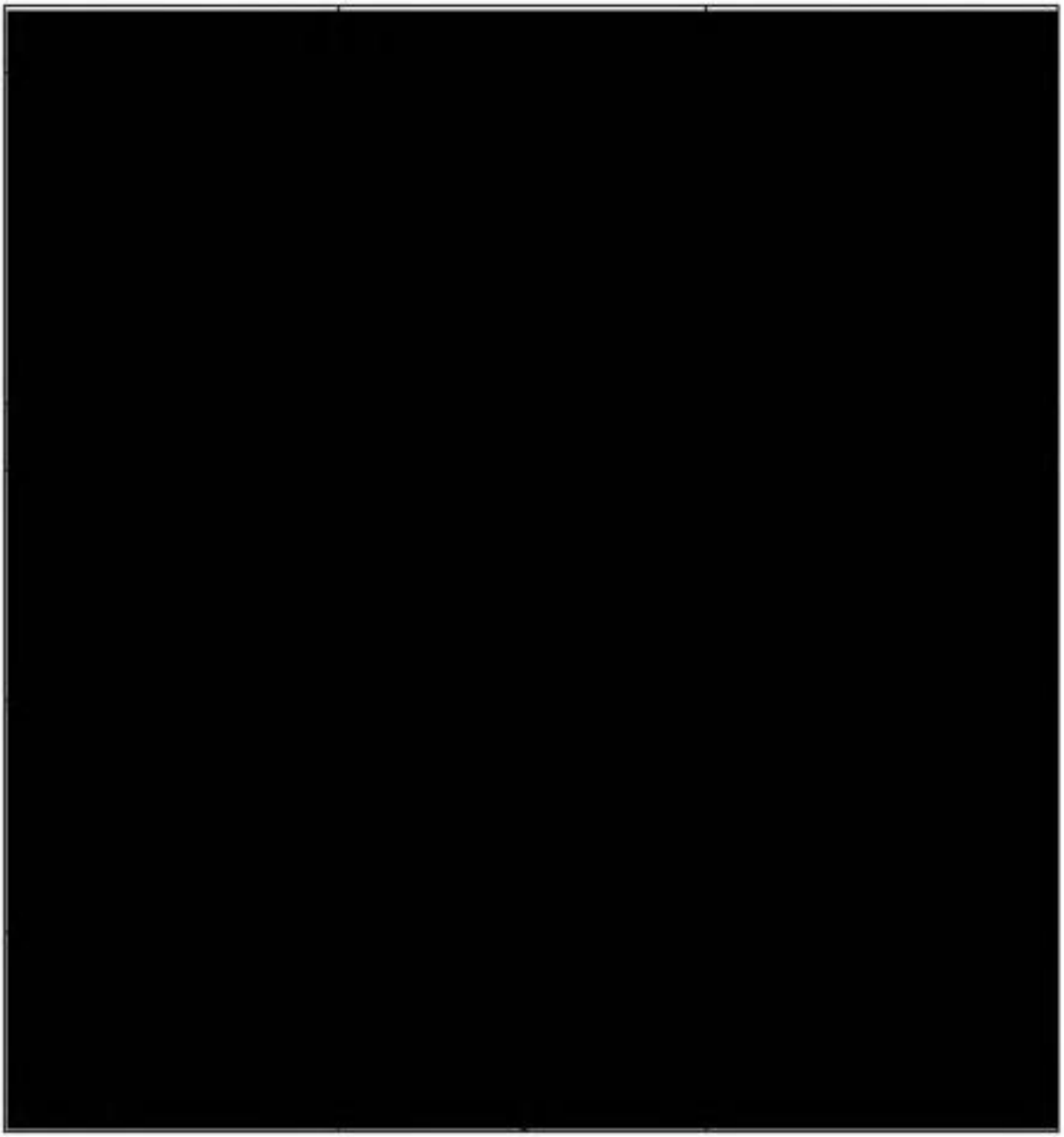
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —306 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	DGOAE DAT MEPSI 01	
(Nombre del sistema A1) *	**MEPSI en Línea**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

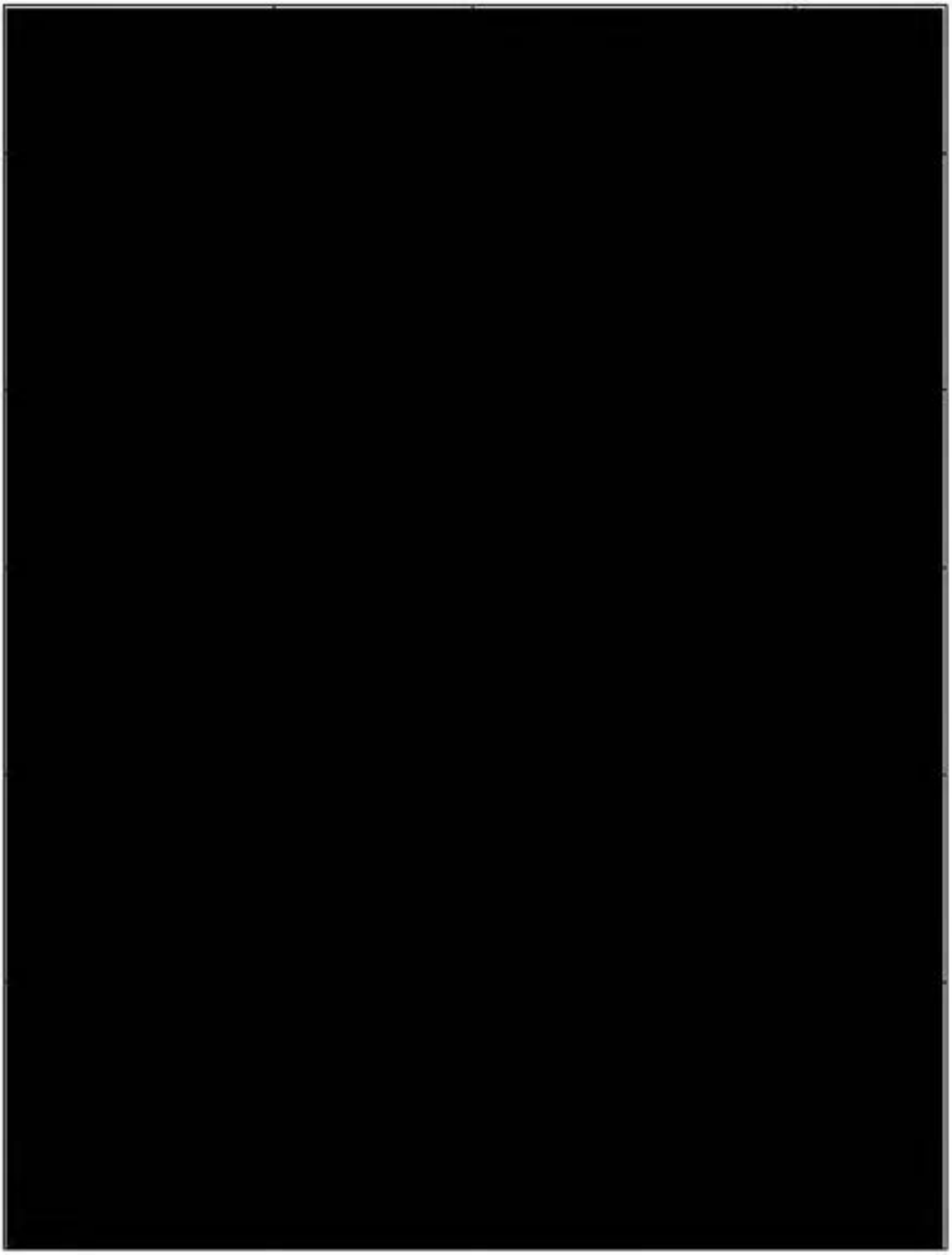
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —307 de 425—



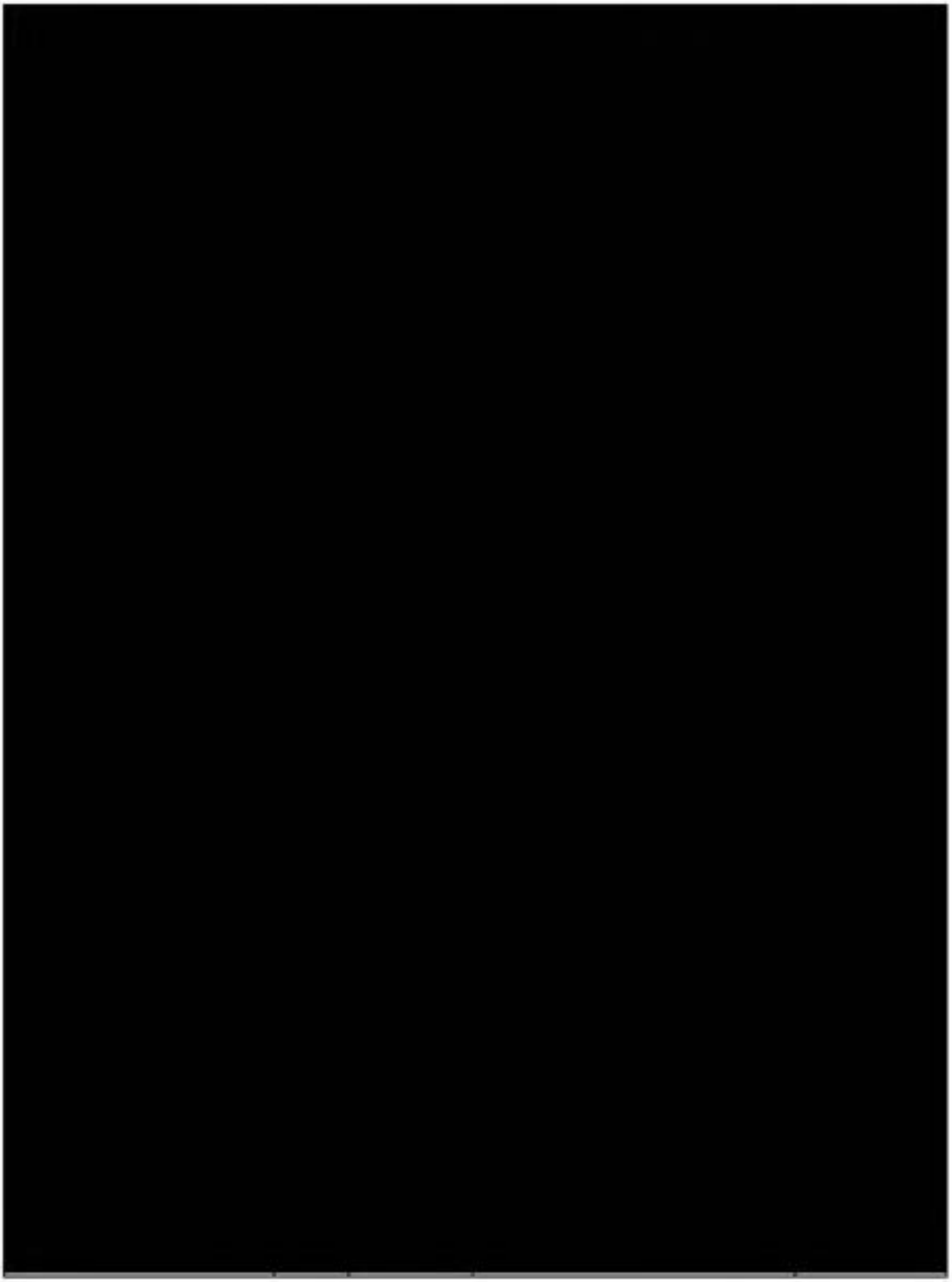
5. Plan de trabajo

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	DGOAE_DAT_MEPSI_01		
(Nombre del sistema A1) *	MEPSI en Línea		
Actividad*	Descripción*	Duración*	Cobertura*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —308 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —309 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 310 de 425—

6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE DAT MEPSI 01**
(Nombre del sistema A1) *	**MEPSI en Línea**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	• Por el momento no hay soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	• Por el momento no hay traslado por soporte electrónico físico.
Transferencias mediante el traslado sobre redes electrónicas:	• Los traslados se deberán de realizar mediante el uso de correos institucionales. • Tener una lista con los correos institucionales a los cuales se les comparte los datos personales. • Todos los archivos que contengan datos personales deberán de ser cifrados para el envío de información. • Se usará una contraseña que debe de ser personal e intransferible para cada encargado. • En el caso requerido las transferencias se formalizarán mediante algún instrumento jurídico. • Cualquier documento que contenga datos personales y que sea impreso, solamente se le podrá entregar al titular de estos datos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica para este sistema.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —311 de 425—

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras actualmente:

I. El área responsable del tratamiento de datos personales en el sistema de MEPSI en línea realiza las siguientes acciones con respecto a las bitácoras en sistema.
   a. El administrador del servidor y DGTIC pueden acceder a las bitácoras
   b. La bitácora se encuentra en soportes electrónicos
   c. La bitácora guarda la siguiente información
      i. Fecha y hora
      ii. Función que se llamó
      iii. Llamada a SQL que se realizó a la base de datos
         1. Ver
         2. Insertar
         3. Actualizar
         4. Borrar
   d. El sistema guarda un registro de las operaciones que se hacen a la base de datos.
   e. Guarda un registro de las operaciones fallidas.
   f. Cada mes se borran las bitácoras que se generan por espacio.
   g. No se crean respaldos de las bitácoras.
   h. Las bitácoras contienen fecha, hora, acción que se realizó y mensaje.
   i. Las bitácoras van a tener una duración de 1 mes en sistema y se creará una copia que se resguardará en algún medio de almacenamiento durante dos años.

II. Con los nuevos requisitos se va a implementar el siguiente sistema de bitácoras.
   a. Se actualizarán la información que se guarda en la bitácora como sigue:
      i. Los datos que guardará
         - Fecha y hora
         - Función SQL y que realizó (Lectura, escritura, inserción)
         - El id de usuario que hizo la acción
         - Los privilegios del usuario
      ii. Estas bitácoras se van a respaldar cada mes y se guardarán por un periodo de dos años en soportes electrónicos.
   b. Se crearán tablas en la base de datos que guarden el registro de actividad por usuario que tenga acceso a datos personales y seguirá el siguiente protocolo:
      i. Los datos que guardará
         - Fecha y hora
         - Función SQL y que realizó (Lectura, escritura, inserción)
         - El id de usuario que hizo la acción
         - Los privilegios del usuario
      ii. Estas tablas que contienen el registro de actividades se respaldarán cada mes y deben de quedarse al menos 4 años resguardadas en soportes electrónicos.

IV. REGISTRO DE INCIDENTES:

En caso de presentar un incidente seguir los siguientes pasos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —312 de 425—

8. Resolver el incidente
9. Pedir el archivo en formato electrónico "Registro de incidentes de datos personales" (pdf).
10. Recopilar la siguiente información:
    a. Resumen del incidente
    b. Resumen de cómo se solucionó el incidente
    c. Especificar si el incidente daño algún archivo, base de datos, servidor, respaldo etc.
    d. Fecha de inicio
    e. Fecha de término o resolución del incidente
    f. El impacto del incidente
    g. La persona quien resolvió el incidente
    h. Nombre del responsable y firma
11. El archivo de registro se actualiza y se crea un respaldo en un soporte electrónico portable para su almacenamiento.
12. La resolución del incidente tiene un tiempo máximo de 3 días hábiles.
13. El encargado de sistema deberá de registrar el incidente en un archivo donde se encuentre el resumen de lo sucedido.
14. Si el incidente es un robo o extravío de información se deberá reportar inmediatamente a los encargados y responsables del sistema, ellos avisaran al titular y a los encargados en la UNAM de lo sucedido.

La recuperación de datos de los sistemas de respaldo la podrá solicitar los encargados y el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

a. Seguridad perimetral exterior

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —313 de 425—

horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

b. Seguridad perimetral interior

Para las personas que acceden a dichos espacios interiores:

Las oficinas del Centro de Orientación Especializada (COE) y Departamento de Instrumentos de Orientación se encuentran de la Dirección General de Orientación y Atención Educativa en la planta baja y alta respectivamente.

1. ¿Cómo las identifica?

   Las personas a quienes atendemos son: alumnado, egresadas y egresados de la UNAM.

2. ¿Cómo las autentifica?

   Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. ¿Cómo les autoriza el acceso?

   En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 314 de 425—

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

En el caso de que un titular identifique que sus datos personales son incorrectos, se podrá hacer un cambió si y solo si el titular sigue el siguiente protocolo:

6. Obtener y llenar el documento del ANEXO II donde el titular requiere una actualización en los datos personales.
7. Mandar al correo innovaoe@unam.mx lo siguiente:
    a. Adjuntar el documento firmado del ANEXO II en el correo electrónico,
8. El titular recibirá un correo donde se le avisará de la recepción del correo en un tiempo aproximado de 3 días hábiles.
9. Esperar el aviso dé que se realizó el cambio en los datos personales solicitados
10. Revisar que el cambió se realizó correctamente.
    a. Se tiene un tiempo de espera de 2 días hábiles para cualquier corrección de los datos que se cambiaron.
    b. SI todo es correcto, dejar como está.
    c. Si hay algún dato que no se cambió, favor de enviar el dato incorrecto con el correcto como respuesta del aviso. Y verificar nuevamente. Estos cambios se deben de realizar en menos de 12 horas.

Para los responsables y encargados de cambiar los datos, seguir el siguiente protocolo.

5. Al recibir el correo, el encargado responderá al titular:
    a. El cambio se realizará dentro de 3 días hábiles.
    b. Hay que informar que persona va a realizar el cambio, deberá ser la misma que mande la respuesta de los días hábiles.
6. Levantar un reporte de la incidencia.
7. Se realiza el cambio.
8. Se envía un correo para que el titular verifique que el cambio se hizo correctamente pidiendo que mande una respuesta si el cambio se hizo correctamente o no.
    a. Si se recibe una respuesta afirmativa, ponemos fin a la incidencia.
    b. Si se recibe un correo donde sigue la inconsistencia en los datos, revisar de nuevo la petición y hacer el cambio inmediatamente y volver a confirmar que se realizó el cambio.
    c. Si no se recibe el correo, después de dos días del envío del correo de verificación de la realización de cambios en los datos personales. Podemos poner fin a la incidencia.
    d. Si llegara la información después de los dos días hábiles el titular deberá de volver a pedir el cambio.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —315 de 425—

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
Toda comunicación con el sitio web está asegurado por el protocolo ***https*** para que la información viaje encriptada en la red.
Aplicación ***MEPSI en línea*** tiene la siguiente configuración:

1. Para acceder al sistema se cuenta con un usuario y contraseña.
2. El usuario está definido por el número de cuenta o por el correo electrónico.
3. La contraseña se genera a partir de un "dato personal".
4. La contraseña se guarda encriptada en la base de datos y se usa un método de encriptación para poder obtenerla al momento de iniciar la sesión.
5. Los perfiles de la aplicación son solo de **usuario** que solamente tiene acceso a sus datos personales y para responder el instrumento.

Contenedor de la máquina virtual tiene la siguiente configuración:

1. Se crea un perfil, usuario y contraseña para el uso de la máquina virtual
2. Se conecta a través de una IP fija o mediante SSH y un conjunto de llaves privada y pública (*SSH Public Key Authentication*).
3. El usuario tiene permiso de *root* para hacer la configuración de servidor.

Base de datos tiene la siguiente configuración:

1. El acceso a estas bases de datos es por medio de un usuario y contraseña que lo tiene el administrador.
2. El administrador de la base de datos puede crear, modificar, borrar, actualizar lo siguiente:
    a. Esquema de la base de datos
    b. Tablas
    c. Registros
    d. Hacer respaldos de la información de las bases
    e. Creación de usuarios de la base
    f. Modificación de privilegios de los usuarios

Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área.
Resumen de la verificación de perfiles de usuario y contraseñas:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —316 de 425—

1. Modelo de control de acceso:

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? **SI**
b) ¿Es discrecional (matriz de control de acceso)? **No**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Si**

2. Perfiles de usuario y contraseñas en el sistema operativo de red: NO APLICA

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **NO**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **NO APLICA**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **NO APLICA**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Si**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Se cifra la contraseña, pero no el nombre de usuario**

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? **Administrador**
b) ¿Quién autoriza la creación de nuevos perfiles? **Encargado de los Usuarios**
c) ¿Se lleva registro de la creación de nuevos perfiles? **Si**

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **NO**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **SI, solo el administrador de la base puede entrar por este medio**
c) ¿Cómo se evita el acceso remoto no autorizado? **Mediante la autenticación por llave y por IP**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos del sistema los realiza el encargado del sistema en la DGOAE.

DGOAE

1. Los respaldos se realizan manualmente y completos.
2. El respaldo se realiza cada mes
3. Si se realiza alguna aplicación del instrumento, acabando el periodo de aplicación se obtiene un respaldo manual.
4. Estos respaldos se quedan en un disco duro.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —317 de 425—

5. Los respaldos los resguarda el encargado en la Dirección de Apoyo Técnico.
6. Los respaldos se realizan de forma automática cada tercer día y guardan el estado de la máquina virtual. donde se aloja el sistema.

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.

- Tener respaldos de la base de datos y del código.
- Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
- Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
- El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
- Una vez que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
- Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una vez hecha la conexión se carga el respaldo de la base de datos.
- En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
- Realizar pruebas al sistema de inicio de sesión, cierre de sesión, registro de universitarias y universitarios, consulta del programa del Encuentro Virtual de Empleabilidad, inscripción y baja a las diferentes actividades que ofrece éste.

2. El tiempo que se demore DGTIC en darnos el nuevo espacio fue de un día, ya que se le explico que era de carácter urgente.
3. No aplica.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 318 de 425—

Dirección de Apoyo Técnico		
Identificador único*	DGOAE DAT MEPSI 01	
(Nombre del sistema A1)*	*MEPSI en Linea*	
Recurso*	**Descripción***	**Control***
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicaran el tráfico que existen en el servidor	Se hace manual y solamente será usada cuando se genere un ataque al sistema
Bitácoras generadas por el servidor	Las bitácoras generadas por el servidor nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas en la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.
Wireshark	Se hace una revisión de parte del cliente para saber qué es lo que puede ver y asegurar que los datos viajan encriptados.	Wireshark se usa para la identificación de paquetes por etiquetas TCP y IP, analizar que se envía y que se recibe.
Ambiente de pruebas	Se debe de tener una computadora donde se pueda hacer pruebas y que solamente se pueda acceder localmente o en red local.	Se tiene una computadora con Centos 7 para poder hacer las pruebas necesarias.
Nmpa, netcat, Tcpdump	Utilizar las herramientas para la detección de fallos y verificación del funcionamiento y seguridad del sistema	Las herramientas son libres y se hará una revisión cada semestre con estas herramientas

7.2 Procedimiento para la revisión de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 319 de 425—

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	DGOAE DAT MEPSI 01	
(Nombre del sistema A1)*	*MEPSI en Línea*	
Medida de seguridad*	**Procedimiento***	**Responsable***
Contar con las medidas de seguridad que DGTIC pide.	Se seguirán las recomendaciones que DGTIC propone para la seguridad en los sistemas	Administrador del Sistema 28 días laborables
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones	Administrador del Sistema 5 días laborables
Lista de verificación de seguridad	Diseñar un documento donde llevemos una lista de verificación sobre las reglas de seguridad que debe de tener el sistema	Administrador del Sistema 28 días laborables

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	DGOAE DAT MEPSI 01	
(Nombre del sistema A1) *	*MEPSI en Línea*	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Se deberá de mandar la aplicación al CERT en DGTIC para la evaluación del sistema	I. Ausencia de encabezados de seguridad II. Envío de Credenciales en texto claro	Pedro Xavier Contla Romero 4 de abril de 2019

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —320 de 425—

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE DAT MEPSI 01**	
(Nombre del sistema A1)*	**MEPSI en línea**	
Medida de seguridad*	**Acciones***	**Responsable***
Se resolvieron los diferentes riesgos de seguridad según el reporte de DGTIC	I. Se implementó la sobreescritura de cabeceras II. Se implementó el certificado de Let's Encrypt.	Pedro Xavier Contla Romero 15 de abril del 2019

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT MEPSI 01**		
(Nombre del sistema A1)*	**MEPSI en línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son	Duración: Un día Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —321 de 425—

	vulnerables, cual es el impacto, etc.		tenga acceso a los datos personales.
Resguardo de información mediante los protocolos antes establecidos	Contar con un documento donde explique los objetivos principales de la implementación de la seguridad para el sistema	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Programación de los sistemas usando framework seguros	Estar actualizando las herramientas de desarrollo conforme avanza la tecnología	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores que actualicen los sistemas tendrán que buscar si lo que se usa es seguro para el resguardo de los datos personales. Cada año generar el análisis sobre la tecnología que se usa.
****Pruebas de obtención de datos mediante perfiles***	Realizar pruebas sobre los diferentes perfiles en el sistema	Duración: una semana Inicio: Por definir Termino: Por definir	Contar con el análisis de los perfiles y sus privilegios del sistema Al incorporar un nuevo perfil al sistema
Creación de Certificados SSL	Contar con un documento en donde se documente como generar in certificado SSL por medio de Let's Encrypt	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores podrán contar con un método para generar sus certificados mientras se obtiene el principal. Al incorporar un nuevo desarrollador al equipo
Curso de protección a las máquinas virtuales	Contar con un curso de administrador tipo Linux para capacitar a nuevos administradores sobre la configuración en el servidor	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Curso de hacker ético para pruebas en el sistema	Contar con un curso para probar	Duración: un mes Inicio: Por definir	Los desarrolladores y administradores del servidor y base de datos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —322 de 425—

	los sistemas en desarrollo.	Termino: Por definir	Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Protocolo interno para verificación de la seguridad	Contar con un documento que indique los pasos que se deben llevar para probar la seguridad de los sistemas	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Antes de salir a producción. *

Nota: La capacitación se realiza cuando los usuarios aumenten, por lo que las fechas no están definidas. Por el momento los que usan el sistema ya están capacitados

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT MEPSI 01**		
(Nombre del sistema A1) *	**MEPSI en línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso integral dentro de la DGOAE	*La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.*	*Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.*	*Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.*
Aviso particular del área responsable del dar el servicio por medio del sistema	*La distribución es en la página del sistema y está al alcance en dos lugares.* *Si existe registro, antes de darle aceptar.* *Si ya están registrados, donde se despliegan los datos personales.*	*Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.*	*Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —323 de 425—

Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	*LA distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.*	Duración: permanente Inicio: Por definir Termino: Por definir	*Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —324 de 425—

9. Mejora continua

9.1.Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT MEPSI 01**		
(Nombre del sistema A1) *	**MEPSI en Línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Análisis de los reportes de los usuarios acerca de los bugs, mal funcionamiento y documentación sobre el funcionamiento del sistema.	*Contar con la información necesaria para evaluar los puntos en donde se necesita hacer una actualización del sistema.*	Duración: dos semanas Inicio: Por definir Termino: Por definir	*Actualización y mejora del sistema actual, parcialmente.*
Actualización de mensajes de error y éxito.	*Agregar unas respuestas en para el Módulo de los Administradores para que tenga una mejor retroalimentación de las*	*Duración: un mes* *Inicio: Por definir* *Termino: Por definir*	*Mejor retroalimentación a los administradores para el uso de las funcionalidades del sistema.*

	modificaciones o borrado que se realiza.		
Pantallas de verificación	*Agregar pantallas antes de realizar algún cambio para evitar modificaciones no deseadas.*	*Duración: un mes* *Inicio: Por definir* *Termino: Por definir*	*Total*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —325 de 425—

9.2.Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT MEPSI 01**		
(Nombre del sistema A1) *	**MEPSI en Línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en que estado se encuentran*	Duración: Cada año Inicio: Por definir Termino: Por definir	*Total*
Actualizar o cambiar los equipos de desarrollo lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: 1 mes Inicio: Por definir Termino: Por definir	*Total*

9.3.Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE_DAT_MEPSI_01**	
(Nombre del sistema A1)*	**MEPSI en línea**	
Proceso*	**Descripción***	**Responsable***
Respaldo en soporte electrónico de la base de datos	1. *Realizar un respaldo de la base de datos.* 2. *El nombre del archivo respaldo es nombre de la base y la fecha cuando se realizó el respaldo* 3. *Guardarlo en la carpeta donde se encuentran los demás respaldos.*	*Administrador de la base de datos* *3 días.*
Respaldo en soporte electrónico portable (usb, disco duro, CD-R) de la base de datos	1. *Copiar los respaldos que se encuentran en la carpeta a soportes electrónicos portables para el resguardo de la información.*	*Administrador de la base de datos* *1 días.*
Respaldo de los archivos de reporte que contenga datos personales	1. *Generar los reportes que serán enviados a las diferentes dependencias.* 2. *Comprimir los reportes en un archivo con el nombre de la dependencia y la fecha cuando se generaron los reportes.* 3. *Guardar el archivo en un soporte electrónico.* 4. *Pedir al área de sistemas el soporte electrónico portable donde se va a guardar el archivo comprimido.* 5. *Guardar el archivo en un soporte electrónico portable.* 6. *Enviar el soporte electrónico portable al área de sistemas para su resguardo.*	*Encargado de traslado de reportes.* *3 días.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 326 de 425—

9.4.Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT MEPSI 01**		
(Nombre del sistema A1) *	**MEPSI en Línea**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en que estado se encuentran*	Duración: Cada año Inicio: Por definir Termino: Por definir	*Total*
Actualizar o cambiar los equipos de desarrollo lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: 1 mes Inicio: Por definir Termino: Por definir	*Total*

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A. DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

- La Dirección de Apoyo Técnico y la Coordinación de Orientación Educativa acordarán la cancelación del sistema mediante un escrito donde indique lo siguiente:
  a. Fecha cuando deja de dar servicio el sistema
  b. Fecha de cancelación de sistema
     Estas fechas al menos deben de tener un mes de separación.
  c. Motivo de la cancelación
  d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —327 de 425—

B. PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

8. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
9. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
10. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
11. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
12. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
13. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
14. Bajar del servidor el sistema para que no pueda ser visto por red.

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C. Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)
En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —328 de 425—

- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D. PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)
Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Portal de Orientación Educativa que se encuentren dentro sistema.

E. MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Con respecto a los discos duros, cualquier software que realice un borrado de bajo nivel. Los métodos de borrado que evitan que se pueda recuperar los datos de los dispositivos de almacenamiento una vez se han eliminado son la desmagnetización, la destrucción y la sobreescritura.
La desmagnetización y la destrucción física no permiten reutilizar el dispositivo posteriormente. En la desmagnetización se expone el soporte a un campo magnético con una potencia que variará en función del tamaño del dispositivo, mientras que en la destrucción física se elimina el soporte físicamente por completo siendo imposible su reutilización. Sin embargo, el método de sobreescritura elimina la información sin que ésta pueda ser recuperada y permite volver a utilizar el dispositivo con garantías de que funcione correctamente.
Esta forma de borrado se utiliza por ejemplo en los casos en los que se pretende donar los ordenadores antiguos de una empresa, y se desea tener la seguridad de que toda la información eliminada es irrecuperable
(https://www.incibe.es/protege-tu-empresa/blog/borrar-informacion-dispositivo-ciberseguridad).
Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización.

Instrumento PROUNAM II e INVOCA en línea.

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —329 de 425—

Dirección de Apoyo Técnico	
Identificador único*	**DGOAE DAT POE 01**
(Nombre del sistema B1) *	**Portal de Orientación Educativa**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de Identificación** • Nombre • Correo electrónico • Fecha de nacimiento • Sexo **Datos de Académicos** • Escuela / Facultad • Número de cuenta • Semestre • Grupo **Datos Sociodemográficos** • Años de cursar la secundaria • Promedio de Secundaria • Promedio Actual • Materias Reprobadas • Área del conocimiento • Bienes • Número de focos • Número de cuartos en casas • Número de personas que viven en casa • Ingreso familiar • Escolaridad Padre • Escolaridad Madre
Responsable*:	DGTIC, Departamento de Instrumentos, DGOAE y Dirección de Apoyo técnico, DGOAE
Nombre*:	**Lic. José Antonio Sánchez Yllanez**
Cargo*:	**Director de Apoyo Técnico de la DGOAE**
Funciones*:	Responsable del cuidado de datos personales en los sistemas desarrollados por su área de trabajo.
Obligaciones*:	Verificar y ver que se cumplan los protocolos para el cumplimiento de los derechos ARCOP en los sistemas desarrollados en la Dirección de Apoyo Técnico.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 330 de 425—

	Encargados[3]:
(Nombre del Encargado 1*)	**M. en C. Pedro Xavier Contla Romero**
Cargo*:	**Técnico Académico Titular "A"**
Funciones*:	Desarrollo y automatización de sistemas web para la DGOAE
Obligaciones*:	Diseño, Desarrollo, Implementación, mantenimiento y Actualización de Sistemas web en la DGOAE.
(Nombre del Encargado 2*)	**Lic. Alejandro Garrido Hernández**
Cargo*:	**Jefe de Departamento de Instrumentos de Orientación, DGOAE**
Funciones*:	Coordinar la aplicación de instrumentos.
Obligaciones*:	Coordinar la aplicación de instrumentos de orientación vocacional a alumnos de bachillerato UNAM y de escuelas incorporadas. Coordinar y aplicar pruebas psicológicas a aspirantes de posgrado de la UNAM evaluación de ferias y exposiciones organizadas por la DGOAE. Actualizar los instrumentos.
	Usuarios:
(Nombre del Usuario 1*)	Lic. Alejandro Garrido Hernández
Cargo*:	Jefe de Departamento de Instrumentos de Orientación, DGOAE
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de alumnos, envío de información, actualización de datos personales, académicos.
(Nombre del Usuario 2*)	M. en C. Pedro Xavier Contla Romero
Cargo*:	Técnico Académico Titular "A"
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de usuarios y alumnos, envío de información, actualización de datos personales, académicos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —331 de 425—

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único**	DGOAE_DAT_POE_01
(Nombre del sistema B1*)	Portal de Orientación Educativa
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de datos relacional, hojas de cálculo
Características del lugar donde se resguardan los soportes: *	• El alojamiento del sistema Portal de Orientación Educativa se encuentra en los servidores de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Toda comunicación con el sitio web está asegurado por el protocolo HTTPS para que la información viaje encriptada en la red. • Los datos se encuentran resguardados en bases de datos de MySQL que solamente tiene acceso el encargado M. en C. Xavier Contla. • La conexión a al servidor se realiza mediante SSH y un conjunto de llaves privada y pública (SSH Public Key Authentication). • El acceso a estas bases de datos es por medio de un usuario y contraseña. • Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área. • Para el acceso al sistema es por un nombre de usuario y contraseña, las cuales se generan para cada alumno usuario del sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 332 de 425—

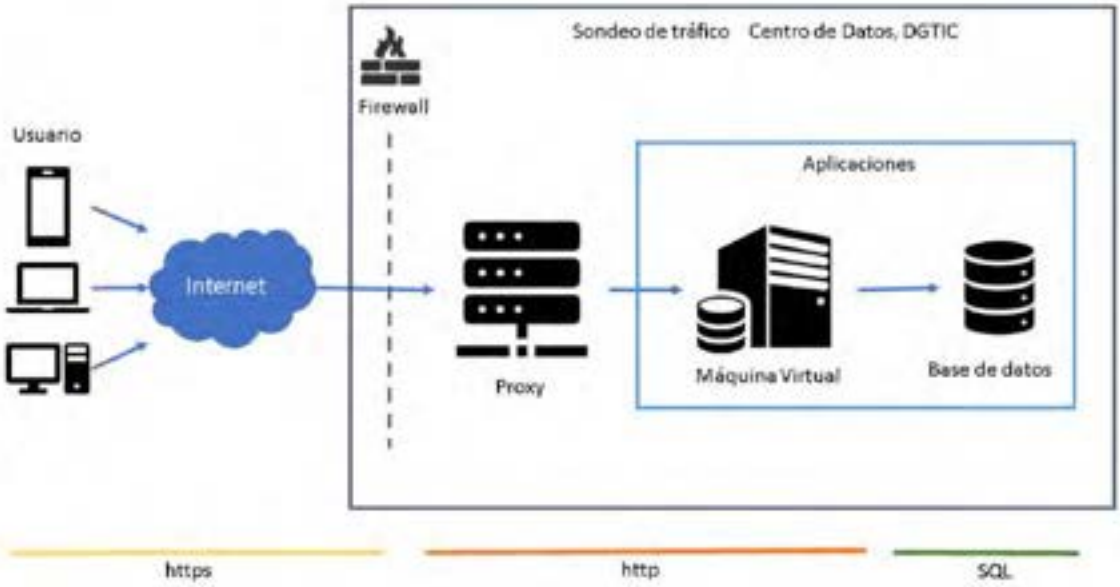


Ilustración 3. Diagrama de Seguridad

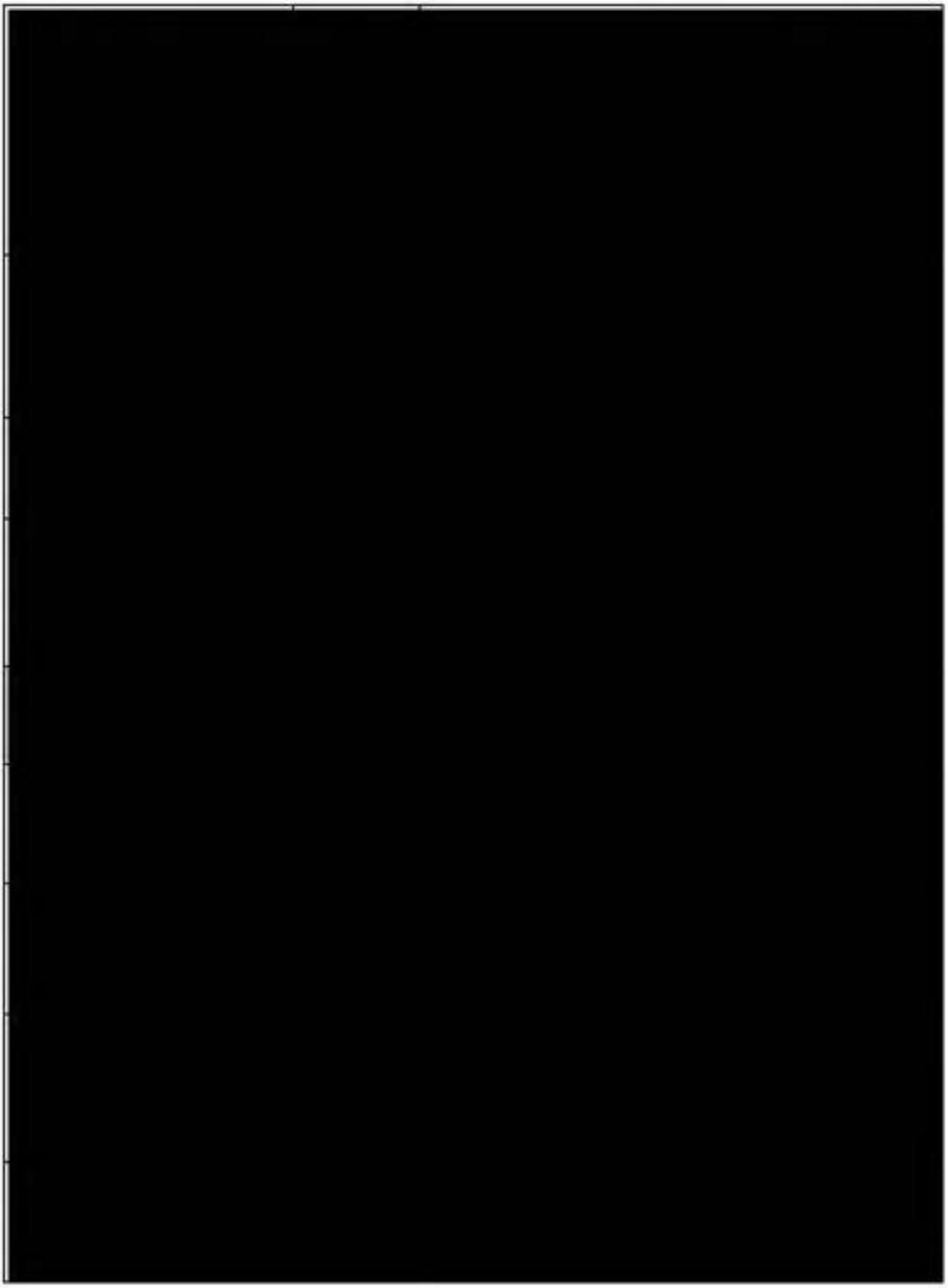
La Ilustración 1 muestra como es el acceso a la información dentro del sistema que se encuentra alojado en los servidores del Centro de Datos de DGTIC. Se tienen varios niveles de seguridad:

- La comunicación de un usuario con el sistema se hace mediante internet usando el protocolo de seguridad https, el cual cifra los datos que viajan en internet y solamente los puede leer el sistema.
- Dentro del Centro de datos, existe in firewall para monitorear la red entrante y saliente y decide su permite o bloquea el tráfico en función de un conjunto definido de reglas.
- Si los datos son seguros pasa a través de un proxy el cual, no solo realiza la tarea de balancear la carga a los servidores si no, es el punto de inicio a la conexión de la aplicación.
- El usuario que quiere usar la aplicación tiene un nombre de usuario y contraseña para poder acceder al aplicativo.
- Cada usuario tiene un perfil el cual tiene permisos específicos para acceder a la información de datos personales.
- Al pedir alguna información que se encuentra dentro de la base de datos, el sistema tiene un usuario y contraseña único para acceder a la información.

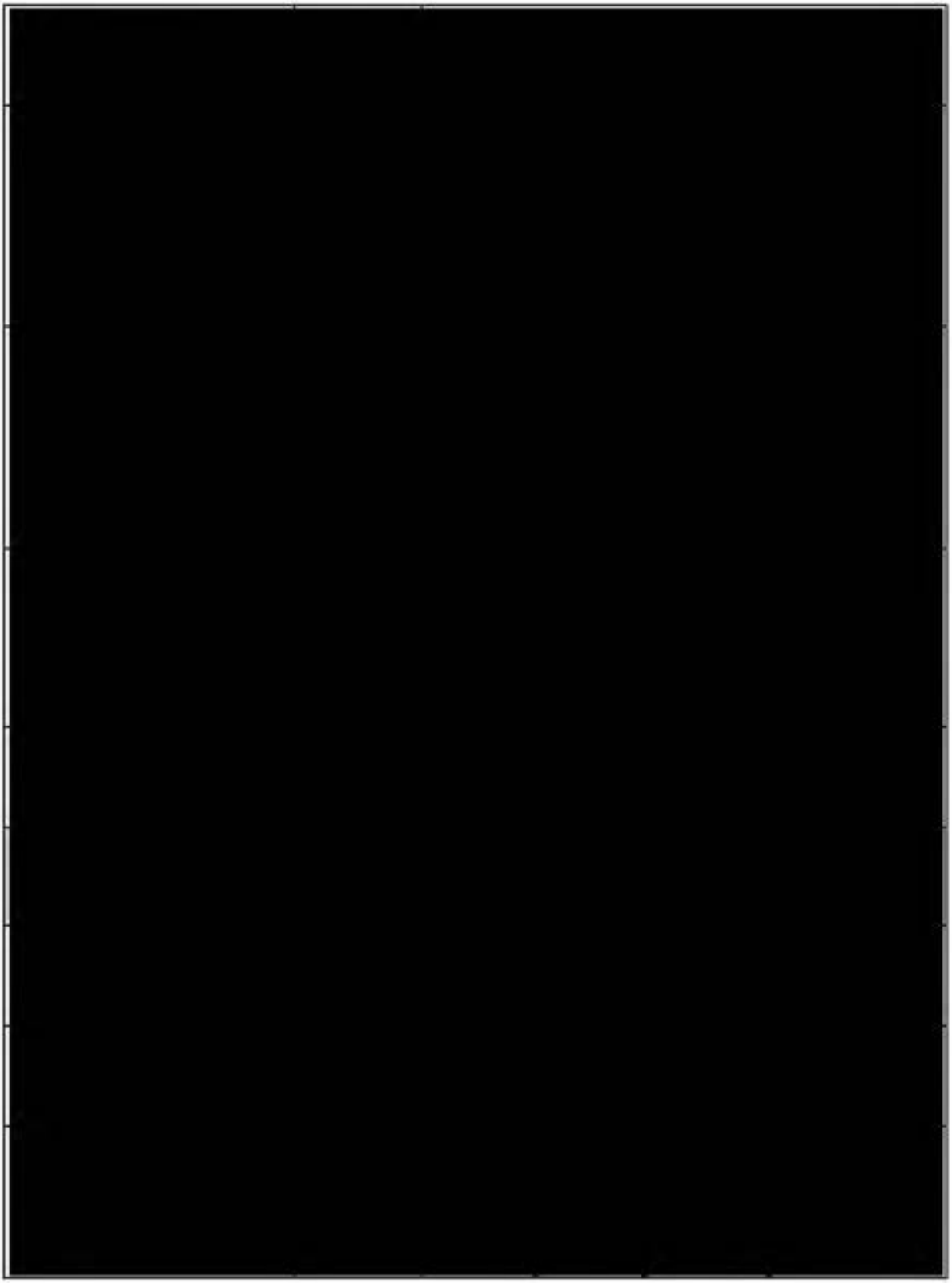
3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE DAT POE 01**	
(Nombre del sistema B1) *	**Portal de Orientación Educativa**	
Riesgo*	**Impacto***	**Mitigación***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 333 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —334 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 335 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE_DAT_POE_01**	
(Nombre del sistema B1)*	**Portal de Orientación Educativa**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

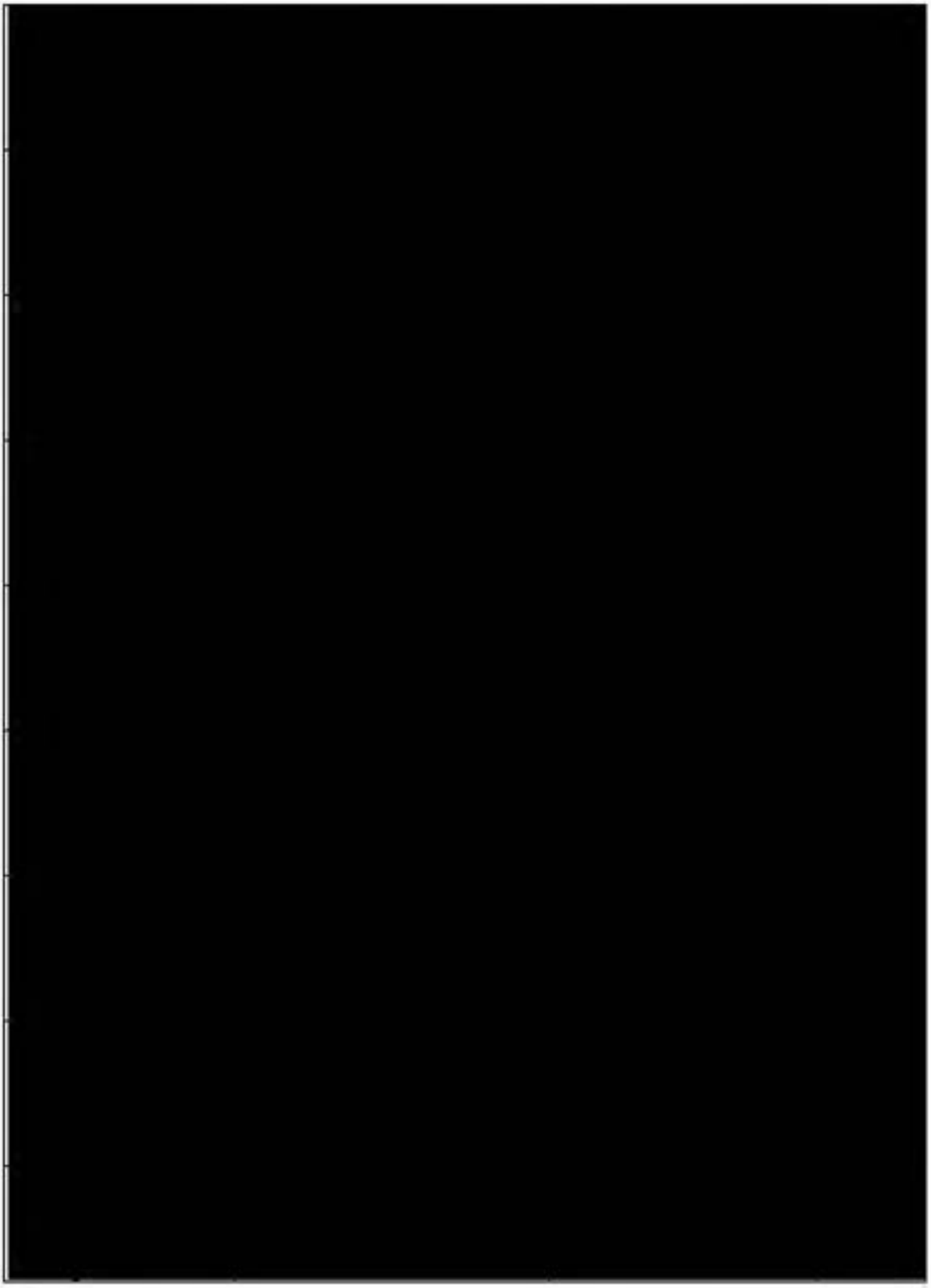
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud5=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 336 de 425—



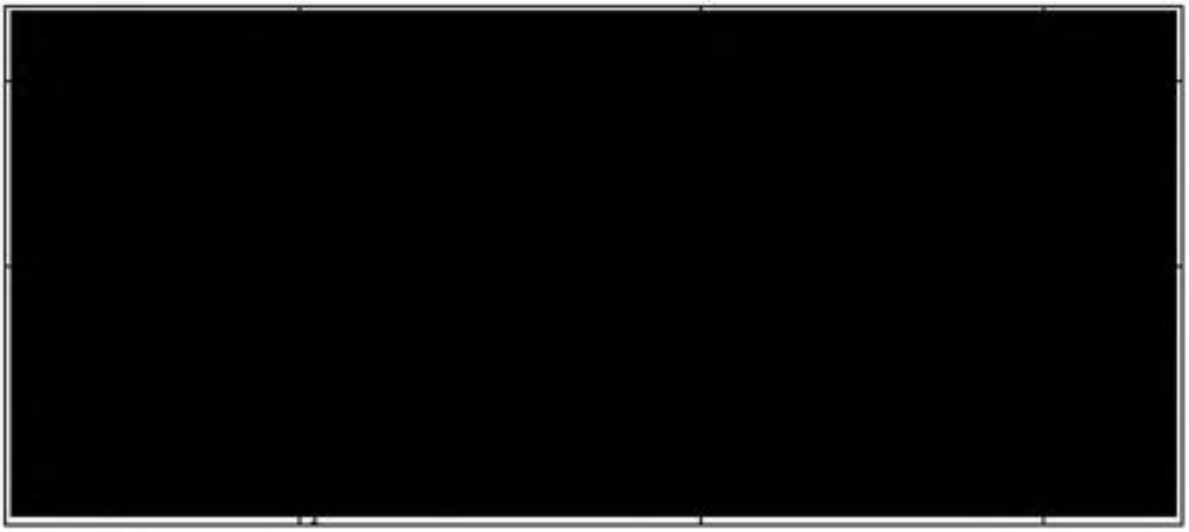
5. Plan de trabajo

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	DGOAE_DAT_POE_01		
(Nombre del sistema B1) *	Portal de Orientación Educativa		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 337 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 338 de 425—



6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE_DAT_POE_01**
(Nombre del sistema B1) *	**Portal de Orientación Educativa**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	• Por el momento no hay soporte físico.
Transferencias mediante el traslado de soportes electrónicos:	• Por el momento no hay traslado por soporte electrónico físico.
Transferencias mediante el traslado sobre redes electrónicas:	• Los traslados se deberán de realizar mediante el uso de correos institucionales. • Tener una lista con los correos institucionales a los cuales se les comparte los datos personales. • Todos los archivos que contengan datos personales deberán de ser cifrados para el envío de información. • Se usará una contraseña que debe de ser personal e intransferible para cada encargado. • En el caso requerido las transferencias se formalizarán mediante algún instrumento jurídico.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 339 de 425—

	• Cualquier documento que contenga datos personales y que sea impreso, solamente se le podrá entregar al titular de estos datos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica para este sistema.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras actualmente:

I. El área responsable del tratamiento de datos personales en el sistema de Portal de Orientación Educativa realiza las siguientes acciones con respecto a las bitácoras en sistema.

a. El administrador del servidor y DGTIC pueden acceder a las bitácoras
b. La bitácora se encuentra en soportes electrónicos
c. La bitácora guarda la siguiente información
   i. Fecha y hora
   ii. Función que se llamó
   iii. Llamada a SQL que se realizó a la base de datos
      1. Ver
      2. Insertar

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 340 de 425—

3. Actualizar
4. Borrar

d. El sistema guarda un registro de las operaciones que se hacen a la base de datos.
e. Guarda un registro de las operaciones fallidas.
f. Las bitácoras contienen fecha, hora, acción que se realizó y mensaje.
g. Las bitácoras van a tener una duración de 1 mes en sistema y se creará una copia que se resguardará en algún medio de almacenamiento durante dos años.

II. Con los nuevos requisitos se va a implementar el siguiente sistema de bitácoras.

a. Se actualizarán la información que se guarda en la bitácora como sigue:
   i. Los datos que guardará
      - Fecha y hora
      - Función SQL y que realizó (Lectura, escritura, inserción)
      - El id de usuario que hizo la acción
      - Los privilegios del usuario

   ii. Estas bitácoras se van a respaldar cada mes y se guardarán por un periodo de dos años en soportes electrónicos
b. Se crearán tablas en la base de datos que guarden el registro de actividad por usuario que tenga acceso a datos personales y seguirá el siguiente protocolo:
   i. Los datos que guardará
      - Fecha y hora
      - Función SQL y que realizó (Lectura, escritura, inserción)
      - El id de usuario que hizo la acción
      - Los privilegios del usuario
   ii. Estas tablas que contienen el registro de actividades se respaldarán cada mes y deben de quedarse al menos 4 años resguardadas en soportes electrónicos.

IV. REGISTRO DE INCIDENTES

En caso de presentar un incidente seguir los siguientes pasos.

1. Resolver el incidente
2. Pedir el archivo en formato electrónico "Registro de incidentes de datos personales" (pdf).
3. Recopilar la siguiente información:
   a. Resumen del incidente
   b. Resumen de cómo se solucionó el incidente
   c. Especificar si el incidente daño algún archivo, base de datos, servidor, respaldo etc.
   d. Fecha de inicio
   e. Fecha de término o resolución del incidente
   f. El impacto del incidente

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —341 de 425—

g. La persona quien resolvió el incidente
h. Nombre del responsable y firma

4. El archivo de registro se actualiza y se crea un respaldo en un soporte electrónico portable para su almacenamiento.
5. La resolución del incidente tiene un tiempo máximo de 3 días hábiles.
6. El encargado de sistema deberá de registrar el incidente en un archivo donde se encuentre el resumen de lo sucedido.
7. Si el incidente es un robo o extravío de información se deberá reportar inmediatamente a los encargados y responsables del sistema, ellos avisaran al titular y a los encargados en la UNAM de lo sucedido.

La recuperación de datos de los sistemas de respaldo la podrá solicitar los encargados y el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —342 de 425—

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. Seguridad perimetral interior

Para las personas que acceden a dichos espacios interiores:
Las oficinas del Centro de Orientación Especializada (COE) y Departamento de Instrumentos de Orientación se encuentran de la Dirección General de Orientación y Atención Educativa en la planta baja y alta respectivamente.

1. ¿Cómo las identifica?

Las personas a quienes atendemos son: alumnado, egresadas y egresados de la UNAM.

2. ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 343 de 425—

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

En el caso de que un titular identifique que sus datos personales son incorrectos, se podrá hacer un cambió si y solo si el titular sigue el siguiente protocolo:

1. Obtener y llenar el documento del ANEXO II donde el titular requiere una actualización en los datos personales.
2. Mandar al correo innovaoe@unam.mx lo siguiente:
    a. Adjuntar el documento firmado del ANEXO II en el correo electrónico,
3. El titular recibirá un correo donde se le avisará de la recepción del correo en un tiempo aproximado de 3 días hábiles.
4. Esperar el aviso dé que se realizó el cambio en los datos personales solicitados
5. Revisar que el cambió se realizó correctamente.
    a. Se tiene un tiempo de espera de 2 días hábiles para cualquier corrección de los datos que se cambiaron.
    b. SI todo es correcto, dejar como está.
    c. Si hay algún dato que no se cambió, favor de enviar el dato incorrecto con el correcto como respuesta del aviso. Y verificar nuevamente. Estos cambios se deben de realizar en menos de 12 horas.

Para los responsables y encargados de cambiar los datos, seguir el siguiente protocolo.

1. Al recibir el correo, el encargado responderá al titular:
    a. El cambio se realizará dentro de 3 días hábiles.
    b. Hay que informar que persona va a realizar el cambio, deberá ser la misma que mande la respuesta de los días hábiles.
2. Levantar un reporte de la incidencia.
3. Se realiza el cambio.
4. Se envía un correo para que el titular verifique que el cambio se hizo correctamente pidiendo que mande una respuesta si el cambio se hizo correctamente o no.
    a. Si se recibe una respuesta afirmativa, ponemos fin a la incidencia.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —344 de 425—

b. Si se recibe un correo donde sigue la inconsistencia en los datos, revisar de nuevo la petición y hacer el cambio inmediatamente y volver a confirmar que se realizó el cambio.
c. Si no se recibe el correo, después de dos días del envío del correo de verificación de la realización de cambios en los datos personales. Podemos poner fin a la incidencia.
d. Si llegara la información después de los dos días hábiles el titular deberá de volver a pedir el cambio.

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
Toda comunicación con el sitio web está asegurado por el protocolo ***https*** para que la información viaje encriptada en la red.
Aplicación ***Portal Orientación Educativa*** tiene la siguiente configuración:

1. Para acceder al sistema se cuenta con un usuario y contraseña.
2. El usuario está definido por el número de cuenta o por el correo electrónico.
3. La contraseña se genera a partir de un "dato personal".
4. La contraseña se guarda encriptada en la base de datos y se usa un método de encriptación para poder obtenerla al momento de iniciar la sesión.
5. El sistema cuenta con los siguientes perfiles
    a. **Usuario** El usuario solo podrá ver sus datos personales, Nombres, Apellidos, Fecha de nacimiento, Sexo, Escuela / Facultada, Semestre, Número de cuenta si es alumno universitario.
    b. Alumno El alumno puede realizar el instrumento del PROUNAM II e INVOCA en línea y también podrá checar sus resultados cuando sean evaluados, pueden bajar sus resultados en un PDF.
    c. **Administrador** El administrador tiene permisos para ver, crear, modificar y borrar datos personales de identificación de los usuarios.
    d. **Administrador Alumno:** El administrador Alumno tiene permisos para ver, crear, modificar y borrar datos académicos.
    e. **Administrador Orientador** El administrador Orientador tiene permisos para ver, crear, modificar y borrar datos de los orientadores del sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —345 de 425—

f. **Tester** El Tester solamente puede ver el instrumento, no puede contestar ni guardar ninguna información adicional. Es el que prueba el sistema.

Contenedor de la máquina virtual tiene la siguiente configuración:

1. Se crea un perfil, usuario y contraseña para el uso de la máquina virtual
2. Se conecta a través de una IP fija o mediante SSH y un conjunto de llaves privada y pública (*SSH Public Key Authentication*).

Base de datos tiene la siguiente configuración:

1. El acceso a estas bases de datos es por medio de un usuario y contraseña que lo tiene el administrador.
2. El administrador de la base de datos puede crear, modificar, borrar, actualizar lo siguiente:
   a. Esquema de la base de datos
   b. Tablas
   c. Registros
   d. Hacer respaldos de la información de las bases
   e. Creación de usuarios de la base
   f. Modificación de privilegios de los usuarios

Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área.
Resumen de la verificación de perfiles de usuario y contraseñas:

1. Modelo de control de acceso:

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? **SI**
b) ¿Es discrecional (matriz de control de acceso)? **No**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Si**

2. Perfiles de usuario y contraseñas en el sistema operativo de red: NO APLICA

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **NO**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **NO APLICA**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **NO APLICA**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —346 de 425—

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Si**

b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Se cifra la contraseña, pero no el nombre de usuario**

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? **Administrador general**

b) ¿Quién autoriza la creación de nuevos perfiles? **Administrador de usuarios**

c) ¿Se lleva registro de la creación de nuevos perfiles? **Si**

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? NO

b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? SI, **solo el administrador de la base puede entrar por este medio**

c) ¿Cómo se evita el acceso remoto no autorizado? **Mediante la autenticación por llave y por IP**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos del sistema los realiza el encargado del sistema en la DGOAE.

DGOAE

1. Los respaldos se realizan manualmente y completos.
2. El respaldo se realiza cada mes
3. Si se realiza alguna aplicación del instrumento, acabando el periodo de aplicación se obtiene un respaldo manual.
4. Estos respaldos se quedan en un disco duro.
5. Los respaldos los resguarda el encargado en la Dirección de Apoyo Técnico.
6. Los respaldos se realizan de forma automática cada tercer día y guardan el estado de la máquina virtual. donde se aloja el sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —347 de 425—

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.
   - Tener respaldos de la base de datos y del código.
   - Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
   - Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
   - El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
   - Una vez que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
   - Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una vez hecha la conexión se carga el respaldo de la base de datos.
   - En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
   - Realizar pruebas al sistema de inicio de sesión, cierre de sesión, registro de universitarias y universitarios, consulta del programa del Encuentro Virtual de Empleabilidad, inscripción y baja a las diferentes actividades que ofrece éste.
2. El tiempo que se demore DGTIC en darnos el nuevo espacio fue de un día, ya que se le explico que era de carácter urgente.
3. No aplica.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	DGOAE DAT POE 01

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —348 de 425—

(Nombre del sistema B1) *	Portal de Orientación Educativa	
Recurso*	**Descripción***	**Control***
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicaran el tráfico que existen en el servidor	Se hace manual y solamente será usada cuando se genere un ataque al sistema
Bitácoras generadas por el servidor	Las bitácoras generadas por el servidor nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas en la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.
Wireshark	Se hace una revisión de parte del cliente para saber qué es lo que puede ver y asegurar que los datos viajan encriptados.	Wireshark se usa para la identificación de paquetes por etiquetas TCP y IP, analizar que se envía y que se recibe.
Ambiente de pruebas	Se debe de tener una computadora donde se pueda hacer pruebas y que solamente se pueda acceder localmente o en red local.	Se tiene una computadora con *Centos* 7 para poder hacer las pruebas necesarias.
nmpa, netcat, tcpdump	Utilizar las herramientas para la detección de fallos y verificación del funcionamiento y seguridad del sistema	Las herramientas son libres y se hará una revisión cada semestre con estas herramientas

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único*	DGOAE_DAT_MEPSI_01
(Nombre del sistema B1) *	***Portal de Orientación Educativa***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —349 de 425—

Medida de seguridad*	Procedimiento*	Responsable*
Contar con las medidas de seguridad que DGTIC pide.	Se seguirán las recomendaciones que DGTIC propone para la seguridad en los sistemas	Administrador del Sistema 28 días laborables
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones	Administrador del Sistema 5 días laborables
Lista de verificación de seguridad	Diseñar un documento donde llevemos una lista de verificación sobre las reglas de seguridad que debe de tener el sistema	Administrador del Sistema 28 días laborables

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	DGOAE DAT POE 01	
(Nombre del sistema B1) *	***Portal de Orientación Educativa***	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Se deberá de mandar la aplicación al CERT en DGTIC para la evaluación del sistema	I. *Ausencia de encabezados de seguridad* II. *Envío de Credenciales en texto claro*	*Pedro Xavier Contla Romero* *4 de abril de 2019*

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	DGOAE DAT POE 01	
(Nombre del sistema B1) *	**Portal de Orientación Educativa**	
Medida de seguridad*	**Acciones***	**Responsable***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 350 de 425—

Se resolvieron los diferentes riesgos de seguridad según el reporte de DGTIC	*I. Se implementó la sobreescritura de cabeceras* *II. Se implementó el certificado de Let's Encrypt.*	*Pedro Xavier Contla Romero 15 de abril del 2019*

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT POE 01**		
(Nombre del sistema B1) *	**Portal de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	Duración: Un día Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Resguardo de información mediante los protocolos antes establecidos	Contar con un documento donde explique los objetivos principales de la implementación de la seguridad para el sistema	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Programación de los sistemas usando framework seguros	Estar actualizando las herramientas de desarrollo conforme avanza la tecnología	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores que actualicen los sistemas tendrán que buscar si lo que se usa es seguro para el resguardo de los datos personales. Cada año generar el análisis sobre la tecnología que se usa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —351 de 425—

Pruebas de obtención de datos mediante perfiles	Realizar pruebas sobre los diferentes perfiles en el sistema	Duración: una semana Inicio: Por definir Termino: Por definir	Contar con el análisis de los perfiles y sus privilegios del sistema Al incorporar un nuevo perfil al sistema
Creación de Certificados SSL	Contar con un documento en donde se documente como generar in certificado SSL por medio de Let's Encrypt	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores podrán contar con un método para generar sus certificados mientras se obtiene el principal. Al incorporar un nuevo desarrollador al equipo
Curso de protección a las máquinas virtuales	Contar con un curso de administrador tipo Linux para capacitar a nuevos administradores sobre la configuración en el servidor	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Curso de hacker ético para pruebas en el sistema	Contar con un curso para probar los sistemas en desarrollo.	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Protocolo interno para verificación de la seguridad	Contar con un documento que indique los pasos que se deben llevar para probar la seguridad de los sistemas	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Antes de salir a producción. *

Nota: La capacitación se realiza cuando los usuarios aumenten, por lo que las fechas no están definidas. Por el momento los que usan el sistema ya están capacitados

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —352 de 425—

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	DGOAE_DAT_POE_01		
(Nombre del sistema B1) *	**Portal de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Aviso particular del área responsable del dar el servicio por medio del sistema	La distribución es en la página del sistema y está al alcance en dos lugares. Si existe registro, antes de darle aceptar. Si ya están registrados, donde se despliegan los datos personales.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de infografías y videos informativos de los datos personales de los titulares están resguardados en el sistema.	La distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Duración: permanente Inicio: Por definir Termino: Por definir	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	DGOAE_DAT_POE_01

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 353 de 425—

(Nombre del sistema B1) *	Portal de Orientación Educativa		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Análisis de los reportes de los usuarios acerca de los bugs, mal funcionamiento y documentación sobre el funcionamiento del sistema.	*Contar con la información necesaria para evaluar los puntos en donde se necesita hacer una actualización del sistema.*	Duración: dos semanas Inicio: Por definir Termino: Por definir	*Actualización y mejora del sistema actual, parcialmente.*
Actualización de mensajes de error y éxito.	*Agregar umas respuestas en para el Módulo de los Administradores para que tenga una mejor retroalimentación de las modificaciones o borrado que se realiza.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Mejor retroalimentación a los administradores para el uso de las funcionalidades del sistema.*
Pantallas de verificación	*Agregar pantallas antes de realizar algún cambio para evitar modificaciones no deseadas.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Total*

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	DGOAE DAT POE 01		
(Nombre del sistema B1) *	**Portal de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en qué estado se encuentran*	Duración: Cada año Inicio: Por definir Termino: Por definir	*Total*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 354 de 425—

Actualizar o cambiar los equipos de desarrollo lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: 1 mes Inicio: Por definir Termino: Por definir	*Total*

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE_DAT_POE_01**	
(Nombre del sistema B1) *	**Portal de Orientación Educativa**	
Proceso*	**Descripción***	**Responsable***
Respaldo en soporte electrónico de la base de datos	1. *Realizar un respaldo de la base de datos.* 2. *El nombre del archivo respaldo es nombre de la base y la fecha cuando se realizó el respaldo* 3. *Guardarlo en la carpeta donde se encuentran los demás respaldos.*	*Administrador de la base de datos* *3 días.*
Respaldo en soporte electrónico portable (USB, disco duro, CD-R) de la base de datos	1. *Copiar los respaldos que se encuentran en la carpeta a soportes electrónicos portables para el resguardo de la información.*	*Administrador de la base de datos* *1 días.*
Respaldo de los archivos de reporte que contenga datos personales	1. *Generar los reportes que serán enviados a las diferentes dependencias.* 2. *Comprimir los reportes en un archivo con el nombre de la dependencia y la fecha cuando se generaron los reportes.* 3. *Guardar el archivo en un soporte electrónico.* 4. *Pedir al área de sistemas el soporte electrónico portable donde se va a guardar el archivo comprimido.* 5. *Guardar el archivo en un soporte electrónico portable.*	*Encargado de traslado de reportes.* *3 días.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 355 de 425—

	6. Enviar el soporte electrónico portable al área de sistemas para su resguardo.	

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE DAT POE 01**	
(Nombre del sistema B1) *	**Portal de Orientación Educativa**	
Proceso*	**Descripción***	**Responsable***
Proceso de borrado de equipos de computo	*Reportar que equipo y de que persona es el equipo en el cual se va a realizar el borrado.* *Generar un respaldo de la información principal del usuario del equipo.* *Verificación del respaldo para evitar que contenga información de datos personales ajenos.* *Formatear el disco duro mediante una herramienta de bajo nivel para evitar recuperación de información.*	*Encargado del sistema* *1 semana*
Proceso de borrado de respaldos en soporte electrónicos	*La información que se borra de estos dispositivos solamente deberá guardar información del sistema.* *Formatear mediante el un borrado bajo nivel.*	*Encargado del sistema* *1 semana*

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

La Dirección de Apoyo Técnico y la Coordinación de Orientación Educativa acordarán la cancelación del sistema mediante un escrito donde indique lo siguiente:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
   Estas fechas al menos deben de tener un mes de separación.
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 356 de 425—

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
4. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)
En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 357 de 425—

- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Portal de Orientación Educativa que se encuentren dentro sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Con respecto a los discos duros, cualquier software que realice un borrado de bajo nivel. Los métodos de borrado que evitan que se pueda recuperar los datos de los dispositivos de almacenamiento una vez se han eliminado son la desmagnetización, la destrucción y la sobreescritura.

La desmagnetización y la destrucción física no permiten reutilizar el dispositivo posteriormente. En la desmagnetización se expone el soporte a un campo magnético con una potencia que variará en función del tamaño del dispositivo, mientras que en la destrucción física se elimina el soporte físicamente por completo siendo imposible su reutilización. Sin embargo, el método de sobreescritura elimina la información sin que ésta pueda ser recuperada y permite volver a utilizar el dispositivo con garantías de que funcione correctamente.

Esta forma de borrado se utiliza por ejemplo en los casos en los que se pretende donar los ordenadores antiguos de una empresa, y se desea tener la seguridad de que toda la información eliminada es irrecuperable
(https://www.incibe.es/protege-tu-empresa/blog/borrar-informacion-dispositivo-ciberseguridad).

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización.

Instrumentos de Orientación Educativa.

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE_DAT_INSTRUMENTOS_01**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 358 de 425—

(Nombre del sistema D1	Instrumentos de Orientación Educativa
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de Identificación** • Correo electrónico • Edad (10 a 20 años) • Ciudad de residencia • País de residencia • Sexo (Hombre, Mujer o Prefiere no contestar) **Datos de Académicos** • Si es alumno Universitario UNAM, el número de cuenta • Nivel máximo de estudios (secundaria o bachillerato)
Responsable*:	DGTIC, Departamento de Instrumentos, DGOAE y Dirección de Apoyo técnico, DGOAE
Nombre*:	**Lic. José Antonio Sánchez Yllanez**
Cargo*:	**Director de Apoyo Técnico de la DGOAE**
Funciones*:	Responsable del cuidado de datos personales en los sistemas desarrollados por su área de trabajo.
Obligaciones*:	Verificar y ver que se cumplan los protocolos para el cumplimiento de los derechos ARCOP en los sistemas desarrollados en la Dirección de Apoyo Técnico.
	Encargados[4]:
(Nombre del Encargado 1*)	**M. en C. Pedro Xavier Contla Romero**
Cargo*:	**Técnico Académico Titular "A"**
Funciones*:	Desarrollo y automatización de sistemas web para la DGOAE
Obligaciones*:	Diseño, Desarrollo, Implementación, mantenimiento y Actualización de Sistemas web en la DGOAE.
(Nombre del Encargado 2*)	**Mtra. Telma Ríos Condado**
Cargo*:	**Directora de Orientación Educativa de la DGOAE**
Funciones*:	Administrar del sitio web
Obligaciones*:	Análisis de datos
	Usuarios:
(Nombre del Usuario 1*)	M. en C. Pedro Xavier Contla Romero
Cargo*:	Técnico Académico Titular "A"
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de usuarios y alumnos y mantenimiento del sistema

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 359 de 425—

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único*	DGOAE_DAT_INSTRUMENTOS_01
(Nombre del sistema D1*)	Instrumentos de Orientación Educativa
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de datos relacional, hojas de cálculo
Características del lugar donde se resguardan los soportes: *	• El alojamiento del sistema Instrumentos de Orientación Educativa se encuentra en los servidores de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Toda comunicación con el sitio web está asegurado por el protocolo HTTPS para que la información viaje encriptada en la red. • Los datos se encuentran resguardados en bases de datos de MySQL que solamente tiene acceso el encargado M. en C. Xavier Contla. • La conexión a al servidor se realiza mediante SSH y un conjunto de llaves privada y pública (SSH Public Key Authentication). • El acceso a estas bases de datos es por medio de un usuario y contraseña. • Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área. • Para el acceso al sistema es por un nombre de usuario y contraseña, las cuales se generan para cada alumno usuario del sistema.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —360 de 425—

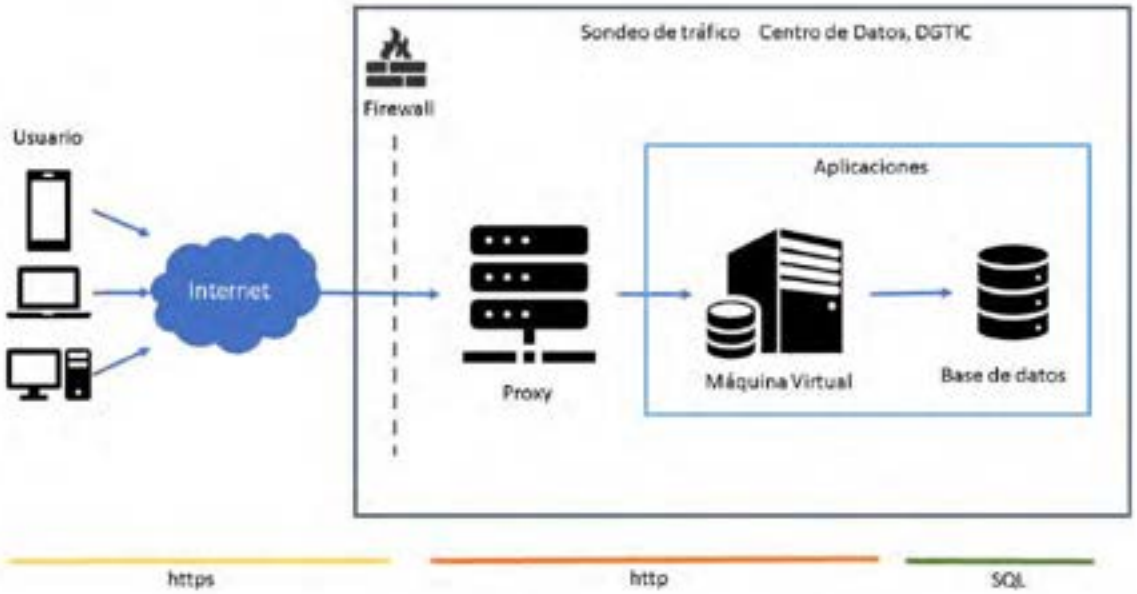


Ilustración 4 Diagrama de Seguridad

La Ilustración 1 muestra como es el acceso a la información dentro del sistema que se encuentra alojado en los servidores del Centro de Datos de DGTIC. Se tienen varios niveles de seguridad:

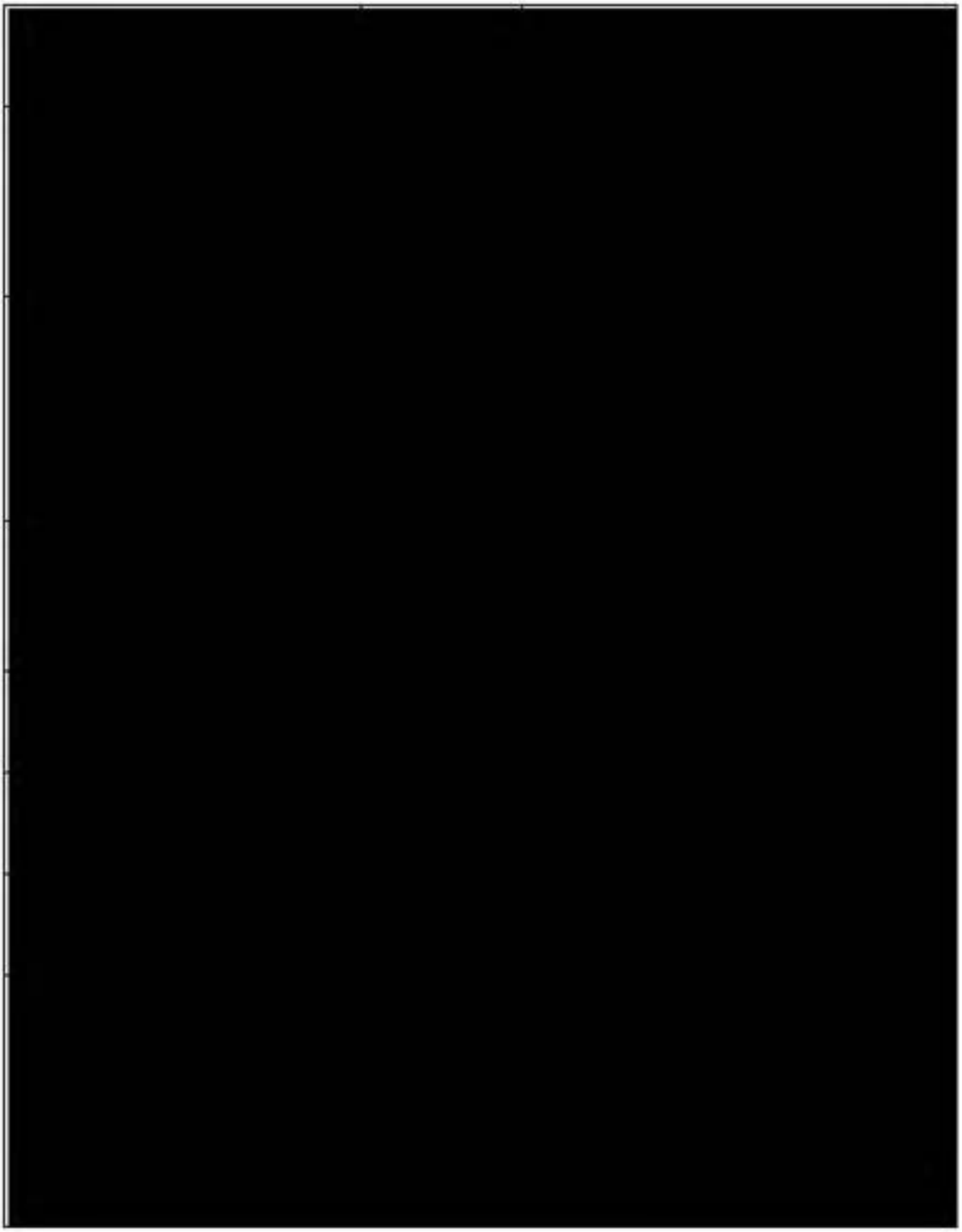
- La comunicación de un usuario con el sistema se hace mediante internet usando el protocolo de seguridad https, el cual cifra los datos que viajan en internet y solamente los puede leer el sistema.
- Dentro del Centro de datos, existe in firewall para monitorear la red entrante y saliente y decide su permite o bloquea el tráfico en función de un conjunto definido de reglas.
- Si los datos son seguros pasa a través de un proxy el cual, no solo realiza la tarea de balancear la carga a los servidores si no, es el punto de inicio a la conexión de la aplicación.
- El usuario que quiere usar la aplicación tiene un nombre de usuario y contraseña para poder acceder al aplicativo.
- Cada usuario tiene un perfil el cual tiene permisos específicos para acceder a la información de datos personales.
- Al pedir alguna información que se encuentra dentro de la base de datos, el sistema tiene un usuario y contraseña único para acceder a la información.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —361 de 425—

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**	
(Nombre del sistema D1) *	**Instrumentos de Orientación Educativa**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —362 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —363 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**	
(Nombre del sistema D1) *	**Instrumentos de Orientación Educativa**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

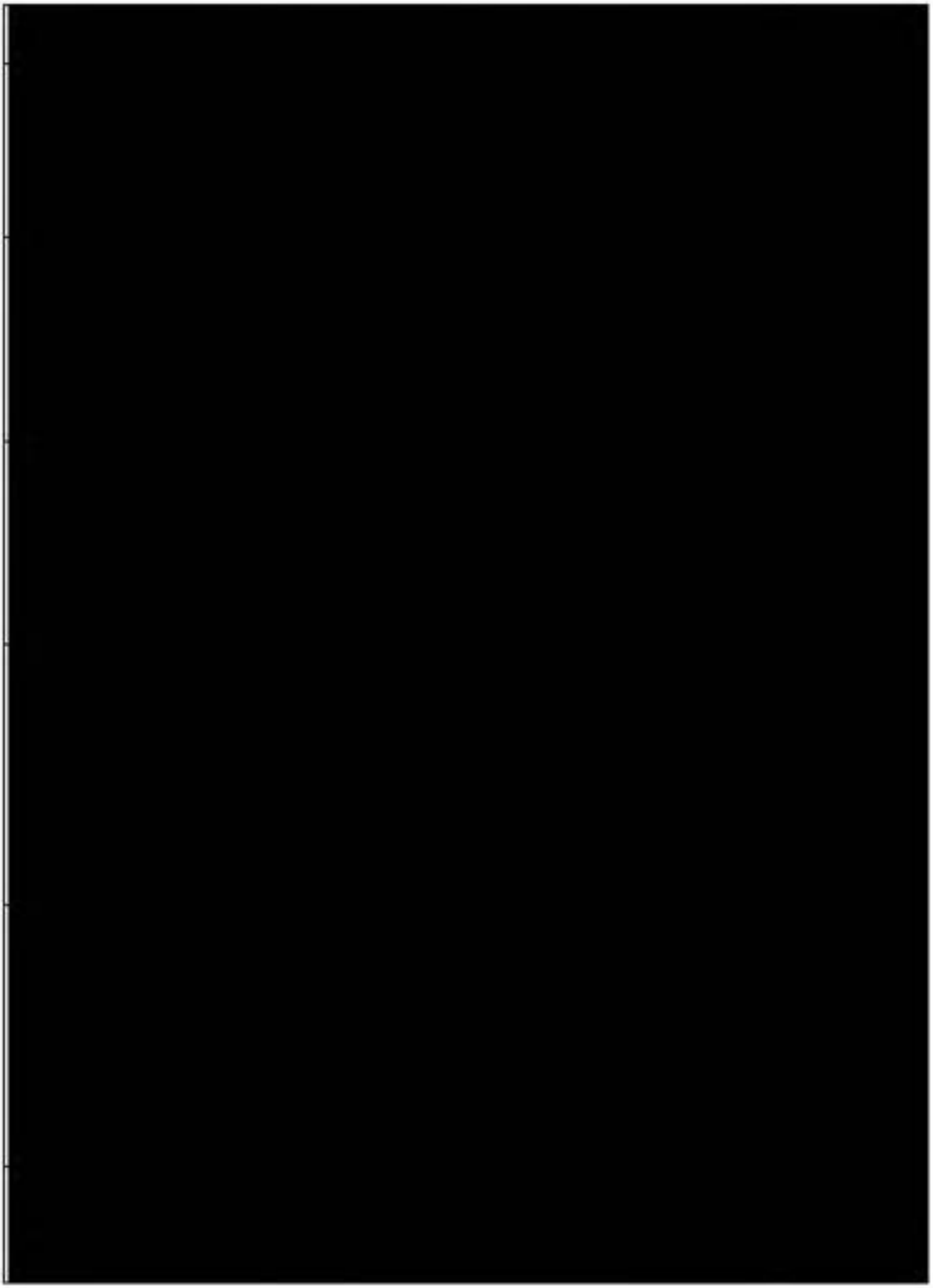
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —364 de 425—

[redacted]

5. Plan de trabajo

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	DGOAE DAT INSTRUMENTOS 01		
(Nombre del sistema D1) *	Instrumentos de Orientación Educativa		
Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —365 de 425—



ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —366 de 425—



6. Medidas de seguridad implementadas

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	• Por el momento no hay soporte físico

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —367 de 425—

Transferencias mediante el traslado de soportes electrónicos:	• Por el momento no hay traslado por soporte electrónico físico
Transferencias mediante el traslado sobre redes electrónicas:	• Los traslados se deberán de realizar mediante el uso de correos institucionales. • Tener una lista con los correos institucionales a los cuales se les comparte los datos personales. • Todos los archivos que contengan datos personales deberán de ser cifrados para el envío de información. • Se usará una contraseña que debe de ser personal e intransferible para cada encargado. • En el caso requerido las transferencias se formalizarán mediante algún instrumento jurídico. • Cualquier documento que contenga datos personales y que sea impreso, solamente se le podrá entregar al titular de estos datos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica para este sistema.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras actualmente:

   I. El área responsable del tratamiento de datos personales en el sistema de Instrumentos de Orientación Educativa realiza las siguientes acciones con respecto a las bitácoras en sistema.
      a. El administrador del servidor y DGTIC pueden acceder a las bitácoras
      b. La bitácora se encuentra en soportes electrónicos
      c. La bitácora guarda la siguiente información
         i. Fecha y hora
         ii. Función que se llamó

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud5=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —368 de 425—

iii. Llamada a SQL que se realizó a la base de datos
1. Ver
2. Insertar
3. Actualizar
4. Borrar

d. El sistema guarda un registro de las operaciones que se hacen a la base de datos.
e. Guarda un registro de las operaciones fallidas.
f. Cada mes se borran las bitácoras que se generan por espacio.
g. No se crean respaldos de las bitácoras.
h. Las bitácoras contienen fecha, hora, acción que se realizó y mensaje.
i. Las bitácoras van a tener una duración de 1 mes en sistema y se creará una copia que se resguardará en algún medio de almacenamiento durante dos años.

II. Con los nuevos requisitos se va a implementar el siguiente sistema de bitácoras.

a. Se actualizarán la información que se guarda en la bitácora como sigue:
i. Los datos que guardará
- Fecha y hora
- Función SQL y que realizó (Lectura, escritura, inserción)
- El id de usuario que hizo la acción
- Los privilegios del usuario

ii. Estas bitácoras se van a respaldar cada mes y se guardarán por un periodo de dos años en soportes electrónicos.

b. Se crearán tablas en la base de datos que guarden el registro de actividad por usuario que tenga acceso a datos personales y seguirá el siguiente protocolo:
i. Los datos que guardará
- Fecha y hora
- Función SQL y que realizó (Lectura, escritura, inserción)
- El id de usuario que hizo la acción
- Los privilegios del usuario

ii. Estas tablas que contienen el registro de actividades se respaldarán cada mes y deben de quedarse al menos 4 años resguardadas en soportes electrónicos.

IV. REGISTRO DE INCIDENTES

En caso de presentar un incidente seguir los siguientes pasos.

1. Resolver el incidente
2. Pedir el archivo en formato electrónico "Registro de incidentes de datos personales"(pdf).

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —369 de 425—

3. Recopilar la siguiente información:
    a. Resumen del incidente
    b. Resumen de cómo se solucionó el incidente
    c. Especificar si el incidente daño algún archivo, base de datos, servidor, respaldo etc.
    d. Fecha de inicio
    e. Fecha de término o resolución del incidente
    f. El impacto del incidente
    g. La persona quien resolvió el incidente
    h. Nombre del responsable y firma
4. El archivo de registro se actualiza y se crea un respaldo en un soporte electrónico portable para su almacenamiento.
5. La resolución del incidente tiene un tiempo máximo de 3 días hábiles.
6. El encargado de sistema deberá de registrar el incidente en un archivo donde se encuentre el resumen de lo sucedido.
7. Si el incidente es un robo o extravío de información se deberá reportar inmediatamente a los encargados y responsables del sistema, ellos avisaran al titular y a los encargados en la UNAM de lo sucedido.

La recuperación de datos de los sistemas de respaldo la podrá solicitar los encargados y el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

1. Seguridad perimetral exterior

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?

La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.

Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —370 de 425—

resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.
Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?
Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.
b) ¿Cómo las autentifica?
Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.
c) ¿Cómo les autoriza el acceso?
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

2. Seguridad perimetral interior
Para las personas que acceden a dichos espacios interiores:
Las oficinas del Centro de Orientación Especializada (COE) y Departamento de Instrumentos de Orientación se encuentran de la Dirección General de Orientación y Atención Educativa en la planta baja y alta respectivamente.

1. ¿Cómo las identifica?
Las personas a quienes atendemos son: alumnado, egresadas y egresados de la UNAM.
2. ¿Cómo las autentifica?
Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.
3. ¿Cómo les autoriza el acceso?
En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —371 de 425—

en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

En el caso de que un titular identifique que sus datos personales son incorrectos, se podrá hacer un cambió si y solo si el titular sigue el siguiente protocolo:

1. Obtener y llenar el documento del ANEXO II donde el titular requiere una actualización en los datos personales.
2. Mandar al correo innovaoe@unam.mx lo siguiente:
    a. Adjuntar el documento firmado del ANEXO II en el correo electrónico,
3. El titular recibirá un correo donde se le avisará de la recepción del correo en un tiempo aproximado de 3 días hábiles.
4. Esperar el aviso dé que se realizó el cambio en los datos personales solicitados
5. Revisar que el cambió se realizó correctamente.
    a. Se tiene un tiempo de espera de 2 días hábiles para cualquier corrección de los datos que se cambiaron.
    b. SI todo es correcto, dejar como está.
    c. Si hay algún dato que no se cambió, favor de enviar el dato incorrecto con el correcto como respuesta del aviso. Y verificar nuevamente. Estos cambios se deben de realizar en menos de 12 horas.

Para los responsables y encargados de cambiar los datos, seguir el siguiente protocolo.

1. Al recibir el correo, el encargado responderá al titular:
    a. El cambio se realizará dentro de 3 días hábiles.
    b. Hay que informar que persona va a realizar el cambio, deberá ser la misma que mande la respuesta de los días hábiles.
2. Levantar un reporte de la incidencia.
3. Se realiza el cambio.
4. Se envía un correo para que el titular verifique que el cambio se hizo correctamente pidiendo que mande una respuesta si el cambio se hizo correctamente o no.
    a. Si se recibe una respuesta afirmativa, ponemos fin a la incidencia.
    b. Si se recibe un correo donde sigue la inconsistencia en los datos, revisar de nuevo la petición y hacer el cambio inmediatamente y volver a confirmar que se realizó el cambio.
    c. Si no se recibe el correo, después de dos días del envío del correo de verificación de la realización de cambios en los datos personales. Podemos poner fin a la incidencia.
    d. Si llegara la información después de los dos días hábiles el titular deberá de volver a pedir el cambio.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —372 de 425—

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
Toda comunicación con el sitio web está asegurado por el protocolo ***https*** para que la información viaje encriptada en la red.
Aplicación ***Instrumentos de Orientación Educativa*** tiene la siguiente configuración:

1. Para acceder al sistema se cuenta con un usuario y contraseña.
2. El usuario está definido por el correo electrónico.
3. La contraseña se genera aleatoriamente y enviada por correo al usuario registrado.
4. La contraseña se guarda encriptada en la base de datos y se usa un método de encriptación para poder obtenerla al momento de iniciar la sesión.
5. El sistema cuenta con los siguientes perfiles
    a. **Usuario** El usuario solo podrá ver sus datos como edad al momento de registrarse, sexo (Hombre, Mujer o Prefiere no especificar), Número de cuenta se es alumno de la UNAM, ciudad de residencia, país de residencia y nivel máximo de estudios (secundaria o bachillerato)

Contenedor de la máquina virtual tiene la siguiente configuración:

1. Se crea un perfil, usuario y contraseña para el uso de la máquina virtual
2. Se conecta a través de una IP fija o mediante SSH y un conjunto de llaves privada y pública (*SSH Public Key Authentication*).
3. El usuario tiene permiso de ***root*** para hacer la configuración de servidor.

Base de datos tiene la siguiente configuración:

1. El acceso a estas bases de datos es por medio de un usuario y contraseña que lo tiene el administrador.
2. El administrador de la base de datos puede crear, modificar, borrar, actualizar lo siguiente:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —373 de 425—

a. Esquema de la base de datos
b. Tablas
c. Registros
d. Hacer respaldos de la información de las bases
e. Creación de usuarios de la base
f. Modificación de privilegios de los usuarios

Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área.
Resumen de la verificación de perfiles de usuario y contraseñas:

1. Modelo de control de acceso:

a) ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? **SI**
b) ¿Es discrecional (matriz de control de acceso)? **No**
c) ¿Está basado en roles (perfiles) o grupos? **Si**
d) ¿Está basado en reglas? **Si**

2. Perfiles de usuario y contraseñas en el sistema operativo de red: NO APLICA

a) ¿Cuenta con un sistema operativo de red instalado en sus equipos? **NO**
b) ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **NO APLICA**
c) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **NO APLICA**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

a) ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Si**
b) ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Se cifra la contraseña, pero no el nombre de usuario**

4. Administración de perfiles de usuario y contraseñas:

a) ¿Quién da de alta nuevos perfiles? **Administrador**
b) ¿Quién autoriza la creación de nuevos perfiles? **Encargado de los Usuarios**
c) ¿Se lleva registro de la creación de nuevos perfiles? **Si**

5. Acceso remoto al sistema de tratamiento de datos personales:

a) ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **NO**
b) ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **Si, solo el administrador de la base puede entrar por este medio**

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —374 de 425—

c) ¿Cómo se evita el acceso remoto no autorizado? **Mediante la autenticación por llave y por IP**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos del sistema los realiza el encargado del sistema en la DGOAE.

DGOAE

1. Los respaldos se realizan manualmente y completos.
2. El respaldo se realiza cada mes
3. Si se realiza alguna aplicación del instrumento, acabando el periodo de aplicación se obtiene un respaldo manual.
4. Estos respaldos se quedan en un disco duro.
5. Los respaldos los resguarda el encargado en la Dirección de Apoyo Técnico.

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.
    - Tener respaldos de la base de datos y del código.
    - Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
    - Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
    - El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
    - Una vez que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
    - Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una vez hecha la conexión se carga el respaldo de la base de datos.
    - En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDSzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —375 de 425—

- Realizar pruebas al sistema de inicio de sesión, cierre de sesión, registro de universitarias y universitarios, consulta del programa del Encuentro Virtual de Empleabilidad, inscripción y baja a las diferentes actividades que ofrece éste.

2. El tiempo que se demore DGTIC en darnos el nuevo espacio fue de un día, ya que se le explico que era de carácter urgente.
3. No aplica.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Recurso*	**Descripción***	**Control***
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicaran el tráfico que existen en el servidor	Se hace manual y solamente será usada cuando se genere un ataque al sistema
Bitácoras generadas por el servidor	Las bitácoras generadas por el servidor nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas en la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.
Wireshark	Se hace una revisión de parte del cliente para saber qué es lo que puede ver y asegurar que los datos viajan encriptados.	Wireshark se usa para la identificación de paquetes por etiquetas TCP y IP, analizar que se envía y que se recibe.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 376 de 425—

Ambiente de pruebas	Se debe de tener una computadora donde se pueda hacer pruebas y que solamente se pueda acceder localmente o en red local.	Se tiene una computadora con *Centos* 7 para poder hacer las pruebas necesarias.
Nmpa, netcat, Tcpdump	Utilizar las herramientas para la detección de fallos y verificación del funcionamiento y seguridad del sistema	Las herramientas son libres y se hará una revisión cada semestre con estas herramientas

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	DGOAE DAT INSTRUMENTOS 01	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Contar con las medidas de seguridad que DGTIC pide.	Se seguirán las recomendaciones que DGTIC propone para la seguridad en los sistemas	Administrador del Sistema 28 días laborables
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones	Administrador del Sistema 5 días laborables
Lista de verificación de seguridad	Diseñar un documento donde llevemos una lista de verificación sobre las reglas de seguridad que debe de tener el sistema	Administrador del Sistema 28 días laborables

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —377 de 425—

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE_DAT_INSTRUMENTOS_01**	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Se deberá de mandar la aplicación al CERT en DGTIC para la evaluación del sistema	I. *Ausencia de encabezados de seguridad* II. *Envio de Credenciales en texto claro*	*Pedro Xavier Contla Romero 4 de abril de 2019*

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE_DAT_INSTRUMENTOS_01**	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Medida de seguridad*	**Acciones***	**Responsable***
Se resolvieron los diferentes riesgos de seguridad según el reporte de DGTIC	I. *Se implementó la sobreescritura de cabeceras* II. *Se implementó el certificado de Let's Encrypt.*	*Pedro Xavier Contla Romero 15 de abril del 2019*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 378 de 425—

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**		
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	Duración: Un día Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Resguardo de información mediante los protocolos antes establecidos	Contar con un documento donde explique los objetivos principales de la implementación de la seguridad para el sistema	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Programación de los sistemas usando framework seguros	Estar actualizando las herramientas de desarrollo conforme avanza la tecnología	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores que actualicen los sistemas tendrán que buscar si lo que se usa es seguro para el resguardo de los datos personales. Cada año generar el análisis sobre la tecnología que se usa.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —379 de 425—

Pruebas de obtención de datos mediante perfiles	Realizar pruebas sobre los diferentes perfiles en el sistema	Duración: una semana Inicio: Por definir Termino: Por definir	Contar con el análisis de los perfiles y sus privilegios del sistema Al incorporar un nuevo perfil al sistema
Creación de Certificados SSL	Contar con un documento en donde se documente como generar in certificado SSL por medio de Let's Encrypt	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores podrán contar con un método para generar sus certificados mientras se obtiene el principal. Al incorporar un nuevo desarrollador al equipo
Curso de protección a las máquinas virtuales	Contar con un curso de administrador tipo Linux para capacitar a nuevos administradores sobre la configuración en el servidor	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Curso de hacker ético para pruebas en el sistema	Contar con un curso para probar los sistemas en desarrollo.	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Protocolo interno para verificación de la seguridad	Contar con un documento que indique los pasos que se deben llevar para probar la seguridad de los sistemas	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Antes de salir a producción. *

Nota: La capacitación se realiza cuando los usuarios aumenten, por lo que las fechas no están definidas. Por el momento los que usan el sistema ya están capacitados

8.2. Programa de difusión de la protección a los datos personales

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 380 de 425—

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**		
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Aviso particular del área responsable del dar el servicio por medio del sistema	La distribución es en la página del sistema y está al alcance en dos lugares. Si existe registro, antes de darle aceptar. Si ya están registrados, donde se despliegan los datos personales.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	LA distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Duración: permanente Inicio: Por definir Termino: Por definir	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

9. Mejora continua

9.1. Actualización y mantenimiento de sistemas de información

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 381 de 425—

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico			
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**		
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Análisis de los reportes de los usuarios acerca de los bugs, mal funcionamiento y documentación sobre el funcionamiento del sistema.	*Contar con la información necesaria para evaluar los puntos en donde se necesita hacer una actualización del sistema.*	Duración: dos semanas Inicio: Por definir Termino: Por definir	*Actualización y mejora del sistema actual, parcialmente.*
Actualización de mensajes de error y éxito.	*Agregar umas respuestas en para el Módulo de los Administradores para que tenga una mejor retroalimentación de las modificaciones o borrado que se realiza.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Mejor retroalimentación a los administradores para el uso de las funcionalidades del sistema.*
Pantallas de verificación	*Agregar pantallas antes de realizar algún cambio para evitar modificaciones no deseadas.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Total*

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 382 de 425—

Dirección de Apoyo Técnico			
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**		
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en que estado se encuentran*	Duración: Cada año Inicio: Por definir Termino: Por definir	*Total*
Actualizar o cambiar los equipos de desarrollo lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: 1 mes Inicio: Por definir Termino: Por definir	*Total*

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Proceso*	**Descripción***	**Responsable***
Respaldo en soporte electrónico de la base de datos	1. *Realizar un respaldo de la base de datos.* 2. *El nombre del archivo respaldo es nombre de la base y la fecha cuando se realizó el respaldo* 3. *Guardarlo en la carpeta donde se encuentran los demás respaldos.*	*Administrador de la base de datos* *3 dias.*
Respaldo en soporte electrónico portable (usb, disco duro, CD-R) de la base de datos	1. *Copiar los respaldos que se encuentran en la carpeta a soportes electrónicos portables para el resguardo de la información.*	*Administrador de la base de datos* *1 dias.*
Respaldo de los archivos de reporte que contenga datos personales	1. *Generar los reportes que serán enviados a las diferentes dependencias.*	*Encargado de traslado de reportes.* *3 dias.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 383 de 425—

	2. *Comprimir los reportes en un archivo con el nombre de la dependencia y la fecha cuando se generaron los reportes.* 3. *Guardar el archivo en un soporte electrónico.* 4. *Pedir al área de sistemas el soporte electrónico portable donde se va a guardar el archivo comprimido.* 5. *Guardar el archivo en un soporte electrónico portable.* 6. *Enviar el soporte electrónico portable al área de sistemas para su resguardo.*	

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE DAT INSTRUMENTOS 01**	
(Nombre del sistema D1)*	**Instrumentos de Orientación Educativa**	
Proceso*	**Descripción***	**Responsable***
Proceso de borrado de equipos de computo	*Reportar que equipo y de que persona es el equipo en el cual se va a realizar el borrado.* *Generar un respaldo de la información principal del usuario del equipo.* *Verificación del respaldo para evitar que contenga información de datos personales ajenos.* *Formatear el disco duro mediante la herramienta "" para evitar recuperación de información.*	*Encargado del sistema* *1 semana*
Proceso de borrado de respaldos en soporte electrónicos	*La información que se borra de estos dispositivos*	*Encargado del sistema* *1 semana*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNud5=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —384 de 425—

	solamente deberá guardar información del sistema. Formatear mediante la herramienta "" para evitar recuperación de información.	

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

La Dirección de Apoyo Técnico y la Coordinación de Orientación Educativa acordarán la cancelación del sistema mediante un escrito donde indique lo siguiente:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
   Estas fechas al menos deben de tener un mes de separación.
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
4. Solamente el Lic. Alejandro Garrido Hernández, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 385 de 425—

6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)
En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.
- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)
Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Instrumentos de Orientación Educativa que se encuentren dentro sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 386 de 425—

F) PERSONALES

Con respecto a los discos duros, cualquier software que realice un borrado de bajo nivel. Los métodos de borrado que evitan que se pueda recuperar los datos de los dispositivos de almacenamiento una vez se han eliminado son la desmagnetización, la destrucción y la sobreescritura.

La desmagnetización y la destrucción física no permiten reutilizar el dispositivo posteriormente. En la desmagnetización se expone el soporte a un campo magnético con una potencia que variará en función del tamaño del dispositivo, mientras que en la destrucción física se elimina el soporte físicamente por completo siendo imposible su reutilización. Sin embargo, el método de sobreescritura elimina la información sin que ésta pueda ser recuperada y permite volver a utilizar el dispositivo con garantías de que funcione correctamente.

Esta forma de borrado se utiliza por ejemplo en los casos en los que se pretende donar los ordenadores antiguos de una empresa, y se desea tener la seguridad de que toda la información eliminada es irrecuperable (https://www.incibe.es/protege-tu-empresa/blog/borrar-informacion-dispositivo-ciberseguridad).

Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —387 de 425—

Cuestionario de Resliencia Escolar

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**
(Nombre del sistema C1)	**Resiliencia Escolar**
Datos personales (sensibles o no) contenidos en el sistema*:	**Datos de Identificación** • Nombre • Correo electrónico • Fecha de nacimiento • Sexo **Datos de Académicos** • Escuela / Facultad • Número de cuenta • Semestre • Promedio • Turno • Tiene Beca Datos familiares • Con quien vive • Número de hermanos • Que hermano es • Tiene hijos • Estado Civil de los padres • Edad de la madre • Edad del padre • Escolaridad de la madre • Escolaridad del padre • Lugar de Residencia de la Madre • Lugar de Residencia del Padre Datos de trabajo • Si trabaja • En que trabaja
Responsable*:	DGTIC, Departamento de Instrumentos, DGOAE y Dirección de Apoyo técnico, DGOAE
Nombre*:	**Lic. José Antonio Sánchez Yllanez**
Cargo*:	**Director de Apoyo Técnico de la DGOAE**
Funciones*:	Responsable del cuidado de datos personales en los sistemas desarrollados por su área de trabajo.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 388 de 425—

Obligaciones*:	Verificar y ver que se cumplan los protocolos para el cumplimiento de los derechos ARCOP en los sistemas desarrollados en la Dirección de Apoyo Técnico.
	Encargados[5]:
(Nombre del Encargado 1*)	**M. en C. Pedro Xavier Contla Romero**
Cargo*:	**Técnico Académico Titular "A"**
Funciones*:	Desarrollo y automatización de sistemas web para la DGOAE
Obligaciones*:	Diseño, Desarrollo, Implementación, mantenimiento y actualización de Sistemas web en la DGOAE.
(Nombre del Encargado 2*)	**Dr. Libia Gómez Altamirano**
Cargo*:	**Técnica Académico Titular "A"**
Funciones*:	Coordinar la aplicación del instrumento de Resiliencia Escolar.
Obligaciones*:	Pruebas y responsable del contenido del cuestionario.
	Usuarios:
(Nombre del Usuario 1*)	**Dr. Libia Gómez Altamirano**
Cargo*:	**Técnica Académico Titular "A"**
Funciones*:	Administrador de Usuarios y Aspirantes
Obligaciones*:	Registro de alumnos, envío de información.
(Nombre del Usuario 2*)	**M. en C. Pedro Xavier Contla Romero**
Cargo*:	**Técnico Académico Titular "A"**
Funciones*:	Administrador de Usuarios
Obligaciones*:	Registro de usuarios y alumnos, envío de información, actualización de datos personales, académicos.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único*	DGOAE_DAT_RESILIENCIA_01
(Nombre del sistema C1) *	Resiliencia Escolar
Tipo de soporte: *	Soporte Electrónico
Descripción: *	Base de datos relacional, hojas de cálculo
Características del lugar donde se resguardan los soportes: *	• El alojamiento del sistema Resiliencia Escolar se encuentra en los servidores de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC). • Incorporar lo que DGTIC

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 389 de 425—

	• Toda comunicación con el sitio web está asegurado por el protocolo HTTPS para que la información viaje encriptada en la red. • Los datos se encuentran resguardados en bases de datos de MySQL que solamente tiene acceso el encargado M. en C. Xavier Contla. • La conexión a al servidor se realiza mediante SSH y un conjunto de llaves privada y pública (SSH Public Key Authentication). • El acceso a estas bases de datos es por medio de un usuario y contraseña. • Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área. • Para el acceso al sistema es por un nombre de usuario y contraseña, las cuales se generan para cada alumno usuario del sistema.

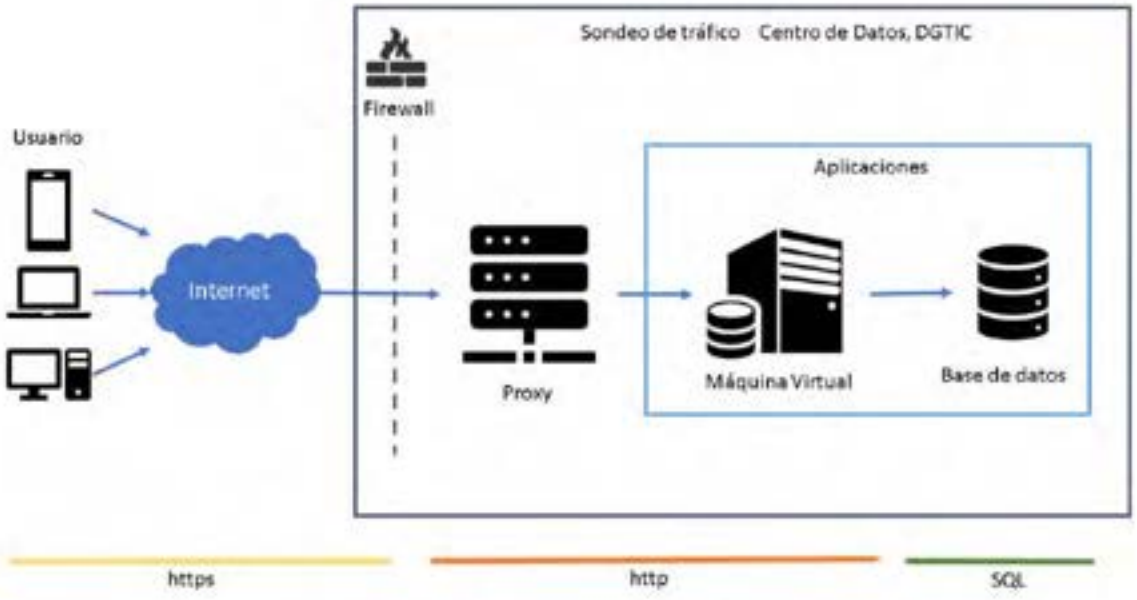


Ilustración 5 Diagrama de Seguridad

La Ilustración 1 muestra como es el acceso a la información dentro del sistema que se encuentra alojado en los servidores del Centro de Datos de DGTIC. Se tienen varios niveles de seguridad:

- La comunicación de un usuario con el sistema se hace mediante internet usando el protocolo de seguridad https, el cual cifra los datos que viajan en internet y solamente los puede leer el sistema.

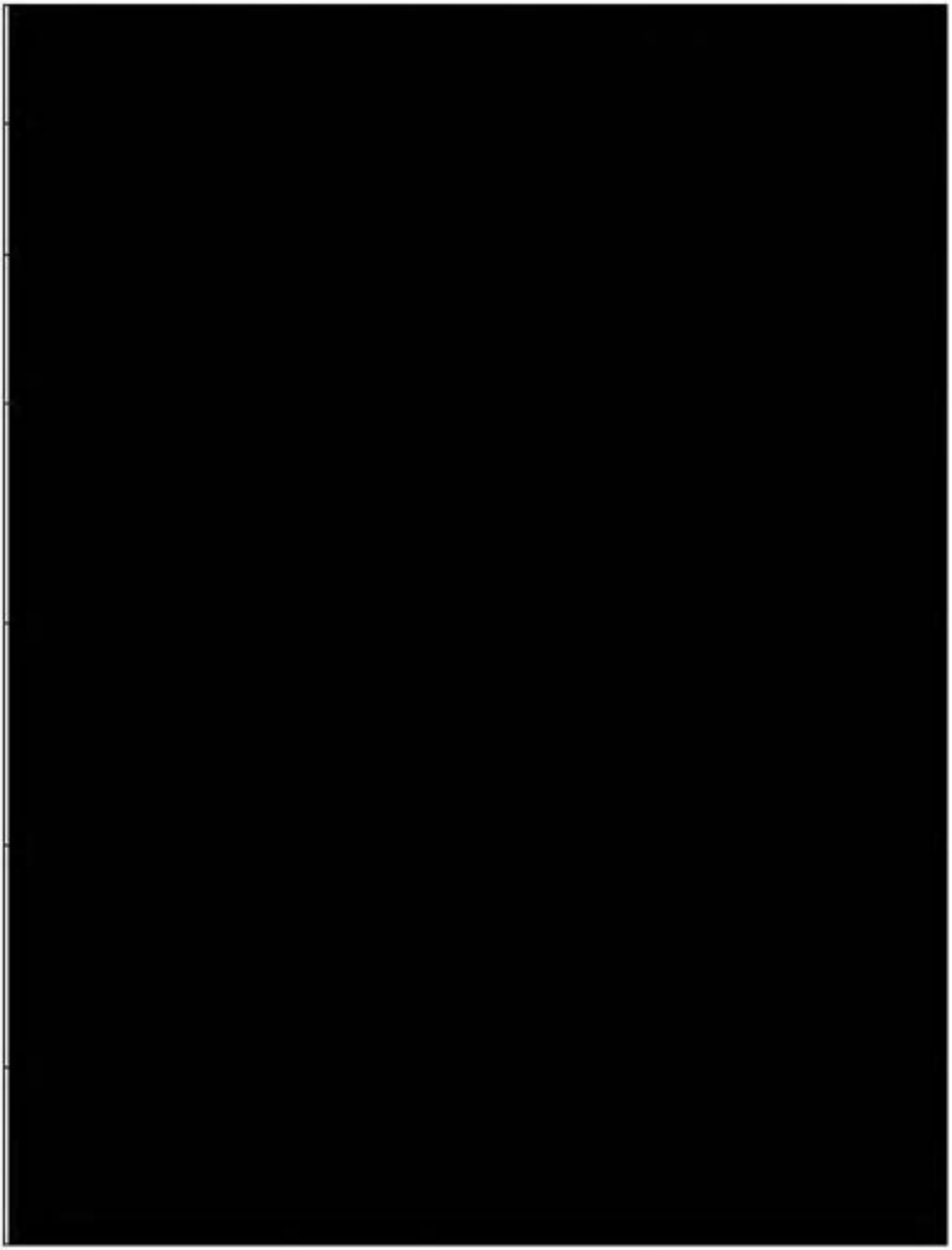
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 390 de 425—

- Dentro del Centro de datos, existe in firewall para monitorear la red entrante y saliente y decide su permite o bloquea el tráfico en función de un conjunto definido de reglas.
- Si los datos son seguros pasa a través de un proxy el cual, no solo realiza la tarea de balancear la carga a los servidores si no, es el punto de inicio a la conexión de la aplicación.
- El usuario que quiere usar la aplicación tiene un nombre de usuario y contraseña para poder acceder al aplicativo.
- Cada usuario tiene un perfil el cual tiene permisos específicos para acceder a la información de datos personales.
- Al pedir alguna información que se encuentra dentro de la base de datos, el sistema tiene un usuario y contraseña único para acceder a la información.

3. Análisis de riesgos

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**	
(Nombre del sistema C1) *	**Resiliencia Escolar**	
Riesgo*	**Impacto***	**Mitigación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 391 de 425—



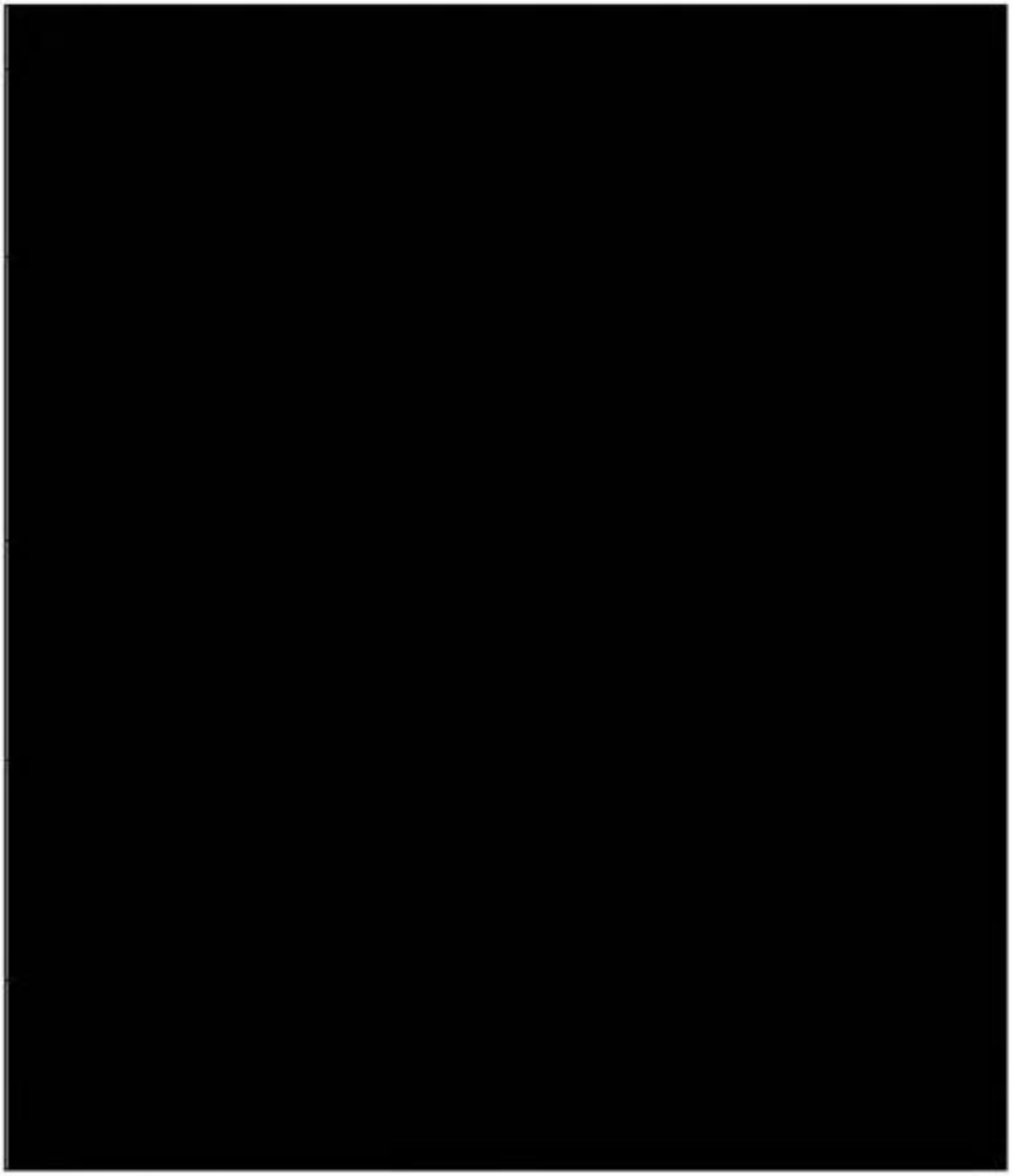
ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —392 de 425—

[redacted]

4. Análisis de brecha

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	DGOAE_DAT_RESILIENCIA_01	
(Nombre del sistema C1) *	**Resiliencia Escolar**	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]		

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 393 de 425—



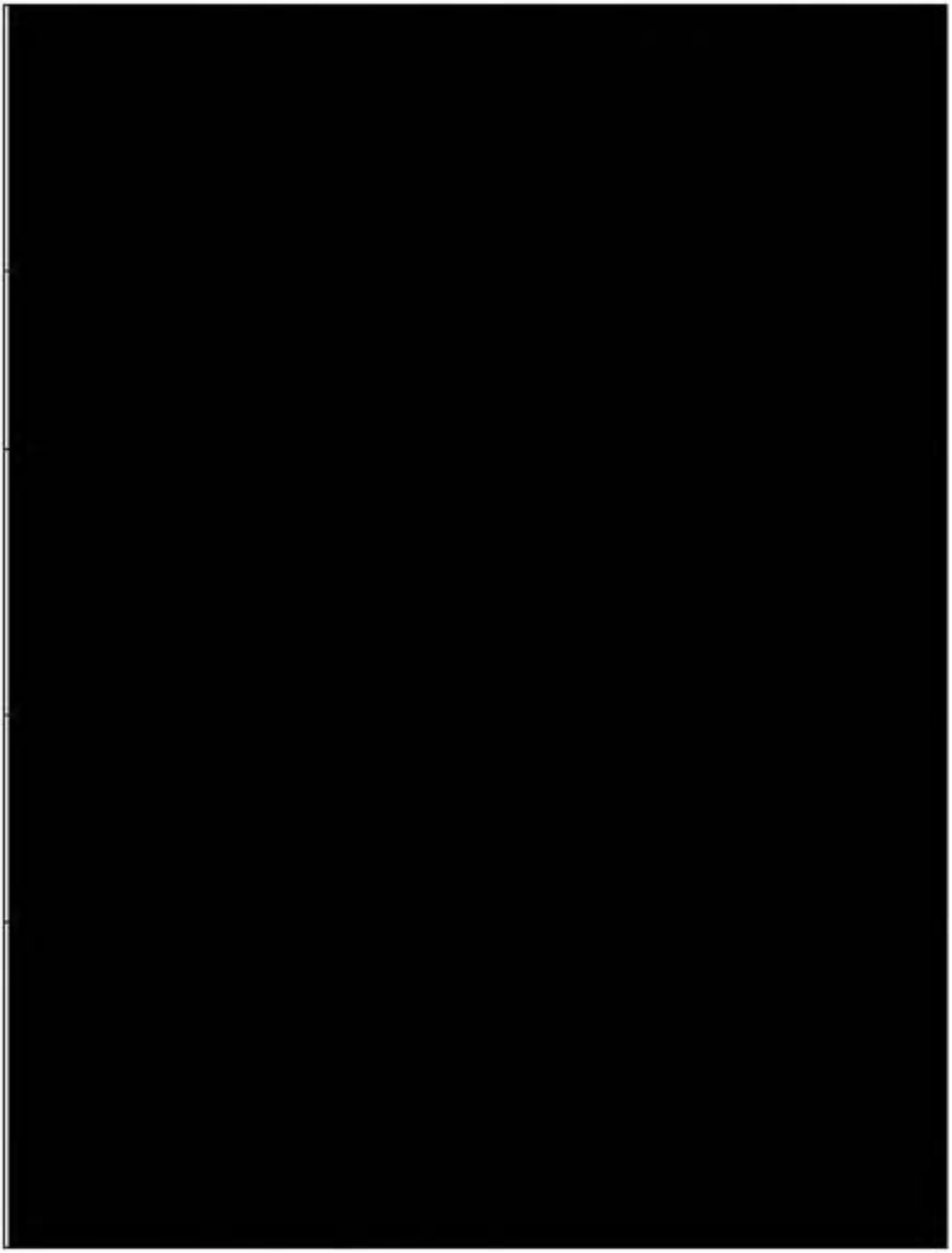
5. Plan de trabajo

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico	
Identificador único*	DGOAE DAT RESILIENCIA 01

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —394 de 425—

(Nombre del sistema C1) *	Resiliencia Escolar		
Actividad*	Descripción*	Duración*	Cobertura*
[redacted]			

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 395 de 425—



6. Medidas de seguridad implementadas

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNud8=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 396 de 425—

I. TRANSFERENCIAS DE DATOS PERSONALES

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**	
Identificador único*	**DGOAE DAT RESILIENCIA 01**
(Nombre del sistema C1)*	**Resiliencia Escolar**
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	• Por el momento no hay soporte físico
Transferencias mediante el traslado de soportes electrónicos:	• Por el momento no hay traslado por soporte electrónico físico
Transferencias mediante el traslado sobre redes electrónicas:	• Los traslados se deberán de realizar mediante el uso de correos institucionales. • Tener una lista con los correos institucionales a los cuales se les comparte los datos personales. • Todos los archivos que contengan datos personales deberán de ser cifrados para el envío de información. • Se usará una contraseña que debe de ser personal e intransferible para cada encargado. • En el caso requerido las transferencias se formalizarán mediante algún instrumento jurídico. • Cualquier documento que contenga datos personales y que sea impreso, solamente se le podrá entregar al titular de estos datos.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No aplica para este sistema.

1. Señalar las medidas de seguridad que ha implementado el área universitaria para el resguardo de los soportes físicos del sistema de manera que evite la alteración, pérdida o acceso no autorizado a los mismos.
2. Señalar en un listado las personas (nombre, cargo, funciones y obligaciones) que tienen acceso a los soportes físicos del sistema

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —397 de 425—

1. Los datos que se registran en las bitácoras actualmente:

I. El área responsable del tratamiento de datos personales en el sistema de Resiliencia Escolar realiza las siguientes acciones con respecto a las bitácoras en sistema.
   a. El administrador del servidor y DGTIC pueden acceder a las bitácoras
   b. La bitácora se encuentra en soportes electrónicos
   c. La bitácora guarda la siguiente información
      i. Fecha y hora
      ii. Función que se llamó
      iii. Llamada a SQL que se realizó a la base de datos
         1. Ver
         2. Insertar
         3. Actualizar
         4. Borrar
   d. El sistema guarda un registro de las operaciones que se hacen a la base de datos.
   e. Guarda un registro de las operaciones fallidas.
   f. Cada mes se borran las bitácoras que se generan por espacio.
   g. No se crean respaldos de las bitácoras.
   h. Las bitácoras contienen fecha, hora, acción que se realizó y mensaje.
   i. Las bitácoras van a tener una duración de 1 mes en sistema y se creará una copia que se resguardará en algún medio de almacenamiento durante dos años.

II. Con los nuevos requisitos se va a implementar el siguiente sistema de bitácoras.
   a. Se actualizarán la información que se guarda en la bitácora como sigue:
      i. Los datos que guardará
         - Fecha y hora
         - Función SQL y que realizó (Lectura, escritura, inserción)
         - El id de usuario que hizo la acción
         - Los privilegios del usuario
      iii. Estas bitácoras se van a respaldar cada mes y se guardarán por un periodo de dos años en soportes electrónicos.
   b. Se crearán tablas en la base de datos que guarden el registro de actividad por usuario que tenga acceso a datos personales y seguirá el siguiente protocolo:
      i. Los datos que guardará
         - Fecha y hora
         - Función SQL y que realizó (Lectura, escritura, inserción)
         - El id de usuario que hizo la acción
         - Los privilegios del usuario
      ii. Estas tablas que contienen el registro de actividades se respaldarán cada mes y deben de quedarse al menos 4 años resguardadas en soportes electrónicos.

IV. REGISTRO DE INCIDENTES

En caso de presentar un incidente seguir los siguientes pasos.

1. Resolver el incidente

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: — 398 de 425—

2. Pedir el archivo en formato electrónico "Registro de incidentes de datos personales"(pdf).
3. Recopilar la siguiente información:
    a. Resumen del incidente
    b. Resumen de cómo se solucionó el incidente
    c. Especificar si el incidente daño algún archivo, base de datos, servidor, respaldo etc.
    d. Fecha de inicio
    e. Fecha de término o resolución del incidente
    f. El impacto del incidente
    g. La persona quien resolvió el incidente
    h. Nombre del responsable y firma
4. El archivo de registro se actualiza y se crea un respaldo en un soporte electrónico portable para su almacenamiento.
5. La resolución del incidente tiene un tiempo máximo de 3 días hábiles.
6. El encargado de sistema deberá de registrar el incidente en un archivo donde se encuentre el resumen de lo sucedido.
7. Si el incidente es un robo o extravío de información se deberá reportar inmediatamente a los encargados y responsables del sistema, ellos avisaran al titular y a los encargados en la UNAM de lo sucedido.

La recuperación de datos de los sistemas de respaldo la podrá solicitar los encargados y el responsable del sistema.

V. ACCESO A LAS INSTALACIONES

a. Seguridad perimetral exterior

¿Qué medidas ha implementado para controlar el acceso de personas a sus instalaciones?
La Dirección General de Orientación y Atención Educativa, cuenta con un sólo edificio de dos niveles (Ex cafetería central) ubicado entre las facultades de ingeniería y arquitectura; existen dos accesos principales, uno en cada uno de los niveles, y una salida de emergencia. Los accesos son controlados por personal de vigilancia, que de acuerdo con las categorías y horarios se cubre el servicio 24 horas al día, de lunes a domingo, incluyendo días festivos y periodos vacacionales, así como los días de asueto.
Para mayor seguridad de las instalaciones las ventanas y ventanales que dan al exterior se encuentran reforzados con protecciones de herrería, así mismo la entrada de planta baja cuenta con una cortina metálica.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —399 de 425—

Actualmente las instalaciones son monitoreadas con 8 videocámaras (sólo video, sin audio) y se encuentran instaladas en el perímetro exterior del inmueble y en los dos accesos principales, la finalidad de este sistema es resguardar el patrimonio universitario, por lo que no existen cámaras instaladas en áreas comunes de trabajo y/o pasillos, que vulneren los derechos laborales o personales de quiénes visitan o laboran en esta dependencia.

Para las personas que acceden a sus instalaciones.

a) ¿Cómo las identifica?

Cada persona que ingresa es identificada por el personal de vigilancia, en caso de ser visitantes, se les pide un registro en la bitácora de visitantes.

b) ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

c) ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

b. Seguridad perimetral interior

Para las personas que acceden a dichos espacios interiores:

Las oficinas del Centro de Orientación Especializada (COE) y Departamento de Instrumentos de Orientación se encuentran de la Dirección General de Orientación y Atención Educativa en la planta baja y alta respectivamente.

1. ¿Cómo las identifica?

Las personas a quienes atendemos son: alumnado, egresadas y egresados de la UNAM.

2. ¿Cómo las autentifica?

Con una identificación oficial que se queda en resguardo del personal de vigilancia, quién entrega en cambio un gafete de visitante y se canjea al término de su visita.

3. ¿Cómo les autoriza el acceso?

En cada una de las entradas está instalado un módulo de vigilancia sin control de acceso automatizado, el acceso se brinda únicamente verbalmente.

Nota: El sistema se encuentra alojado en el Centro de Datos de DGTIC, quienes cuentan con su propio control de acceso.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —400 de 425—

En este apartado se deberá establecer un mecanismo o procedimiento institucional para la actualización de la información personal contenida en el sistema, en donde se establezca la frecuencia con la que se efectúa y la forma en que se está solicitando al titular acreditar de manera idónea sus requerimientos de rectificación de datos inexactos.

En el caso de que un titular identifique que sus datos personales son incorrectos, se podrá hacer un cambió si y solo si el titular sigue el siguiente protocolo:

1. Obtener y llenar el documento del ANEXO II donde el titular requiere una actualización en los datos personales.
2. Mandar al correo innovaoe@unam.mx lo siguiente:
    a. Adjuntar el documento firmado del ANEXO II en el correo electrónico,
3. El titular recibirá un correo donde se le avisará de la recepción del correo en un tiempo aproximado de 3 días hábiles.
4. Esperar el aviso dé que se realizó el cambio en los datos personales solicitados
5. Revisar que el cambió se realizó correctamente.
    a. Se tiene un tiempo de espera de 2 días hábiles para cualquier corrección de los datos que se cambiaron.
    b. SI todo es correcto, dejar como está.
    c. Si hay algún dato que no se cambió, favor de enviar el dato incorrecto con el correcto como respuesta del aviso. Y verificar nuevamente. Estos cambios se deben de realizar en menos de 12 horas.
    d.

Para los responsables y encargados de cambiar los datos, seguir el siguiente protocolo.

1. Al recibir el correo, el encargado responderá al titular:
    a. El cambio se realizará dentro de 3 días hábiles.
    b. Hay que informar que persona va a realizar el cambio, deberá ser la misma que mande la respuesta de los días hábiles.
2. Levantar un reporte de la incidencia.
3. Se realiza el cambio.
4. Se envía un correo para que el titular verifique que el cambio se hizo correctamente pidiendo que mande una respuesta si el cambio se hizo correctamente o no.
    a. Si se recibe una respuesta afirmativa, ponemos fin a la incidencia.
    b. Si se recibe un correo donde sigue la inconsistencia en los datos, revisar de nuevo la petición y hacer el cambio inmediatamente y volver a confirmar que se realizó el cambio.
    c. Si no se recibe el correo, después de dos días del envío del correo de verificación de la realización de cambios en los datos personales. Podemos poner fin a la incidencia.
    d. Si llegara la información después de los dos días hábiles el titular deberá de volver a pedir el cambio.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —401 de 425—

Las medidas de seguridad previstas a continuación en los incisos VII al IX, sólo aplican para soportes electrónicos.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.
Toda comunicación con el sitio web está asegurado por el protocolo ***https*** para que la información viaje encriptada en la red.
Aplicación ***Resiliencia Escolar*** tiene la siguiente configuración:

1. Para acceder al sistema se cuenta con un usuario y contraseña.
2. El usuario está definido por el número de cuenta o por el correo electrónico.
3. La contraseña se genera a partir de un "dato personal".
4. La contraseña se guarda encriptada en la base de datos y se usa un método de encriptación para poder obtenerla al momento de iniciar la sesión.
5. El sistema cuenta con los siguientes perfiles
    a. **Usuario** El usuario solo podrá ver sus datos personales, Nombres, Apellidos, Fecha de nacimiento, Sexo, Datos de Académicos, Datos Familiares y Datos Laborales en caso de que trabaje y Número de cuenta si es alumno universitario.

Contenedor de la máquina virtual tiene la siguiente configuración:

1. Se crea un perfil, usuario y contraseña para el uso de la máquina virtual
2. Se conecta a través de una IP fija o mediante SSH y un conjunto de llaves privada y pública (*SSH Public Key Authentication*).
3. El usuario tiene permiso de ***root*** para hacer la configuración de servidor.

Base de datos tiene la siguiente configuración:

1. El acceso a estas bases de datos es por medio de un usuario y contraseña que lo tiene el administrador.
2. El administrador de la base de datos puede crear, modificar, borrar, actualizar lo siguiente:
    a. Esquema de la base de datos
    b. Tablas
    c. Registros
    d. Hacer respaldos de la información de las bases
    e. Creación de usuarios de la base
    f. Modificación de privilegios de los usuarios

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —402 de 425—

Todos los archivos que se comparten se hacen en hojas de cálculo y se envían a través de los correos institucionales a los encargados de cada área.

Resumen de la verificación de perfiles de usuario y contraseñas:

1. Modelo de control de acceso:

- **a)** ¿Es obligatorio (etiquetas para objetos y acreditación para sujetos)? **SI**
- **b)** ¿Es discrecional (matriz de control de acceso)? **No**
- **c)** ¿Está basado en roles (perfiles) o grupos? **Si**
- **d)** ¿Está basado en reglas? **Si**

2. Perfiles de usuario y contraseñas en el sistema operativo de red: NO APLICA

- **a)** ¿Cuenta con un sistema operativo de red instalado en sus equipos? **NO**
- **b)** ¿Proporciona dicho sistema operativo un manejo riguroso de perfiles de usuario y contraseñas? **NO APLICA**
- **c)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **NO APLICA**

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

- **a)** ¿Ofrece dicho software un manejo riguroso de perfiles de usuario y contraseñas? **Si**
- **b)** ¿Cifra el mencionado software los nombres de usuario y las contraseñas cuando los almacena? **Se cifra la contraseña, pero no el nombre de usuario**

4. Administración de perfiles de usuario y contraseñas:

- **a)** ¿Quién da de alta nuevos perfiles? **Administrador**
- **b)** ¿Quién autoriza la creación de nuevos perfiles? **Encargado de los Usuarios**
- **c)** ¿Se lleva registro de la creación de nuevos perfiles? **Si**

5. Acceso remoto al sistema de tratamiento de datos personales:

- **a)** ¿Requieren los usuarios acceso remoto al equipo de cómputo que por lo general utilizan para trabajar con el sistema? **NO**
- **b)** ¿Requiere el administrador acceso remoto al equipo donde reside el sistema para realizar tareas de mantenimiento? **SI, solo el administrador de la base puede entrar por este medio**
- **c)** ¿Cómo se evita el acceso remoto no autorizado? **Mediante la autenticación por llave y por IP**

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos del sistema los realiza el encargado del sistema en la DGOAE.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —403 de 425—

1. Los respaldos se realizan manualmente y completos.
2. El respaldo se realiza cada mes
3. Si se realiza alguna aplicación del instrumento, acabando el periodo de aplicación se obtiene un respaldo manual.
4. Estos respaldos se quedan en un disco duro.
5. Los respaldos los resguarda el encargado en la Dirección de Apoyo Técnico.
6. Los respaldos se realizan de forma automática cada tercer día y guardan el estado de la máquina virtual. donde se aloja el sistema.

IX. PLAN DE CONTINGENCIA

1. Plan de contingencia que garantiza la continuidad de la operación del sistema.
   - Tener respaldos de la base de datos y del código.
   - Ponerse en contacto con el jefe de departamento de Informática y pedirle que solicite a DGTIC un espacio para montar el sistema y la base de datos.
   - Los requerimientos con los que debe contar este espacio son los requeridos por la versión del framework que utiliza el sistema a recuperar.
   - El tiempo en que DGTIC entregue el espacio es variado, ya que depende de la carga de trabajo que tengan, sin embargo, se les puede decir que es de carácter urgente.
   - Una vez que nos hayan entregado el espacio, nos deberán proporcionar el usuario y contraseña para acceder como usuario del sistema operativo y también las credenciales de la base de datos.
   - Es importante conectar el software de administración de bases de datos con la nueva base de datos para que la visualización sea un poco más fácil. Una vez hecha la conexión se carga el respaldo de la base de datos.
   - En un navegador se comprueba que el sitio sea visible y la conexión a la base de datos.
   - Realizar pruebas al sistema de inicio de sesión, cierre de sesión, registro de universitarias y universitarios, consulta del programa del Encuentro Virtual de Empleabilidad, inscripción y baja a las diferentes actividades que ofrece éste.
2. El tiempo que se demore DGTIC en darnos el nuevo espacio fue de un día, ya que se le explico que era de carácter urgente.
3. No aplica.

7. Mecanismos de monitoreo y revisión de las medidas de seguridad

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —404 de 425—

7.1 Herramientas y recursos para monitoreo de la protección de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**	
(Nombre del sistema C1) *	**Resiliencia Escolar**	
Recurso*	**Descripción***	**Control***
Bitácoras generadas por DGTIC	Las bitácoras generadas por DGTIC nos indicaran el tráfico que existen en el servidor	Se hace manual y solamente será usada cuando se genere un ataque al sistema
Bitácoras generadas por el servidor	Las bitácoras generadas por el servidor nos darán pruebas de cómo se realizan las peticiones a la base de datos, así como los usuarios que están realizando las actividades dentro del sistema.	Se hace manual la revisión buscando palabras claves para la identificación de los registros que tengan algún acceso indebido al sistema.
Bitácoras generadas en la base de datos	Se crearán tablas donde se maneja que acciones el usuario ha realizado dentro del sistema, así como el ingreso y salida de la plataforma.	Se usa SQL para el registro de la actividad dentro de la base.
Wireshark	Se hace una revisión de parte del cliente para saber qué es lo que puede ver y asegurar que los datos viajan encriptados.	Wireshark se usa para la identificación de paquetes por etiquetas TCP y IP, analizar que se envía y que se recibe.
Ambiente de pruebas	Se debe de tener una computadora donde se pueda hacer pruebas y que solamente se pueda acceder localmente o en red local.	Se tiene una computadora con *Centos* 7 para poder hacer las pruebas necesarias.
Nmpa, netcat, Tcpdump	Utilizar las herramientas para la detección de fallos y verificación del	Las herramientas son libres y se hará una revisión cada semestre con estas herramientas

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —405 de 425—

	funcionamiento y seguridad del sistema	

7.2 Procedimiento para la revisión de las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT RESILIENCIA 01**	
(Nombre del sistema C1) *	**Resiliencia Escolar**	
Medida de seguridad*	**Procedimiento***	**Responsable***
Contar con las medidas de seguridad que DGTIC pide.	Se seguirán las recomendaciones que DGTIC propone para la seguridad en los sistemas	Administrador del Sistema 28 días laborables
Contar con un repositorio para manejo de versiones	Tener un sitio donde se realice el manejo de versiones	Administrador del Sistema 5 días laborables
Lista de verificación de seguridad	Diseñar un documento donde llevemos una lista de verificación sobre las reglas de seguridad que debe de tener el sistema	Administrador del Sistema 28 días laborables

7.3 Resultados de la evaluación y pruebas a las medidas de seguridad

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE DAT RESILIENCIA 01**	
(Nombre del sistema C1)*	**Resiliencia Escolar**	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Se deberá de mandar la aplicación al CERT en DGTIC para la evaluación del sistema	I. *Ausencia de encabezados de seguridad* II. *Envio de Credenciales en texto claro*	*Pedro Xavier Contla Romero* *4 de abril de 2019*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —406 de 425—

7.4 Acciones para la corrección y actualización de las medidas de seguridad

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**	
(Nombre del sistema C1)*	**Resiliencia Escolar**	
Medida de seguridad*	**Acciones***	**Responsable***
Se resolvieron los diferentes riesgos de seguridad según el reporte de DGTIC	I. *Se implementó la sobreescritura de cabeceras* II. *Se implementó el certificado de Let's Encrypt.*	*Pedro Xavier Contla Romero 15 de abril del 2019*

8. Programa específico de capacitación

8.1. Programa de capacitación a los responsables de seguridad de datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**		
(Nombre del sistema C1)*	**Resiliencia Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a los datos personales	Concientizar a los usuarios del sistema sobre los datos personales, que son, como son vulnerables, cual es el impacto, etc.	Duración: Un día Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y tenga acceso a los datos personales.
Resguardo de información mediante los protocolos antes establecidos	Contar con un documento donde explique los objetivos principales de la implementación	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los usuarios del sistema. Cada vez que exista algún nuevo usuario que opere el sistema y

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —407 de 425—

	de la seguridad para el sistema		tenga acceso a los datos personales.
Programación de los sistemas usando framework seguros	Estar actualizando las herramientas de desarrollo conforme avanza la tecnología	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores que actualicen los sistemas tendrán que buscar si lo que se usa es seguro para el resguardo de los datos personales. Cada año generar el análisis sobre la tecnología que se usa.
****Pruebas de obtención de datos mediante perfiles***	Realizar pruebas sobre los diferentes perfiles en el sistema	Duración: una semana Inicio: Por definir Termino: Por definir	Contar con el análisis de los perfiles y sus privilegios del sistema Al incorporar un nuevo perfil al sistema
Creación de Certificados SSL	Contar con un documento en donde se documente como generar in certificado SSL por medio de Let's Encrypt	Duración: dos semanas Inicio: Por definir Termino: Por definir	Los desarrolladores podrán contar con un método para generar sus certificados mientras se obtiene el principal. Al incorporar un nuevo desarrollador al equipo
Curso de protección a las máquinas virtuales	Contar con un curso de administrador tipo Linux para capacitar a nuevos administradores sobre la configuración en el servidor	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Curso de hacker ético para pruebas en el sistema	Contar con un curso para probar los sistemas en desarrollo.	Duración: un mes Inicio: Por definir Termino: Por definir	Los desarrolladores y administradores del servidor y base de datos Al incorporar un nuevo desarrollador al equipo Al desarrollar un nuevo sistema*
Protocolo interno para verificación de la seguridad	Contar con un documento que indique los pasos que se deben	Duración: dos semanas Inicio: Por definir	Los desarrolladores y administradores del servidor y base de datos

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —408 de 425—

	llevar para probar la seguridad de los sistemas	Termino: Por definir	Antes de salir a producción. *

Nota: La capacitación se realiza cuando los usuarios aumenten, por lo que las fechas no están definidas. Por el momento los que usan el sistema ya están capacitados

8.2. Programa de difusión de la protección a los datos personales

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**		
(Nombre del sistema C1) *	**Resiliencia Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Aviso integral dentro de la DGOAE	La distribución es en la página del sistema antes de ingresar al sitio web con las credenciales del usuario.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Aviso particular del área responsable del dar el servicio por medio del sistema	La distribución es en la página del sistema y está al alcance en dos lugares. Si existe registro, antes de darle aceptar. Si ya están registrados, donde se despliegan los datos personales.	Desde la fecha en que el sistema está en línea hasta que se cancele o deje de funcionar el sitio web.	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.
Creación de videos informativos de los datos personales de los titulares están resguardados en el sistema.	LA distribución podrá ser mediante las redes sociales y los sitios de los sistemas para informar al usuario de una manera rápida a cerca del manejo de los datos personales en la DGOAE.	Duración: permanente Inicio: Por definir Termino: Por definir	Usuario titular de los datos personales. Cada vez que se haga algún cambio para la protección de los datos personales.

9. Mejora continua

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —409 de 425—

9.1. Actualización y mantenimiento de sistemas de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT RESILIENCIA 01**		
(Nombre del sistema C1) *	**Resiliencia Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Análisis de los reportes de los usuarios acerca de los bugs, mal funcionamiento y documentación sobre el funcionamiento del sistema.	*Contar con la información necesaria para evaluar los puntos en donde se necesita hacer una actualización del sistema.*	Duración: dos semanas Inicio: Por definir Termino: Por definir	*Actualización y mejora del sistema actual, parcialmente.*
Actualización de mensajes de error y éxito.	*Agregar unas respuestas en para el Módulo de los Administradores para que tenga una mejor retroalimentación de las modificaciones o borrado que se realiza.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Mejor retroalimentación a los administradores para el uso de las funcionalidades del sistema.*
Pantallas de verificación	*Agregar pantallas antes de realizar algún cambio para evitar modificaciones no deseadas.*	Duración: un mes Inicio: Por definir Termino: Por definir	*Total*

9.2. Actualización y mantenimiento de equipo de cómputo

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**			
Identificador único*	**DGOAE DAT RESILIENCIA 01**		
(Nombre del sistema C1) *	**Resiliencia Escolar**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —410 de 425—

Generar un inventario de los recursos con los que se cuenta para dar mantenimiento al sistema	*Obtener información de cuantos equipos se tienen en uso para el desarrollo del sistema y en qué estado se encuentran*	Duración: Cada año Inicio: Por definir Termino: Por definir	*Total*
Actualizar o cambiar los equipos de desarrollo lo necesiten	*Contar con las herramientas de trabajo en buen estado para el desarrollo de sistemas*	Duración: 1 mes Inicio: Por definir Termino: Por definir	*Total*

9.3. Procesos para la conservación, preservación y respaldos de información

Dirección General de Orientación y Atención Educativa **Dirección de Apoyo Técnico**		
Identificador único*	**DGOAE DAT RESILIENCIA 01**	
(Nombre del sistema C1)*	**Resiliencia Escolar**	
Proceso*	**Descripción***	**Responsable***
Respaldo en soporte electrónico de la base de datos	*1. Realizar un respaldo de la base de datos.* *2. El nombre del archivo respaldo es nombre de la base y la fecha cuando se realizó el respaldo* *3. Guardarlo en la carpeta donde se encuentran los demás respaldos.*	*Administrador de la base de datos* *3 días.*
Respaldo en soporte electrónico portable (USB, disco duro, CD-R) de la base de datos	*1. Copiar los respaldos que se encuentran en la carpeta a soportes electrónicos portables para el resguardo de la información.*	*Administrador de la base de datos* *1 días.*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —411 de 425—

Respaldo de los archivos de reporte que contenga datos personales	1. *Generar los reportes que serán enviados a las diferentes dependencias.* 2. *Comprimir los reportes en un archivo con el nombre de la dependencia y la fecha cuando se generaron los reportes.* 3. *Guardar el archivo en un soporte electrónico.* 4. *Pedir al área de sistemas el soporte electrónico portable donde se va a guardar el archivo comprimido.* 5. *Guardar el archivo en un soporte electrónico portable.* 6. *Enviar el soporte electrónico portable al área de sistemas para su resguardo.*	*Encargado de traslado de reportes. 3 días.*

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Dirección General de Orientación y Atención Educativa Dirección de Apoyo Técnico		
Identificador único*	**DGOAE_DAT_RESILIENCIA_01**	
(Nombre del sistema C1) *	**Resiliencia Escolar**	
Proceso*	**Descripción***	**Responsable***
Proceso de borrado de equipos de computo	*Reportar que equipo y de que persona es el equipo en el cual se va a realizar el borrado. Generar un respaldo de la información principal del usuario del equipo. Verificación del respaldo para evitar que contenga*	*Encargado del sistema 1 semana*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —412 de 425—

	información de datos personales ajenos. Formatear el disco duro mediante la herramienta "" para evitar recuperación de información.	
Proceso de borrado de respaldos en soporte electrónicos	*La información que se borra de estos dispositivos solamente deberá guardar información del sistema. Formatear mediante la herramienta "" para evitar recuperación de información.*	*Encargado del sistema 1 semana*

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —413 de 425—

10. Procedimiento para la cancelación de un sistema de tratamiento de datos personales

(Informar y describir el procedimiento para la cancelación de un sistema de tratamiento de datos personales.)

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

La Dirección de Apoyo Técnico y la Coordinación de Orientación Educativa acordarán la cancelación del sistema mediante un escrito donde indique lo siguiente:

a. Fecha cuando deja de dar servicio el sistema
b. Fecha de cancelación de sistema
   Estas fechas al menos deben de tener un mes de separación.
c. Motivo de la cancelación
d. Si existe un sistema que lo remplaza, poner la información del nuevo sistema.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Al tener las fechas de dar de baja el servicio y la cancelación del sistema, entra el periodo de bloqueo del sistema. Al menos se debe de tener un mes para llevar a cabo el bloqueo del sistema. Para el bloque del sistema se llevará a cabo las siguientes acciones:

1. Informar a los usuarios que el sistema está bloqueado y poner el aviso del tratamiento de datos que ser hará cuando se quite el sistema.
2. Informar a los responsables en DGTIC que el sistema se dará de baja, si es que se requiere.
3. Deshabilitar los usuarios de ingreso al sistema (inicio de sesión).
4. Solamente el M. en C. Pedro Xavier Contla Romero, podrá tener acceso durante el bloqueo para cualquier información que necesite obtener del sitio.
5. Una semana antes, informar a los usuarios que tienen acceso durante el bloqueo que les queda una semana.
6. Al término del periodo de bloqueo desactivar los últimos accesos al sistema.
7. Bajar del servidor el sistema para que no pueda ser visto por red.

(Señalar el periodo de bloqueo, considerando los plazos de prescripción para el ejercicio de algún derecho por parte de los titulares de conformidad con la normatividad de cada área universitaria. Asimismo, se debe señalar las condiciones y el procedimiento que se seguirá para realizar el bloqueo)

C) Medidas de seguridad para el bloqueo y posterior supresión del sistema DE TRATAMIENTO DE DATOS PERSONALES:

(Describir las medidas de seguridad aplicables al periodo de bloqueo y la supresión del sistema, considerando el nivel de protección requerido en virtud del tipo de datos personales contenidos en el sistema)
En un documento:

- Listar los datos personales que estarán disponibles durante un periodo en las bases de respaldo.
- Definir cómo se van a usar esos datos y tener un registro de cómo se van a tratar esos datos.

ID del Documento: gIPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —414 de 425—

- Definir el tiempo que se van a quedar los datos de la base de datos, para su uso posterior (estadísticas, análisis, etc.)
- Definir donde se va a quedar respaldado y cuánto tiempo antes de su eliminación total.
- Finalmente seguir el modo de Borrado definitivo si es necesario.
- El tiempo será definido por el COE para su resguardo y acceso a la información de los datos.

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

(Describir el procedimiento para suprimir el sistema, una vez cumplido el plazo de bloqueo)
Después de hacer el respaldo y de bajar el sistema de la red. Comunicarse con el administrador del servidor para borrar todos los aplicativos del Resiliencia Escolar que se encuentren dentro sistema.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Con respecto a los discos duros, cualquier software que realice un borrado de bajo nivel. Los métodos de borrado que evitan que se pueda recuperar los datos de los dispositivos de almacenamiento una vez se han eliminado son la desmagnetización, la destrucción y la sobreescritura.
La desmagnetización y la destrucción física no permiten reutilizar el dispositivo posteriormente. En la desmagnetización se expone el soporte a un campo magnético con una potencia que variará en función del tamaño del dispositivo, mientras que en la destrucción física se elimina el soporte físicamente por completo siendo imposible su reutilización. Sin embargo, el método de sobreescritura elimina la información sin que ésta pueda ser recuperada y permite volver a utilizar el dispositivo con garantías de que funcione correctamente.
Esta forma de borrado se utiliza por ejemplo en los casos en los que se pretende donar los ordenadores antiguos de una empresa, y se desea tener la seguridad de que toda la información eliminada es irrecuperable
(https://www.incibe.es/protege-tu-empresa/blog/borrar-informacion-dispositivo-ciberseguridad).
Para nuestro sistema se ocupará la sobreescritura de discos y en casos de especiales la destrucción física o desmagnetización.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNu6s=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —415 de 425—

Unidad Administrativa

Sistema Institucional de Compras SIC

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0001/2022**
(Nombre del sistema A1) *	**Sistema Institucional de Compras SIC**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, RFC, direcciones, teléfonos personales, firmas autógrafas, correo electrónico
Responsable*:	
Nombre*:	**Adrián Josué Saúl Castellanos**
Cargo*:	**Jefe de Bienes, Suministros y Servicios Generales**
Funciones*:	Consulta, registro, modificación. Consulta de RFC de proveedores, números de contacto particulares y celular, correo electrónico, firma electrónica de usuarios que autorizan operaciones, firma personal, firma jefe de la Unidad Administrativa, firma de representantes legales de proveedores y nombres de contactos con proveedores.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*:	DGOAE/UA/0001/2022
(Nombre del sistema A1*)	**Sistema Institucional de Compras SIC**
Tipo de soporte:*	Soporte físico y electrónico
Descripción:*	Base de datos y formatos físicos
Características del lugar donde se resguardan los soportes:*	Físicos: Oficina del Jefe de Bienes, Archivero 1, 3er rack Electrónico: La responsabilidad recae en Dirección General de Proveeduría

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —416 de 425—

Sistema Admininstrativo Integral UNAM

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0002/2022**
Sistema (Nombre del A2)*:	**Sistema Administrativo Integral UNAM**
Datos personales contenidos en el sistema*:	
	Responsable:
Nombre*:	**Enrique Corrales González**
Cargo*:	**Jefe de la Unidad Administrativa**
Funciones*:	Consulta, registro, modificación. Nombres de usuarios, contraseñas y RFC de usuarios.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.
	Encargados:
(Nombre del Encargado 1*)	**Adrián Josué Saúl Castellanos**
Cargo*:	**Jefe de Bienes, Suministros y Servicios Generales**
Funciones*:	Consulta de nombres, usuarios, contraseñas y RFC de usuarios
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.
(Nombre del Encargado 2*)	Ángel Pitol Hernández
Cargo*:	Almacenista
Funciones*:	Consulta y registro de usuarios, contraseñas y RFC de usuarios.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.
	Usuarios:

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —417 de 425—

(Nombre del Usuario 1*)	Jefes de Dpto., Directores de Área, y Coordinaciones de la DGOAE
Cargo*:	Directores, Coordinadores y Jefes de Departamento

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*	DGOAE/UA/0002/2022
(Nombre del sistema *)	Sistema Administrativo Integral UNAM
Tipo de soporte*:	Soporte físico y electrónico
Descripción*:	Base de datos y formatos físicos
Características del lugar donde se resguardan los soportes*:	Físicos: Almacén. Escritorio 1, Archivero Electrónico. La responsabilidad recae en la Dirección General de Presupuesto

Sistema Integración de Personal

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	DGOAE/UA/0003/2022
Sistema (Nombre del A2)*:	**Sistema Integración de Personal**
Datos personales contenidos en el sistema*:	Nombre, RFC, CURP, domicilio, número telefónico, sueldo, historial dentro de la UNAM, beneficiarios por pago de marcha.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*	DGOAE/UA/0003/2022
(Nombre del sistema A3*)	Sistema Integración de Personal
Tipo de soporte*:	Soporte físico y electrónico

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —418 de 425—

Descripción*:	Base de datos y formatos físicos
Características del lugar donde se resguardan los soportes*:	Físicos: Oficina del Jefe de Bienes, Archivero 1, 3er rack Electrónico: La responsabilidad recae en Dirección General del Patrimonio Universitario

Sistema de Control Patrimonial

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0004/2022**
Sistema (Nombre del A2)*:	**Sistema Integral de Control Patrimonial (SICOP)**
Datos personales contenidos en el sistema*:	RFC, domicilio, nombres de proveedores.
	Responsable:
Nombre*:	**Adrián Josué Saúl Castellanos**
Cargo*:	**Jefe de Bienes, Suministros y Servicios Generales**
Funciones*:	Consulta y registro de RFC de proveedores.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*	DGOAE/UA/0004/2022
(Nombre del sistema A1*)	Sistema Integral de Control Patrimonial (SICOP)
Tipo de soporte:*	
Descripción:*	
Características del lugar donde se resguardan los soportes:*	

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —419 de 425—

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —420 de 425—

Registro remoto de trámites para pago

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	DGOAE/UA/0005/2022
(Nombre del sistema A1) *	**Registro remoto de tramites para pago**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, RFC, número de cuenta UNAM, firmas autógrafas
Responsable*:	
Nombre*:	**Martha Araceli Villegas Ullrich**
Cargo*:	**Jefa de departamento de Presupuesto**
Funciones*:	Registro.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único**	DGOAE/UA/0005/2022
(Nombre del sistema A1*)	Registro remoto de trámites para pago
Tipo de soporte:*	Soporte físico y electrónico
Descripción:*	Base de datos y formatos físicos
Características del lugar donde se resguardan los soportes:*	Física: Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con libreros que

	permiten la conservación adecuada de los documentos, de la Jefatura de presupuesto, Librero 1, nivel 5 Electrónico: La responsabilidad recae en Tesorería UNAM- Dirección General de Control Presupuestal

Factura Fiscal Digital

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0006/2022**
Sistema (Nombre del A2)*:	**Factura fiscal digital**
Datos personales contenidos en el sistema*:	Nombre, RFC, correo electrónico.
	Responsable:
Nombre*:	**Martha Araceli Villegas Ullrich**
Cargo*:	**Jefa de departamento de presupuesto**
Funciones*:	Consulta, registro, modificación.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*	DGOAE/UA/0006/2022
(Nombre del sistema A2*)	Factura fiscal digital
Tipo de soporte*:	Soporte físico y electrónico
Descripción*:	Expediente
Características del lugar donde se resguardan los soportes*:	Física: Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con libreros que

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —421 de 425—

	permiten la conservación adecuada de los documentos de la Jefatura de presupuesto, Librero 1, nivel 5. Electrónico: La responsabilidad recae en Patronato Universitario.

Sistema de Información de la Administración Universitaria

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0007/2022**
(Nombre del sistema A1) *	**Sistema de Información de la Administración Universitaria**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, RFC, CURO, razón social, dirección, número telefónico, correo electrónico
Responsable*:	
Nombre*:	**Martha Araceli Villegas Ullrich**
Cargo*:	**Jefa de departamento de Presupuesto**
Funciones*:	Consulta.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*	**DGOAE/UA/0007/2022**
(Nombre del sistema A3*)	Sistema de información de la administración universitaria
Tipo de soporte*:	Soporte físico y electrónico
Descripción*:	Base de datos y formatos físicos
Características del lugar donde se resguardan los soportes*:	Oficina con ventilación natural, luz natural y artificial, puerta de acceso de madera y chapa, aislada de humedad, con libreros que permiten la

ID del Documento: gIrPdH8ZIn+0FpWtuTZETKtsDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —422 de 425—

	conservación adecuada de los documentos de la Jefatura de presupuesto, Librero 1, nivel 5. Electrónico: La responsabilidad recae en la Dirección General de control Presupuestal-Patronato Universitario.

Aplicaciones finanzas

1. Inventario de sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa **Unidad Administrativa**	
Identificador único*	**DGOAE/UA/0008/2022**
(Nombre del sistema A1) *	**Aplicaciones finanzas**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombres, RFC
Responsable*:	
Nombre*:	**Martha Araceli Villegas Ullrich**
Cargo*:	**Jefa de departamento de Presupuesto**
Funciones*:	Registro, consulta.
Obligaciones*:	Mantener y resguardar la información contenida en el sistema, garantizando la protección de mi usuario y contraseña.

2. Estructura y descripción de los sistemas de tratamiento de datos personales

Dirección General de Orientación y Atención Educativa Unidad Administrativa	
Identificador único*:	DGOAE/UA/0008/2022
(Nombre del sistema A4*)	**Aplicaciones finanzas**
Tipo de soporte*:	Electrónico
Descripción*:	Base de datos
Características del lugar donde se resguardan los soportes*:	Electrónico: La responsabilidad recae en la Dirección General de Finanzas-Patronato Universitario.

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —423 de 425—

Aprobación del Documento de Seguridad

Dirección	Desarrollo	Revisó	Aprobó
Dirección de Orientación Educativa	Mtro. Marco Antonio Bonaparte Madrigal Jefe de Departamento de Programas y Proyectos de Orientación Educativa Mtro. Pedro Benitez Bautista Jefe de Departamento de Informática	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Mtra. Telma Ríos Condado Directora de Orientación Educativa dgoae.orientacion@unam.mx
Dirección de Becas y Enlace con la Comunidad	Mtra. Esperanza Vitela Ibañez Jefa del Departamento de Enlace con la Comunidad Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Dr. Mauricio Reyna Lara Director de Becas y Enlace con la Comunidad mreyna@unam.mx
Dirección de Servicio Social	Jorge Olguín Carro Asistente de Procesos del Departamento de Registro y seguimiento	Lic. Socorro Becerril Quintana Técnico Académico Asociado C Tiempo Completo Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Lic. Claudia Navarrete García Directora de Servicio Social y Voluntariado Teléfono: 56220440 claudiang@unam.mx
Dirección de Planeación	Mtro. Víctor Arturo Morales Díaz. Técnico académico. Mtro. Pedro Benitez Bautista Jefe de Departamento de Informática	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Lic. Laura Patricia Montoya Jiménez Directora de Planeación dgoae.planeacion@unam.mx
Dirección de Apoyo Técnico	Mtro. Pedro Benitez Bautista Jefe de Departamento de Informática	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Lic. José Antonio Sánchez Yllanez Director de Apoyo Técnico dgoae.dat@unam.mx
Centro de Orientación Educativa	M. en C. Pedro Xavier Contla Romero.	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Mtra. Wendy Abigail Bautista Montoya Coordinadora del Centro de

ID del Documento: gIPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNudS=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —424 de 425—

	Técnico académico Titular 'A' Tiempo Completo Mtro. Pedro Benitez Bautista Jefe de Departamento de Informática		Orientación Educativa dgoae.coe@unam.mx
Unidad Administrativa	C.P. Martha Araceli Villegas Ullrich Jefa del Departamento de Presupuesto Lic. Adrián Josué Saúl Castellanos Jefe del Departamento de Bienes, Suministros y Servicios Generales	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas	Mtro. Enrique Corrales González Jefe de la Unidad Administrativa Teléfono 55 5622-0453 dgoae.ua@unam.mx

Integro el Documento:	Ing. Antonio Baruch Cuevas Ortiz Coordinador de Sistemas 5556220479 dgoae.sistemas@unam.mx
Autorizó:	Dr. Germán Alvarez Diaz de León. Director General de Orientación y Atención Educativa. dgoae.direccion@unam.mx
Fecha de aprobación:	**30 de Junio de 2022**

ID del Documento: gIrPdH8ZIni+0FpWtuTZETKisDGzBuuCzNtqNULNuds=
Fecha de procesamiento: 2022-08-17T09:55:01
Páginas: —425 de 425—