DOCUMENTO DE SEGURIDAD
DEL

CENTRO DE CIENCIAS DE LA COMPLEJIDAD

Enero 2024

ÍNDICE

INTRODUCCIÓN 3

NORMATIVIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES 4

CENTRO DE CIENCIAS DE LA COMPLEJIDAD 5

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES 6
2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES 16
3. ANÁLISIS DE RIESGOS 19
4. ANÁLISIS DE BRECHA 24
5. PLAN DE TRABAJO 30
6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS 59
7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD 60
8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN 77
9. MEJORA CONTINUA 82
10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES 85
11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD 86

INTRODUCCIÓN

El Centro de Ciencias de la Complejidad (C3) es un espacio de encuentro en la UNAM donde buscamos reunir a los científicos, artistas, humanistas y técnicos de Facultades, Escuelas, Centros e Institutos para colaborar y enfrentar, con un enfoque integrador, desafíos transdisciplinarios de relevancia nacional aprovechando la sinergia resultante de la interacción entre diferentes áreas del conocimiento.

La Universidad Nacional Autónoma de México, a través de la Unidad de Transparencia, se ha dado a la tarea de transparentar el ejercicio de las actividades que se realizan en esta Casa De estudios, conlas acciones necesarias que permitan el ejercicio pleno del derecho de acceso a la información pública que obra en los archivos unviersitarios.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), establece las bases, principios y procedimientos para garantizar el derecho de Constitucional a la protección de datos personales que se encuentren en esta Dependencia.

NORMATIVIDAD EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

1. Ley General de Protección de Datos Personales en posesión de Sujetos Obligado (LGPDPPSO)

2. Anexo único del Acuerdo por el que se Aprueba la Adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público

3. Lineamientos Generales de Protección de Datos Personales para el Sector Público

4. Acuerdo por el que se Establecen los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México

5. Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad

6. Anexos de las Normas Complementarias sobre Medidas de Seguridad Técnicas, Administrativas y Físicas para la Protección de Datos Personales en Posesión de la Universidad

7. Formato de solicitud de ejercicio de derechos Acceso, Rectificación, Cancelación y Oposición (ARCO)

CENTRO DE CIENCIAS DE LA COMPLEJIDAD

El Centro de Ciencias de la Complejidad es un proyecto Especial de la UPEID, misma que pertenece a la Coordinación de la Investigación Científica, creado por acuerdo del Dr. José Narro Robles, publicado en Gaceta UNAM el 22 de septiembre de 2014.

Misión

Estamos comprometidos con la sociedad para la solución de problemas complejos a través de proyectos trans-disciplinarios, de la formación de recursos humanos y del desarrollo de conocimiento en las ciencias de la complejidad.

Visión

Ser un centro académico adaptable que promueve la sinergia en la generación y gestión de proyectos con enfoque sistémico que impacta en el avance de las ciencias de la complejidad y en la comprensión, prevención de problemas sociales y ambientales.

Ser un espacio de encuentro que integra capital intelectual para investigar y solucionar problemas complejos, de relevancia social, de forma flexible, pertinente y adaptativa.

Objetivo

Impulsar el desarrollo de las ciencias de la complejidad, mediante la generación y gestión de proyectos con enfoque sistémico y transdisciplinario que impacte en el avance de estas ciencias y en la comprensión, prevención de problemas sociales, ambientales, nacionales y mundiales, así como la formación de recursos humanos altamente especializados.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Delegación Administrativa	
Identificador único*	SILSFC3-CCTV-2023
(Nombre del sistema A1) *	**Monitoreo de CCTV**
Datos personales (sensibles o no) contenidos en el sistema*:	Imagen de las personas que ingresan y transitan a las instalaciones en espacios comunes
Responsable*:	Ing. Oscar Mendoza
Cargo*:	Jefe de Sección Académica - Cómputo
Funciones*:	Administrar el equipo de CCTV Crear y asignar usuarios para acceso a las cámaras del CCTV Asignar permisos a las cámaras Brindar las grabaciones cuando éstas sean solicitadas por el personal autorizado
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor Salvaguardar la información en el servidor Mantener el servicio en correcto funcionamiento
Encargado/Usuario:	Fis. Antonio Ramírez
Cargo*:	Superintendente de obra en el C3
Funciones*:	Monitorear las cámaras de CCTV de las instalaciones de forma aleatoria Asignar permisos a las cámaras Instalar y dar mantenimiento a las cámaras de CCTV Solicitar y revisar las grabaciones en caso de incidente
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor Mantener el servicio en correcto funcionamiento

Encargado/Usuario:	Mtro. José Luis Gordillo, Mtro. Romel Calero Ramos
Cargo*:	Responsable de Cómputo de Alto Rendimiento, Responsable de Ciencia de Datos
Funciones*:	Monitorear las cámaras de CCTV de las instalaciones de forma aleatoria Asignar permisos a las cámaras Solicitar y revisar las grabaciones en caso de incidente
Obligaciones*:	No difundir información de los datos personales No modificar la información almacenada en el servidor Salvaguardar la información en el servidor Mantener el servicio en correcto funcionamiento

Delegación Administrativa	
Identificador único*	SILSED3-SIC-2023
(Nombre del sistema A1) *	**Sistema Institucional de Compras**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, Teléfono, Domicilio, RFC, Correo electrónico.
Responsable/Usuario*:	Lic. Adriana Cruz Cortés
Cargo*:	Delegada Administrativa
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Recibir solicitudes de datos y tramitar el acceso a la información necesaria. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando.
Obligaciones*:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a

	personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales.
Encargado/Usuario:	C. Edgar Rojas Vivas
Cargo*:	Jefe de Bienes y Suministros
Funciones*:	Recibir y dar trámite a solicitudes de compras de bienes y servicios.
Obligaciones*:	Proteger los datos personales y confidenciales, no divulgación, reserva y resguardo de información.
Usuarios:	Yoselin Bermúdez Reyes, Christopher Rhodes Stephens, Francisco Xavier Soberón, Humberto Andrés Carrillo Calvet, José Luis Gordillo Ruiz, Oscar Mendoza Santiago, Patricia Peña González, Romel Calero Ramos, Aleida Carolina Rueda Rodríguez, Antonio Ramírez Fernández, Esperanza Hernández Olalde, Guadalupe Rojas Guzmán
Cargo*:	Jefe de Área, Académico, Asistente Ejecutivo
Funciones*:	Registros de solicitudes de bienes y Servicios.
Obligaciones*:	No difundir información de los datos personales

Delegación Administrativa	
Identificador único*	SILSED3-SIAF-2023
(Nombre del sistema A1) *	**Sistema Integral de Información Financiera**
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre, RFC.
Responsable/Usuario*:	Lic. Adriana Cruz Cortés

Cargo*:	Delegada Administrativa
Funciones*:	Capturar los movimientos presupuestales que se generan en el centro. Establecer quiénes son aquellos que tendrán acceso al sistema y las sus funciones. Recibir solicitudes de datos y tramitar el acceso a la información necesaria. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando.
Obligaciones*:	Preservar la integridad de los datos e información del sistema, utilizarlo para análisis y toma de decisiones. No difundir información de los datos personales

Delegación Administrativa	
Identificador único*	SILSED3-MCA-2023
(Nombre del sistema A1) *	**Módulo de Control de Asistencia del Sistema Integral de personal**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales de los trabajadores a) Datos de identificación: Nombre, R.F.C., b) Datos laborales: Plaza que ocupa, número de trabajador, antigüedad en el puesto, sueldo mensual.
Responsable/Usuario*:	Lic. Adriana Cruz Cortés
Cargo*:	Delegada Administrativa
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Recibir solicitudes de datos y tramitar el acceso a la información necesaria. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando.
Obligaciones*:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales.

Encargado/Usuario*:	Lic. Yoselin Bermúdez Reyes
Cargo*:	Jefe de Área de Personal y Servicios Generales
Funciones*:	Registrar los justificantes emitidos por ISSSTE, CENDI y STUNAM. Registrar los retardos y faltas injustificadas de los trabajadores. Registrar los justificantes de control interno de incidencias autorizadas. Registrar el tiempo extra de los trabajadores para trámite de pago.Registrar tiempo de la prima dominical para trámite de pago.
Obligaciones*:	Proteger los datos personales de los trabajadores. No difundir la información de datos personales de los trabajadores. Mantener la información de datos personales en el servidor de archivos del Centro y no usar la información indebidamente. Utilizar el sistema de gestión de acuerdo con los permisos autorizados. Verificar que la información de incidencias sea correcta para evitar descuentos indebidos.

Coordinación de Investigación	
Identificador único*	SILSVC3-CDTME-2023
(Nombre del sistema A1) *	**Plataforma de Registro de Conductome**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales en general: a) Datos de identificación: Nombre, correo electrónico. b) Datos académicos: carrera que estudia, campus universitario.
Responsable/Usuario*:	Dr. Christopher Stephens
Cargo*:	Coordinador de Investigación
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando. Recibir solicitudes de datos de los investigadores participantes en el proyecto

Obligaciones*:	Proteger los datos personales de los participantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en la plataforma. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargado/Usuario:	Mtro. Romel Calero Ramos
Cargo*:	Responsable de Ciencia de Datos.
Funciones*:	Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Mantener correcto funcionamiento del sistema.
Obligaciones*:	Proteger los datos personales y confidenciales, no divulgación, reserva y resguardo de información. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios:	Estefa Espitia, Ixel Alonso, Dagmara Wrzecionkowska, Jorge Rojas
Cargo*:	Administrador
Funciones*:	Creación y gestión y asignación de accesos de usuarios del sistema. Registro y gestión de estudiantes participantes en el proyecto.
Obligaciones*:	No difundir información de los datos personales. Garantizar seguridad de los datos y accesos al sistema.
Usuarios:	Deyanira Shellye González González, Jorge Barajas Márquez, María del Carmen Blanno García, Anel Mayela Cruz Lemolle, Esperanza Lugo Miranda, Jairo Isael Ramírez Jiménez, Carlos Eduardo Sánchez Meza, Arturo Obregón Díaz, Adrian Medina Aguilar, Eliana López Castillo, Camila Aixchell Alonso, Irisvet Rodríguez Peña, Ángel López Castillo, Cristian Salvador Rivera

	García, Georgina Sanabria Medina, Brenda Mónica Adame Rojo, Erika Alejandra Lorenzo Contreras, Mariana Gutiérrez Pérez, Cynthia García, Edgar Octavio Gómez Torres, Paulina Cipres, Mayra Adriana García Cerecedo
Cargo*:	Encuestador
Funciones*:	Registro y gestión de estudiantes participantes en el proyecto.
Obligaciones*:	No difundir información de los datos personales.

Coordinación de Investigación	
Identificador único*	SILSVC3-LS-2023
(Nombre del sistema A1) *	**Plataforma de Gestión de cuestionarios Lime Survey**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales en general: a) Datos de identificación: Nombre, correo electrónico, dirección personal, número de teléfono, sexo, estado civil, Fecha de nacimiento b) Datos académicos: carrera que estudia, campus universitario, semestre, información de estados de salud, o, número de cuenta universitaria
Responsable/Usuario*:	Dr. Christopher Stephens
Cargo*:	Coordinador de Investigación
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando. Recibir solicitudes de datos de los investigadores participantes en el proyecto
Obligaciones*:	Proteger los datos personales de los participantes. No modificar la información de datos personales. No difundir la información de datos personales contenidos en la plataforma. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.

Encargado/Usuario:	Mtro. Romel Calero Ramos
Cargo*:	Responsable de Ciencia de Datos.
Funciones*:	Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Mantener correcto funcionamiento del sistema.
Obligaciones*:	Proteger los datos personales y confidenciales, no divulgación, reserva y resguardo de información. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Usuarios:	Adriana Robles Cabrera, Estefa Espitia, Isaac Rendón Sánches, Dagmara Wrzecionkowska, Juan Pablo Gutiérrez, Juan Pablo Gutiérrez, Mariana Gutiérrez, Octavio Gómez, Mayra Adriana García, Carlos Sánchez Mena
Cargo*:	Administrador de cuestionario
Funciones*:	Creación y gestión de cuestionarios. Manejo de datos colectados en los cuestionarios Publicación de cuestionarios
Obligaciones*:	No difundir información de los datos personales. Garantizar seguridad de los datos y accesos al sistema.

Coordinación de Académica	
Identificador único*	SILSVC3-SGDWAAC3-2023
(Nombre del sistema A1) *	**Sistema de Gestión del Directorio Web de Académicos Asociados al C3**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales en general: a) Datos de identificación: Nombre, correo electrónico, b) Datos laborales: adscripción, teléfono de oficina y extensión, cargo actual c) Datos académicos: proyectos académicos, dirección URL de proyectos

Responsable/Usuario*:	Dr. Osbaldo Resendis
Cargo*:	Coordinador Académico
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando. Recibir solicitudes de datos de los académicos asociados
Obligaciones*:	Proteger los datos personales de los académicos asociados. No modificar la información de datos personales. No difundir la información de datos personales contenidos en la plataforma. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargado/Usuario:	Mtra. Patricia Peña González
Cargo*:	Responsable de Diseño y Difusión
Funciones*:	Recibir y dar trámite a las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Efectuar las notificaciones a los solicitantes en los procedimientos de acceso a la información, constituyéndose como vínculo entre el Centro y el solicitante. Atiende las solicitudes recibidas vía e-mail o telefónicas de la Coordinación Académica o del propio interesado(a).
Obligaciones*:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá..

Coordinación Académica	
Identificador único*	SILNRC3-SGD-2023
(Nombre del sistema A1) *	**Sistema de Gestión de Difusión**
Datos personales (sensibles o no) contenidos en el sistema*:	Datos personales en general: a) Datos de identificación: Nombre, correo electrónico, teléfono particular, teléfono celular b) Datos laborales: adscripción, teléfono de oficina y extensión, cargo actual c) Datos académicos: Grado académico, , proyectos académicos, dirección URL de proyectos, libros o artículos escritos, formación académica, cursos, congresos, eventos académicos, premios obtenidos
Responsable/Usuario*:	Dr. Osbaldo Resendis
Cargo*:	Coordinadora Académico
Funciones*:	Establecer quiénes son aquellos que tendrán acceso al sistema de gestión de datos, y las funciones que a ellos compete. Asigna el personal técnico que debe atender las solicitudes y mantener el sistema operando.
Obligaciones*:	Proteger los datos personales de los académicos asociados. No modificar la información de datos personales. No difundir la información de datos personales contenidos en la plataforma. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.
Encargado/Usuario:	Mtra. Patricia Peña González
Cargo*:	Responsable de Diseño y Difusión
Funciones*:	Recibir y dar trámite a las solicitudes de acceso a la información. Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información. Consulta información de datos personales (si los hay) de las solicitudes de información. Efectuar las notificaciones a los

	solicitantes en los procedimientos de acceso a la información, constituyéndose como vínculo entre el Centro y el solicitante. Atiende las solicitudes recibidas vía e-mail o telefónicas de la Coordinación Académica o del propio interesado(a).
Obligaciones*:	Proteger los datos personales de los solicitantes. No modificar la información de datos personales contenidos en las solicitudes de información. No difundir la información de datos personales contenidos en las solicitudes de información a personas no autorizadas. Reconducir las solicitudes cuando lo que soliciten sean datos personales. Utilizar el sistema de gestión de acuerdo con los permisos que les fueron otorgados y no más allá.

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Delegación Administrativa	
Identificador único¨*	SILSFC3-CCTV-2023
(Nombre del sistema A1*)	Monitoreo de CCTV
Tipo de soporte:*	Servidor físico, datos almacenados en entorno digital
Descripción:*	Plataforma Web con acceso a cámaras disponibles a través de la LAN interna
Características del lugar donde se resguardan los soportes:*	Alojada en un servidor físico. Segmento de red aislado con exclusividad para el sistema de cámaras. Servidor disponible en site del centro con acceso limitado a través de llaves.

Delegación Administrativa	
Identificador único¨*	SILSED3-SIC-2023
(Nombre del sistema A1*)	Sistema Instituciona de Compras
Tipo de soporte:*	Soporte físico y electrónico
Descripción:*	Plataforma Web accesible a través de la red universitaria. Se gestionan datos de proveedores, así como las órdenes de servicio o compra de bienes.
Características del lugar donde se resguardan los soportes:*	Alojada en un servidor de DGP. La información impresa se almacena en archivero del centro, en oficina con acceso limitado a través de llaves.

Delegación Administrativa

Identificador único¨*	SILSED3-SIAF-2023
(Nombre del sistema A1*)	Sistema Integral de Información Financiera
Tipo de soporte:*	Soporte físico y electrónico
Descripción:*	Plataforma informática accesible a través de la LAN del centro.
Características del lugar donde se resguardan los soportes:*	Alojada en un servidor virtual. La información impresa se almacena en archivero del centro, en oficina con acceso limitado a través de llaves.

Delegación Administrativa	
Identificador único¨*	SILSED3-MDA-2023
(Nombre del sistema A1*)	Módulo de Control de Asistencia del Sistema Integral de personal
Tipo de soporte:*	Soporte electrónico y físico
Descripción:*	Plataforma informática accesible a través de la LAN del centro.
Características del lugar donde se resguardan los soportes:*	En el servidor de DGP. La información impresa se almacena en archivero del centro, en oficina con acceso limitado a través de llaves.

Coordinación de Investigación	
Identificador único¨*	SILSVC3-CDTME-2023
(Nombre del sistema A1*)	Plataforma de Registro de Conductome
Tipo de soporte:*	Soporte electrónico
Descripción:*	Plataforma Web accesible a través de internet.
Características del lugar donde se resguardan los soportes:*	Servidor virtual en el site del centro. Acceso limitado al lugar donde está el servidor a través de llaves.

Coordinación de Investigación	
Identificador único¨*	SILSVC3-LS-2023
(Nombre del sistema A1*)	Plataforma de Gestión de cuestionarios Lime Survey
Tipo de soporte:*	Soporte electrónico
Descripción:*	Plataforma Web accesible a través de internet.
Características del lugar donde se resguardan los soportes:*	Servidor virtual en el site del centro. Acceso limitado al lugar donde está el servidor a través de llaves.

Coordinación Académica	
Identificador único¨*	SILSVC3-SGDWAAC3-2023
(Nombre del sistema A1*)	Sistema de Gestión del Directorio Web de Académicos Asociados al C3

Tipo de soporte:*	Soporte electrónico
Descripción:*	Plataforma Web accesible a través de internet.
Características del lugar donde se resguardan los soportes:*	Servidor virtual en el site del centro. Acceso limitado al lugar donde está el servidor a través de llaves.

Coordinación Académica	
Identificador único¨*	SILNRC3-SGD-2023
(Nombre del sistema A1*)	Sistema de Gestión de Difusión
Tipo de soporte:*	Soporte electrónico
Descripción:*	Directorio de contactos en formato electrónico.
Características del lugar donde se resguardan los soportes:*	Equipo de cómputo del centro en la oficina de encargado de diseño. Acceso limitado al equipo por contraseñas. Acceso limitado al lugar donde está el equipo a través de llaves.

3. ANÁLISIS DE RIESGOS

Delegación Administrativa		
Identificador único*	SILSFC3-CCTV-2023	
(Nombre del sistema A1) *	Monitoreo de CCTV	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Delegación Administrativa	
Identificador único*	SILSED3-SIC-2023
(Nombre del sistema A1) *	Sistema Institucional de Compras

Riesgo*	Impacto*	Mitigación*
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1) *	Sistema Integral de Información Financiera	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]

Delegación Administrativa		
Identificador único*	SILSED3-MDA-2023	
(Nombre del sistema A1) *	Módulo de Control de Asistencia del Sistema Integral de personal	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación de Investigación	
Identificador único*	SILSVC3-CDTME-2023
(Nombre del sistema A1) *	Plataforma de Registro de Conductome

Riesgo*	Impacto*	Mitigación*
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación de Investigación		
Identificador único*	SILSVC3-LS-2023	
(Nombre del sistema A1) *	Plataforma de Gestión de cuestionarios Lime Survey	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Coordinación Académica		
Identificador único*	SILSVC3-SGDWAAC3-2023	
(Nombre del sistema A1) *	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]

Coordinación de Comunicación		
Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1) *	Sistema de Gestión de Difusión	
Riesgo*	**Impacto***	**Mitigación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4. ANÁLISIS DE BRECHA

Delegación Administrativa

Identificador único*	SILSFC3-CCTV-2023	
(Nombre del sistema A1) *	Monitoreo de CCTV	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Delegación Administrativa		
Identificador único*	SILSED3-SIC-2023	
(Nombre del sistema A1)*	Sistema Institucional de Compras	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1)*	Sistema Integral de Información Financiera	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Delegación Administrativa	
Identificador único*	SILSED3-MDA-2023
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal

Medida de seguridad actual*	Medida de seguridad necesaria*	Acciones para remediación*
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación de Investigación		
Identificador único*	SILSVC3-CDTME-2023	
(Nombre del sistema A1)*	Plataforma de Registro de Conductome	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

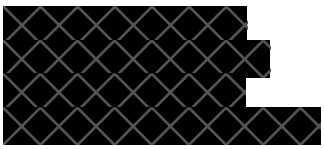
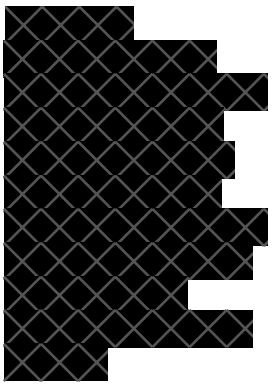
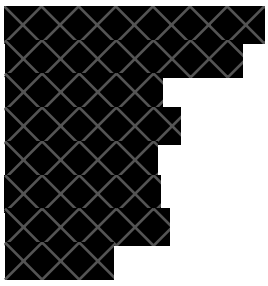
[redacted]	[redacted]	[redacted]

Coordinación de Investigación		
Identificador único*	SILSVC3-LS-2023	
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación Académica	
Identificador único*	SILSVC3-SGDWAAC3-2023

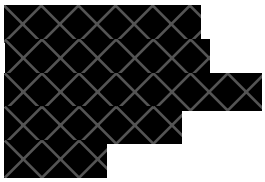
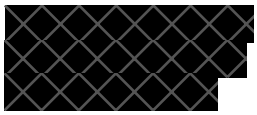
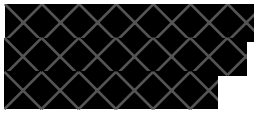
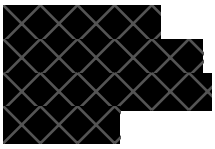
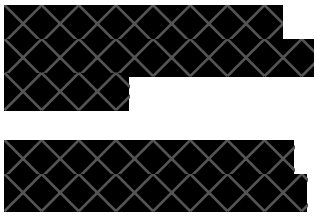
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Coordinación Académica		
Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1)*	Sistema de Gestión de Difusión	
Medida de seguridad actual*	**Medida de seguridad necesaria***	**Acciones para remediación***

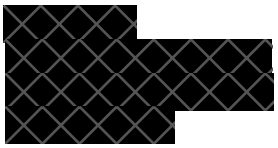
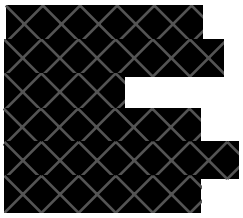
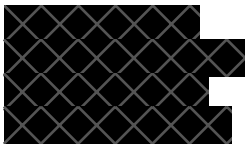
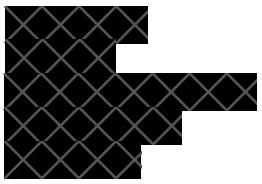
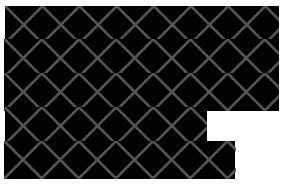
		
		
		

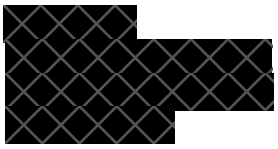
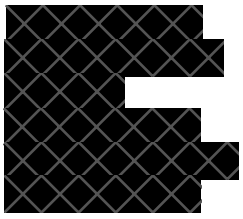
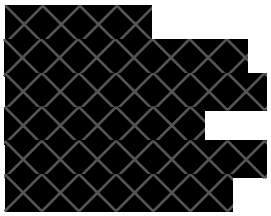
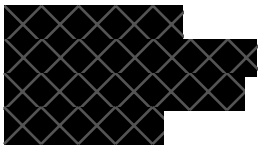
5. PLAN DE TRABAJO

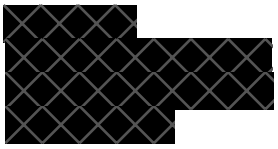
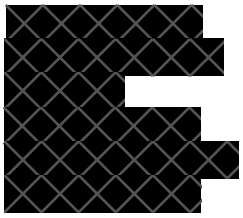
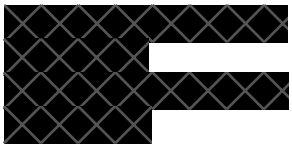
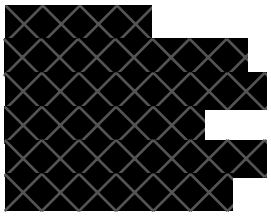
Delegación Administrativa			
Identificador único*	SILSFC3-CCTV-2023		
(Nombre del sistema A1) *	Monitoreo de CCTV		
Actividad*	**Descripción***	**Duración***	**Cobertura***

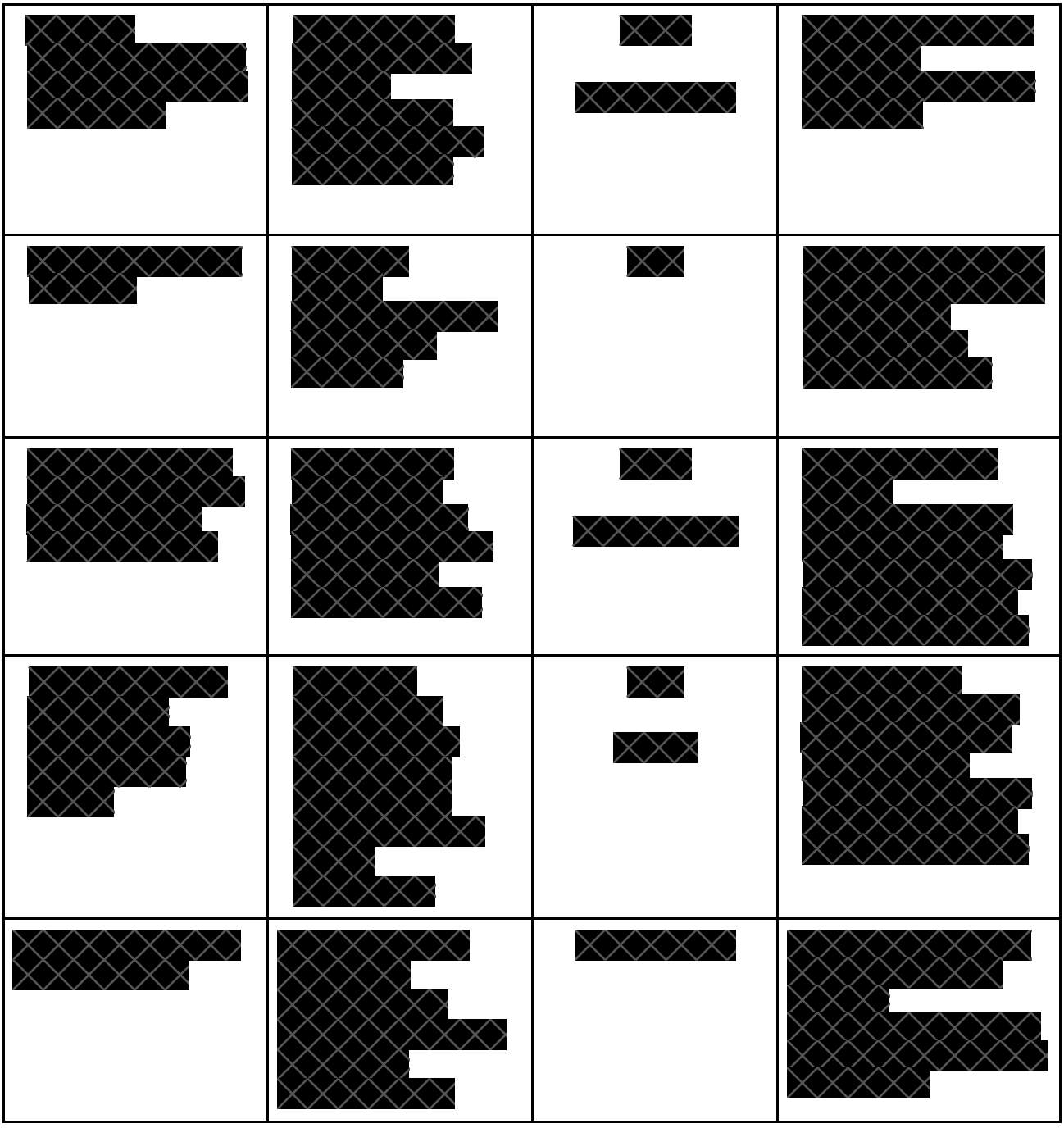
Delegación Administrativa			
Identificador único*	SILSED3-SIC-2023		
(Nombre del sistema A1) *	Sistema Institucional de Compras		
Actividad*	**Descripción***	**Duración***	**Cobertura***

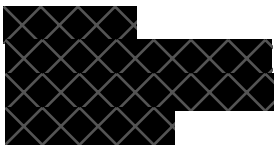
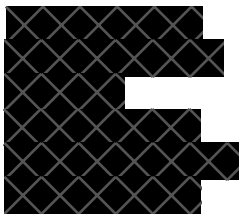
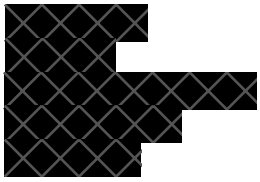
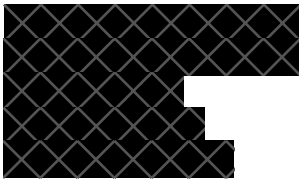
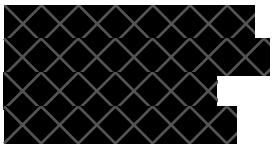
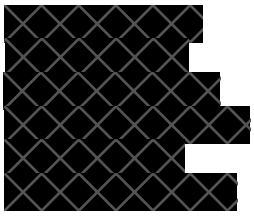
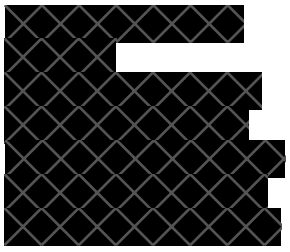
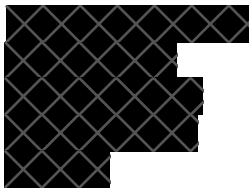
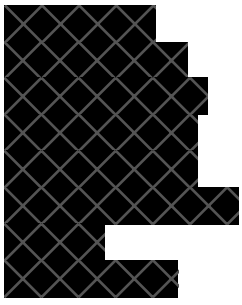
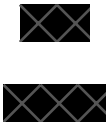
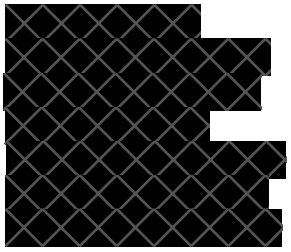
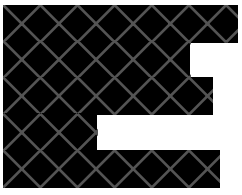
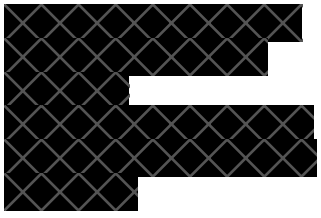
Delegación Administrativa			
Identificador único*	SILSED3-SIAF-2023		
(Nombre del sistema A1) *	Sistema Integral de Información Financiera		
Actividad*	**Descripción***	**Duración***	**Cobertura***
			
			

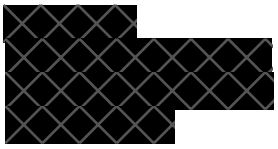
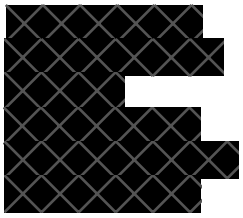
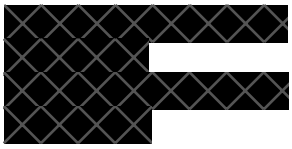
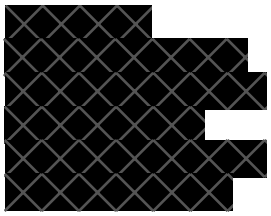
Delegación Administrativa			
Identificador único*	SILSED3-MDA-2023		
(Nombre del sistema A1) *	Módulo de Control de Asistencia del Sistema Integral de personal		
Actividad*	**Descripción***	**Duración***	**Cobertura***
			
			

Coordinación de Investigación			
Identificador único*	SILSVC3-CDTME-2023		
(Nombre del sistema A1) *	Plataforma de Registro de Contuctome		
Actividad*	**Descripción***	**Duración***	**Cobertura***

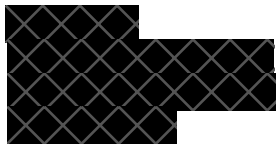
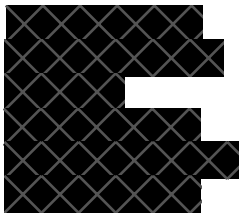
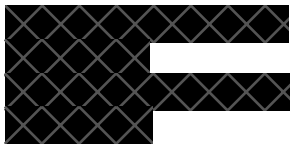
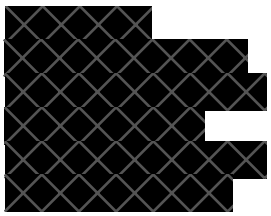
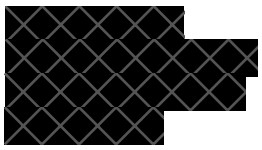


Coordinación de Investigación	
Identificador único*	SILSVC3-LS-2023

(Nombre del sistema A1) *	Plataforma de Gestión de cuestionarios Lime Survey		
Actividad*	**Descripción***	**Duración***	**Cobertura***
			
			
			
			
			

Coordinación Académica			
Identificador único*	SILSVC3-SGDWAAC3-2023		
(Nombre del sistema A1) *	Sistema de Gestión del Directorio Web de Académicos Asociados al C3		
Actividad*	**Descripción***	**Duración***	**Cobertura***
			
			

Coordinación Académica			
Identificador único*	SILNRC3-SGD-2023		
(Nombre del sistema A1) *	Sistema de Gestión de Difusión		
Actividad*	**Descripción***	**Duración***	**Cobertura***

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILSFC3-CCTV-2023
(Nombre del sistema A1)*	Monitoreo de CCTV
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	**a)** La transferencia de la información se hace de manera personal, el encargado acude con el responsable y solicita la información mediante oficio firmado por el titular de la dependencia en cuestión. **b)** La información se almacena en un dispositivo externo y se entrega al encargado para su futura revisión.
Transferencias mediante el traslado de soportes electrónicos:	No aplica
Transferencias mediante el traslado sobre redes electrónicas:	No aplica

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.

   El servidor donde se graban los videos se encuentra en el site cerrado bajo llave y acceso controlado.

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

   Orcar Mendoza
   Responsable de Cómputo del C3

   Antonio Ramírez
   Responsable de la infraestructura técnica del C3

   José Luis Gordillo
   Responsable de área de Cómputo de Alto Rendimiento

   Romel Calero Ramos
   Responsable de área de Ciencia de Datos

III. Bitácoras para accesos y operación cotidiana

1. A través del sistema de accesos se registran los mismos en las bitácoras de: Fecha de acceso, hora y usuario
2. Las bitácoras en soporte electrónico (mecanismos de logs del sistema)
3. La integridad de las bitácoras está respaldada por el propio sistema
4. Análisis de las bitácoras: Es realizado por el Responsable de Cómputo ante la ocurrencia de eventos.

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.

No se cuenta con información al respecto.

V. Acceso a las instalaciones

1.Seguridad perimetral exterior (las instalaciones del área universitaria)**:**
Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)**:**
Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el equipo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y optimización del sistema operativo del servidor que gestiona el software de CCTV. En el encargado de Cómputo es el responsable de llevar a cabo esta actividad.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas y está basado en roles de usuario

2. Perfiles de usuario y contraseña en el sistema operativo
El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas
El Responsable de Cómputo es el encargado de gestionar las cuentas de usuario con acceso al sistema.

5. Acceso remoto a sistema de tratamiento de datos
El servidor donde está instalado el sistema se encuentra en un segmento de red distinto al de la red de los usuarios. Sólo tienen acceso de manera remota a este equipo los responsables antes mencionados con acceso al site. Está establecido este acceso sólo para cuestiones de mantenimiento.

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera incremental automáticamente a un dispositivo externo cada 3 semanas en un disco duro externo. El responsable de la realización del resguardo de la información es el Responsable de Cómputo.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILSED3-SIC-2023
(Nombre del sistema A1)*	Sistema Institucional de Compras
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:	Las conexiones se hacen de forma cifrada mediante el protocolo de SSL.

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.

Los equipos desde donde se hacen las conexiones al servidor se encuentran resguardados en las oficinas asignadas a cada usuario. Para acceder a dichas oficinas es necesario acceder a través del control de acceso. Cada oficina posee además una cerradura con llave, a dicha llave sólo tiene acceso el responsable de cada oficina.

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

Lic. Adriana Cruz
Delegada Administrativa

Edgar Rojas
Jefe de Bienes y Suministros

III. Bitácoras para accesos y operación cotidiana

1. El sistema lleva control de los accesos y cambios de la información que se gestiona
2. Análisis de las bitácoras: Es realizado sólo ante la ocurrencia de eventos.

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.

No se cuenta con información al respecto.

V. Acceso a las instalaciones

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

Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

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

Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso a las oficinas por parte del personal administrativo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

La información no se modifica. Ante errores detectados, se cancela la solicitud y queda la información registrada en el sistema. Se solicita hacer nueva solicitud para mantener la información consistente y atender la solicitud correcta.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas y está basado en roles de usuario

2. Perfiles de usuario y contraseña en el sistema operativo
Se desconoce, sistema centralizado de la UNAM

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas
El encargo de generarlas se encuentra en la Dirección de Personal y se generan a través del área de sistemas de esa dependencia.

5. Acceso remoto a sistema de tratamiento de datos
El acceso se hace mediante la interfaz web de la aplicación y cifrada por el protocolo SSL

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera según las políticas que establece el sistema en sus sedes centrales. No aplica a nuestra responsabilidad.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILSED3-SIAF-2023
(Nombre del sistema A1)*	Sistema Integral de Información Financiera (SIAF)
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:	Las conexiones se hacen de forma cifrada mediante el protocolo de SSL.

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.

El servidor local donde se gestionan los datos se encuentra en el site cerrado bajo llave y acceso controlado.

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

Orcar Mendoza
Responsable de Cómputo del C3

Adriana Cruz
Delegada Administrativa

III. Bitácoras para accesos y operación cotidiana

1. A través del propio sistema se registran las bitácoras
2. Análisis de las bitácoras: Es realizado por el Responsable de Cómputo ante la ocurrencia de eventos.

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.

No se cuenta con información al respecto.

V. Acceso a las instalaciones

1.Seguridad perimetral exterior (las instalaciones del área universitaria)**:**
Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)**:**
Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el servidor local.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y actualización del sistema operativo del servidor que aloja el aplicativo. Se mantiene actualizado cada equipo del personal con acceso al sistema. En el encargado de Cómputo es el responsable de llevar a cabo esta actividad.

VI. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas y está basado en roles de usuario

2. Perfiles de usuario y contraseña en el sistema operativo

El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas
La delegada administrativa quien es responsable del sistema.

5. Acceso remoto a sistema de tratamiento de datos
No se tiene acceso remoto al equipo

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan cada semana de manera automática a un dispositivo externo. El responsable de la realización del resguardo de la información es el Responsable de Cómputo.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILSED3-MDA-2023
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal
TRANSFERENCIAS DE DATOS PERSONALES	

Transferencias mediante el traslado de soportes físicos:	a) La transferencia de datos personales mediante el traslado de soportes físicos se lleva a cabo normalmente vía mensajero. b) El envío del paquete físico con datos personales, se realiza en sobre cerrado y fácil de identificar en caso de que se haya intentado abrir. c) Acuse de recibido por el destinatario, previa acreditación con identificación official en caso de ser la primera ocasión en el área. d) El mensajero no entrega el paquete si el destinatario no se encuentra o no tiene la certeza de la identidad; en ese caso se devuelve el paquete al transmisor.

Transferencias mediante el traslado de soportes electrónicos:	a) El envío de datos personales mediante el traslado de soportes electrónicos USB, se lleva a cabo con un mensajero oficial. b) El paquete con datos personales en soportes electrónicos USB, viaja en sobre debidamente sellado para percibir cualquier intención de apertura. c) Acuse de recibido por el destinatario, previa acreditación con identificación official en caso de ser la primera ocasión en el área. d) El mensajero no entrega el paquete si el destinatario no se encuentra y no tiene la certeza de la identidad y en ese caso se devuelve el paquete al transmisor.

Transferencias mediante el traslado sobre redes electrónicas:	a) La conexión solo es permitida por IP: "El envío de información se realiza a través del sistema SIP y únicamente se permite la conexión desde equipos de cómputo con IP Red UNAM y previamente registrados por el Departamento de Cómputo de la DGP" b) El remitente registra la transferencia en su bitácora, así como en el Sistema de tratamiento de datos personales.

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.

Los equipos desde donde se accede están bajo llave y sólo el personal que los maneja posee la llave. El área administrativa está restringida por control de acceso digital.

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

Adriana Cruz
Delegada Administrativa

Yoselin Bermúdez
Jefe de Área de Personal y Servicios Generales

III. Bitácoras para accesos y operación cotidiana

1. A través del propio sistema en los servidores centrales donde habita la base de datos de la herramienta informática.

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.

No se cuenta con información al respecto.

V. Acceso a las instalaciones

1.Seguridad perimetral exterior (las instalaciones del área universitaria)**:**
Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)**:**
Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal a las oficinas donde están los equipos con acceso.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece mecanismo de manera personalizada en dependencia del vínculo del titular con el centro o por eventos en donde se detecten los datos inexactos.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas.

2. Perfiles de usuario y contraseña en el sistema operativo
El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al equipo de cómputo con acceso al aplicativo. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas
El encargo de generarlas se encuentra en la Dirección de Personal y se generan a través del área de sistemas de esa dependencia.

5. Acceso remoto a sistema de tratamiento de datos
El servidor está ubicado en un área de la universidad externa al C3. Se desconocen las reglas.

VIII. Procedimientos de respaldo y recuperación de datos

Se desconoce el mecanismo de respaldo. Es realizado por personal de otra dependencia de la UNAM.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Coordinación de Investigación	
Identificador único*	SILSVC3-CDTME-2023
(Nombre del sistema A1)*	Plataforma de Registro de Contuctome
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:	Mediante uso de cliente web a través de conexiones cifradas por SSL. El equipo tiene restringido el uso de puertos, base de datos controlada mediante combinación de usuario, contraseña e IP. Equipo protegido por firewall del centro.

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.

El servidor que hospeda la aplicación se encuentra en el site cerrado bajo llave y acceso controlado.

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

Orcar Mendoza
Responsable de Cómputo del C3

Antonio Ramírez
Responsable de la infraestructura técnica del C3

José Luis Gordillo
Responsable de área de Cómputo de Alto Rendimiento

Romel Calero Ramos
Responsable de área de Ciencia de Datos

III. Bitácoras para accesos y operación cotidiana

1. A través del sistema de accesos se registran los mismos en las bitácoras de: Fecha de acceso, hora y usuario
2. Las bitácoras en soporte electrónico (mecanismos de logs del sistema)
3. La integridad de las bitácoras está respaldada por el propio sistema
4. Análisis de las bitácoras: Es realizado por los responsables con acceso al equipo de manera conjunta y ante la ocurrencia de eventos. Además, es cuenta con herramienta de monitoreo continuo para el disparado de alertas ante la detección de posibles errores

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.

No se cuenta con información al respecto. Se está trabajando en la conformación de las políticas adecuadas.

V. Acceso a las instalaciones

1.Seguridad perimetral exterior (las instalaciones del área universitaria)**:**
Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)**:**
Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el equipo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y optimización del sistema operativo del servidor que aloja el sistema. Los miembros de equipo de cómputo son los encargados de llevar a cabo esta actividad.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas y está basado en roles de usuario

2. Perfiles de usuario y contraseña en el sistema operativo
El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas
El Responsable de Ciencia de Datos es el encargado de gestionar las cuentas de usuario con acceso al sistema.

5. Acceso remoto a sistema de tratamiento de datos
Sólo tienen acceso de manera remota al equipo donde se encuentra el sistema los responsables antes mencionados con acceso al site. Está establecido este acceso sólo para cuestiones de mantenimiento.

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera automática cada semana en un disco duro externo. El personal con acceso al site es el responsable de la realización del resguardo de la información.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Coordinación de Investigación	
Identificador único*	SILSVC3-LS-2023
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey

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:	Mediante uso de cliente web a través de conexiones cifradas por SSL. El equipo tiene restringido el uso de puertos, base de datos controlada mediante combinación de usuario, contraseña e IP. Equipo protegido por firewall del centro.

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.

El servidor que hospeda la aplicación se encuentra en el site cerrado bajo llave y acceso controlado.

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

Orcar Mendoza
Responsable de Cómputo del C3

Antonio Ramírez
Responsable de la infraestructura técnica del C3

José Luis Gordillo
Responsable de área de Cómputo de Alto Rendimiento

Romel Calero Ramos
Responsable de área de Ciencia de Datos

III. Bitácoras para accesos y operación cotidiana

1. A través del sistema de accesos se registran los mismos en las bitácoras de: Fecha de acceso, hora y usuario
2. Las bitácoras en soporte electrónico (mecanismos de logs del sistema)
3. La integridad de las bitácoras está respaldada por el propio sistema
4. Análisis de las bitácoras: Es realizado por los responsables con acceso al equipo de manera conjunta y ante la ocurrencia de eventos. Además, se cuenta con herramienta de monitoreo continuo para el disparado de alertas ante la detección de posibles errores

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.

No se cuenta con información al respecto. Se está trabajando en la conformación de las políticas adecuadas.

V. Acceso a las instalaciones

1.Seguridad perimetral exterior (las instalaciones del área universitaria)**:**
Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

2. Seguridad perimetral interior (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos)**:**
Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el equipo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y optimización del sistema operativo del servidor que aloja el sistema. Los miembros de equipo de cómputo son los encargados de llevar a cabo esta actividad.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso
El acceso es mediante usuario y contraseñas y está basado en roles de usuario

2. Perfiles de usuario y contraseña en el sistema operativo
El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema
El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas

El Responsable de Ciencia de Datos es el encargado de gestionar las cuentas de usuario con acceso al sistema.

5. Acceso remoto a sistema de tratamiento de datos

Sólo tienen acceso de manera remota al equipo donde se encuentra el sistema los responsables antes mencionados con acceso al site. Está establecido este acceso sólo para cuestiones de mantenimiento.

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera automática cada semana en un disco duro externo. El personal con acceso al site es el responsable de la realización del resguardo de la información.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILSVC3-SGDWAAC3-2023
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3
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:	Las conexiones se hacen de forma cifrada mediante el protocolo de SSL.

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.

El servidor donde se aloja el servicio se encuentra en el site cerrado bajo llave y acceso controlado.

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

Orcar Mendoza
Responsable de Cómputo del C3

Antonio Ramírez
Responsable de la infraestructura técnica del C3

José Luis Gordillo
Responsable de área de Cómputo de Alto Rendimiento

Romel Calero Ramos
Responsable de área de Ciencia de Datos

Patricia Peña
Responsable de área de Diseño

III. Bitácoras para accesos y operación cotidiana

1. A través del sistema de accesos se registran los mismos en las bitácoras de: Fecha de acceso, hora y usuario
2. Las bitácoras en soporte electrónico (mecanismos de logs del sistema)
3. La integridad de las bitácoras está respaldada por el propio sistema
4. Análisis de las bitácoras: Es realizado por el Responsable de Cómputo ante la ocurrencia de eventos.

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.

No se cuenta con información al respecto. Se está trabajando en la conformación de las políticas adecuadas.

V. Acceso a las instalaciones

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

Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

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

Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el equipo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y optimización del sistema operativo del servidor que alberga el servicio. La responsable de diseño unida a los miembros del equipo de cómputo son los encargados de llevar a cabo esta actividad.

VII. Perfiles de usuario y contraseñas

1. Modelo de control de acceso

El acceso es mediante usuario y contraseñas.

2. Perfiles de usuario y contraseña en el sistema operativo

El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

3. Perfiles de usuario y contraseña manejados por el sistema

El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

4. Administración de perfiles de usuario y contraseñas

El Responsable de diseño controla los datos de usuario y contraseñas con acceso

5. Acceso remoto a sistema de tratamiento de datos

El servidor donde está instalado el sistema se encuentra en un segmento de red distinto al de la red de los usuarios. Sólo tienen acceso de manera remota a este equipo los responsables antes mencionados con acceso al site. Está establecido este acceso sólo para cuestiones de mantenimiento.

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera automática cada semana en un disco duro externo. El personal con acceso al site es el responsable de la realización del resguardo de la información.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

I. Transferencias de datos personales

Delegación Administrativa	
Identificador único*	SILNRC3-SGD-2023
(Nombre del sistema A1)*	Sistema de Gestión de Difusión
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

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.

   El servidor donde se graban los videos se encuentra en el site cerrado bajo llave y acceso controlado.

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

   Oscar Mendoza
   Responsable de Cómputo del C3

   Antonio Ramírez
   Responsable de la infraestructura técnica del C3

   José Luis Gordillo
   Responsable de área de Cómputo de Alto Rendimiento

   Romel Calero Ramos
   Responsable de área de Ciencia de Datos

   Patricia Peña
   Responsable de área de Diseño

   Aleida Rueda
   Responsable de área de Comunicación

III. Bitácoras para accesos y operación cotidiana

5. A través del sistema de accesos se registran los mismos en las bitácoras de: Fecha de acceso, hora y usuario

6. Las bitácoras en soporte electrónico (mecanismos de logs del sistema)
7. La integridad de las bitácoras está respaldada por el propio sistema
8. Análisis de las bitácoras: Es realizado por el Responsable de Cómputo ante la ocurrencia de eventos.

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.

No se cuenta con información al respecto. Se está trabajando en la conformación de las políticas adecuadas.

V. Acceso a las instalaciones

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

Se utiliza el sistema de control de acceso en caso de trabajadores del edificio, se cuenta con el sistema de CCTV. Para los visitantes está control mediante vigilantes a la entrada del edificio y control de registro.

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

Se utiliza el sistema de control de acceso, control mediante llaves físicas y restricción de acceso por parte del personal al site, lugar donde está el equipo.

VI. Actualización de la información contenida en el sistema de tratamiento de datos personales

Se establece un continuo monitoreo y optimización del sistema operativo del servidor que alberga el servicio. Las responsables de diseño y comunicación unidas a los miembros del equipo de cómputo son los encargados de llevar a cabo esta actividad.

VII. Perfiles de usuario y contraseñas

6. Modelo de control de acceso

El acceso es mediante usuario y contraseñas.

7. Perfiles de usuario y contraseña en el sistema operativo

El sistema operativo está controlado por cuenta de usuario y contraseñas. Está limitado el número de usuarios que tienen acceso al servidor. Las contraseñas siguen reglas estrictas de formación para garantizar su seguridad

8. Perfiles de usuario y contraseña manejados por el sistema

El sistema lleva control riguroso de los perfiles de usuario a través de control por roles y funciones.

9. Administración de perfiles de usuario y contraseñas

El Responsable de diseño controla los datos de usuario y contraseñas con acceso

10. Acceso remoto a sistema de tratamiento de datos

El servidor donde está instalado el sistema se encuentra en un segmento de red distinto al de la red de los usuarios. Sólo tienen acceso de manera remota a este equipo los responsables antes mencionados con acceso al site. Está establecido este acceso sólo para cuestiones de mantenimiento.

VIII. Procedimientos de respaldo y recuperación de datos

Los respaldos se realizan de manera automática cada semana en un disco duro externo. El personal con acceso al site es el responsable de la realización del resguardo de la información.

IX Plan de contingencia

Está regido por lo establecido en “PLAN DE CONTINGENCIA QUE DÉ CONTINUIDAD A LA OPERACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN” del centro (Anexo).

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

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

Delegación Administrativa	
Identificador único*	SILSFC3-CCTV-2023

(Nombre del sistema A1)*	Monitoreo de CCTV	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza
Certificado SSL	Certificado SSL *wildcard* para todo el dominio del C3	Renovación automática cada 3 meses. Se cuenta con mecanismo de reemplazo automático. Mtro. José Luis Gordillo.

Delegación Administrativa		
Identificador único*	SILSED3-SIC-2023	
(Nombre del sistema A1)*	Sistema Institucional de Compras	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1)*	Sistema Integral de Información Financiera	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza

Delegación Administrativa		
Identificador único*	SILSED3-MCA-2023SILSED3-MCA-2023	
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza

Delegación Administrativa		
Identificador único*	SILSVC3-CDTME-2023	
(Nombre del sistema A1)*	Plataforma de Registro de Conductome	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza
Certificado SSL	Certificado SSL *wildcard* para todo el dominio del C3	Renovación automática cada 3 meses. Se cuenta con mecanismo de reemplazo automático. Mtro. José Luis Gordillo.

Delegación Administrativa		
Identificador único*	SILSVC3-LS-2023	
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza

Certificado SSL	Certificado SSL *wildcard* para todo el dominio del C3	Renovación automática cada 3 meses. Se cuenta con mecanismo de reemplazo automático. Mtro. José Luis Gordillo.

Delegación Administrativa		
Identificador único*	SILSVC3-SGDWAAC3-2023	
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza
Certificado SSL	Certificado SSL *wildcard* para todo el dominio del C3	Renovación automática cada 3 meses. Se cuenta con mecanismo de reemplazo automático. Mtro. José Luis Gordillo.

Delegación Administrativa

Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1)*	Sistema de Gestión de Difusión	
Recurso*	**Descripción***	**Control***
Fortinet	Firewall institucional para filtrado de datos y detección de ataques	Licencia vigente por 3 años. Responsable por velar la vigencia de la licencia es el Ing. Oscar Mendoza
Certificado SSL	Certificado SSL *wildcard* para todo el dominio del C3	Renovación automática cada 3 meses. Se cuenta con mecanismo de reemplazo automático. Mtro. José Luis Gordillo.

7.2. Procedimiento para la revisión de las medidas de seguridad

Delegación Administrativa		
Identificador único*	SILSFC3-CCTV-2023	
(Nombre del sistema A1)*	Monitoreo de CCTV	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas	Ing. Oscar Mendoza
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	

Delegación Administrativa		
Identificador único*	SILSED3-SIC-2023	
(Nombre del sistema A1)*	Sistema Instituciona de Compras	
Medida de seguridad*	**Procedimiento***	**Responsable***
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	Ing. Oscar Mendoza

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1)*	Sistema Integral de Información Financiera	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas	Ing. Oscar Mendoza
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	

Delegación Administrativa		
Identificador único*	SILSED3-MDA-2023	
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal	
Medida de seguridad*	**Procedimiento***	**Responsable***
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	Ing. Oscar Mendoza

Delegación Administrativa		
Identificador único*	SILSVC3-CDTME-2023	
(Nombre del sistema A1)*	Plataforma de Registro de Conductome	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas	Ing. Oscar Mendoza
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	

Delegación Administrativa		
Identificador único*	SILSVC3-LS-2023	
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas	Ing. Oscar Mendoza
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	

Delegación Administrativa		
Identificador único*	SILSVC3-SGDWAAC3-2023	
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas Segmentación de la red para reducir posibilidades de ataque	Ing. Oscar Mendoza

Vulnerabilidad de la red	y controlar tráfico a través del firewall	

Delegación Administrativa		
Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1)*	Sistema de Gestión de Difusión	
Medida de seguridad*	**Procedimiento***	**Responsable***
Monitoreo de servicio	Servicio de monitoreo constante instalado con alertas de disponibilidad implementadas	Ing. Oscar Mendoza
Vulnerabilidad de la red	Segmentación de la red para reducir posibilidades de ataque y controlar tráfico a través del firewall	

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

Delegación Administrativa		
Identificador único*	SILSFC3-CCTV-2023	
(Nombre del sistema A1)*	Monitoreo de CCTV	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***

Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILSED3-SIC-2023	
(Nombre del sistema A1)*	Sistema Instituciona de Compras	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1)*	Sistema Integral de Información Financiera	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILSED3-MDA-2023	
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILSVC3-CDTME-2023	
(Nombre del sistema A1)*	Plataforma de Registro de Conductome	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa	
Identificador único*	SILSVC3-LS-2023
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey

Medida de seguridad*	Resultado de evaluación*	Responsable*
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILSVC3-SGDWAAC3-2023	
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

Delegación Administrativa		
Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1)*	Sistema de Gestión de Difusión	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Vulnerabilidad de la red	Se requiere modificación de las políticas de filtrado de tráfico entre las distintas VLANs	Ing. Oscar Mendoza En proceso de corrección próximo a concluir migración al nuevo Fortinet (firewall)

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

Delegación Administrativa		
Identificador único*	SILSFC3-CCTV-2023	
(Nombre del sistema A1)*	Monitoreo de CCTV	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico Configuración de nuevo equipo para control de tráfico Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza En Proceso

Delegación Administrativa		
Identificador único*	SILSED3-SIC-2023	
(Nombre del sistema A1)*	Sistema Instituciona de Compras	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza Concluida

	Configuración de nuevo equipo para control de tráfico Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza En Proceso

Delegación Administrativa		
Identificador único*	SILSED3-SIAF-2023	
(Nombre del sistema A1)*	Sistema Integral de Información Financiera	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico Configuración de nuevo equipo para control de tráfico Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza En Proceso

Delegación Administrativa	
Identificador único*	SILSED3-MDA-2023
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal

Medida de seguridad*	Acciones*	Responsable*
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Configuración de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza En Proceso

Delegación Administrativa		
Identificador único*	SILSVC3-CDTME-2023	
(Nombre del sistema A1)*	Plataforma de Registro de Conductome	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Configuración de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza En Proceso

Delegación Administrativa		
Identificador único*	SILSVC3-LS-2023	
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico Configuración de nuevo equipo para control de tráfico Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza En Proceso

Delegación Administrativa		
Identificador único*	SILSVC3-SGDWAAC3-2023	
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico Configuración de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza Concluida Ing. Oscar Mendoza

	Establecimiento de nuevas reglas de filtrado de tráfico	En Proceso

Delegación Administrativa		
Identificador único*	SILNRC3-SGD-2023	
(Nombre del sistema A1)*	Plataforma Web accesible a través de internet.	
Medida de seguridad*	**Acciones***	**Responsable***
Vulnerabilidad de la red	Adquisición de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Configuración de nuevo equipo para control de tráfico	Ing. Oscar Mendoza Concluida
	Establecimiento de nuevas reglas de filtrado de tráfico	Ing. Oscar Mendoza En Proceso

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

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

Delegación Administrativa			
Identificador único*	SILSFC3-CCTV-2023		
(Nombre del sistema A1)*	Monitoreo de CCTV		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección*	*Un día*	*Responsables de seguridad de datos personales del sistema de CCTV*

Curso de actualización/ certificación de monitorieo y seguridad de CCTV	*de datos personales* *Actualizar al personal responsable en temas de seguridad sobrel el tema de CCTV y seguridad de datos personales*	*Por definir*	

Delegación Administrativa			
Identificador único*	SILSED3-SIC-2023		
(Nombre del sistema A1)*	Sistema Instituciona de Compras		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Usuarios del sistema*

Delegación Administrativa			
Identificador único*	SILSED3-SIAF-2023		
(Nombre del sistema A1)*	Sistema Integral de Información Financiera		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Usuarios del sistema*

Delegación Administrativa	
Identificador único*	SILSED3-MDA-2023
(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal

Actividad*	Descripción*	Duración*	Cobertura*
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Usuarios del sistema*

Coordinación de Investigación			
Identificador único*	SILSVC3-CDTME-2023		
(Nombre del sistema A1)*	Plataforma de Registro de Conductome		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Responsable de la plataforma*
Curso de seguridad web con énfasis en protección de datos personales	*Actualizar al personal de cómputo en temas de seguridad y protección de datos en entorno web*	*Por definir*	*Responsable de la plataforma*
Curso de seguridad en filtrado web con Fortinet	*Optimizar el uso del firewall para filtrado web*	*Por definir*	*Responsable de cómputo*

Coordinación de Investigación			
Identificador único*	SILSVC3-LS-2023		
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Responsable de la plataforma*
Curso de seguridad web con énfasis en protección de datos personales	*Actualizar al personal de cómputo en temas de seguridad y protección de datos en entorno web*	*Por definir*	*Responsable de la plataforma*
Curso de seguridad en filtrado web con Fortinet	*Optimizar el uso del firewall para filtrado web*	*Por definir*	*Responsable de cómputo*

Coordinación Académica			
Identificador único*	SILNRC3-SGD-2023		
(Nombre del sistema A1)*	Sistema de Gestión de Difusión		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Responsable de la plataforma*
Curso de seguridad web con énfasis en protección de datos personales	*Actualizar al personal de cómputo en temas de seguridad y protección de datos en entorno web*	*Por definir*	*Responsable de la plataforma*

Curso de seguridad en filtrado web con Fortinet	*Optimizar el uso del firewall para filtrado web*	*Por definir*	*Responsable de cómputo*

Coordinación Académica			
Identificador único*	SILSVC3-SGDWAAC3-2023		
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	*Introducir a los responsables los elementos de interés para una correcta protección de datos personales*	*Un día*	*Responsable de la plataforma*
Curso de seguridad web con énfasis en protección de datos personales	*Actualizar al personal de cómputo en temas de seguridad y protección de datos en entorno web*	*Por definir*	*Responsable de la plataforma*
Curso de seguridad en filtrado web con Fortinet	*Optimizar el uso del firewall para filtrado web*	*Por definir*	*Responsable de cómputo*

8.2 Programa de difusión de la protección a los datos personales

A través de la web institucional se ofrecen los avisos de privacidad. En el caso del sistema de CCTV se anuncian carteles con la señalización adecuada para indicar al público en general que se hace uso de este recurso por motivos de seguridad institucional.

Se prevé la confección de cápsulas de video para ser transmitidas en las pantallas de difusión instaladas en el centro, con la intención de sensibilizar y dar conocimientos sobre el tema a todos los miembros de la institución.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Delegación Administrativa			
Identificador único*	SILSFC3-CCTV-2023		
(Nombre del sistema A1)*	Monitoreo de CCTV		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la plataforma de grabado en red	*Mantener actualizado el sistema de gestión de cámaras y grabado*	*Cada año*	*Actualización de la plataforma web de grabado*
Actualización del sistema operativo del servidor que hospeda la plataforma	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Delegación Administrativa			
Identificador único*	SILSED3-SIC-2023		
(Nombre del sistema A1)*	Sistema Instituciona de Compras		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo del equipo del operario del sistema	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Delegación Administrativa			
Identificador único*	SILSED3-SIAF-2023		
(Nombre del sistema A1)*	Sistema Integral de Información Financiera		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo del equipo del operario del sistema	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Delegación Administrativa	
Identificador único*	SILSED3-MDA-2023

(Nombre del sistema A1)*	Módulo de Control de Asistencia del Sistema Integral de personal		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización del sistema operativo del equipo del operario del sistema	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Coordinación de Investigación			
Identificador único*	SILSVC3-CDTME-2023		
(Nombre del sistema A1)*	Plataforma de Registro de Conductome		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la plataforma para evitar ataques y robo de información	*Mantener actualizado el entorno de desarrollo de la plataforma (frameworks)*	*Continuamente*	*Actualización de la plataforma web del sistema*
Actualización del sistema operativo del servidor que hospeda la plataforma	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Coordinación de Investigación			
Identificador único*	SILSVC3-LS-2023		
(Nombre del sistema A1)*	Plataforma de Gestión de cuestionarios Lime Survey		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la plataforma para evitar ataques y robo de información	*Mantener actualizado el entorno de desarrollo de la plataforma (frameworks)*	*Continuamente*	*Actualización de la plataforma web del sistema*
Actualización del sistema operativo del servidor que hospeda la plataforma	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Coordinación Académica			
Identificador único*	SILSVC3-SGDWAAC3-2023		
(Nombre del sistema A1)*	Sistema de Gestión del Directorio Web de Académicos Asociados al C3		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la plataforma para evitar ataques y robo de información	*Mantener actualizado el entorno de desarrollo de la plataforma (frameworks)*	*Continuamente*	*Actualización de la plataforma web del sistema*
Actualización del sistema operativo del servidor que hospeda la plataforma	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

Coordinación Académica			
Identificador único*	SILNRC3-SGD-2023		
(Nombre del sistema A1)*	Sistema de Gestión de Difusión		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la plataforma para evitar ataques y robo de información	*Mantener actualizado el entorno de desarrollo de la plataforma (frameworks)*	*Continuamente*	*Actualización de la plataforma web del sistema*
Actualización del sistema operativo del servidor que hospeda la plataforma	*Mantener actualizados los elementos de seguridad del sistema operativo*	*Continuamente*	*Garantizar la seguridad del sistema*

9.2. Actualización y mantenimiento de equipo de cómputo

Actualización continua de los sistemas operativos de los equipos de los operarios de los sistemas de tratamiento de datos personales.

Actualización de los servidores que albergan los sistemas de tratamiento de datos personales para reducir vulnerabilidades.

Monitoreo de funcionalidad de los equipos (cámaras y servidor) del sistema de CCTV para garantizar el servicio. Controlar el tráfico hacia el segmento de red que mantiene el sistema.

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

Los datos que se recaban a través del sistema de CCTV son almacenados en el servidor que da soporte a la plataforma. Cada 3 semanas se hace una copia mediante un proceso de respaldo automático que graba la información en disco hacia un dispositivo externo.

Los sistemas desplegados en la institución están gestionados a través de entornos de virtualización. Cada noche se hace copia de la máquina que aloja los datos en los equipos que dan servicio de almacén de datos (MySQL, PostgreSQL). En el resto de los equipos la copia de la máquina virtual se realiza cada semana. En caso de algún evento se restaura la última máquina copiada tanto para el servidor del aplicativo como para el almacén de datos.

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

Este proceso está en definición. Por el momento los equipos y elementos de almacenamiento que han dejado de ser empleados en la gestión de datos personales se encuentran al resguardo del personal de cómputo en una sala con acceso restringido. Se están identificando herramientas informáticas adecuadas para la ejecución de un proceso seguro de borrado y limpieza de la información contenida en los dispositivos de almacenamiento de los equipos antes de darles de baja y hacerlos disponibles a las instituciones competentes dentro de la universidad.

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

En este instante se están creando las políticas definitivas de cancelación de los sistemas de datos personales. En este instante se procede de la siguiente manera (sujeto a cambios de la nueva política):

a) Se restringe el acceso al servicio desde la red de usuarios
b) Se inactivan las cuentas de acceso de todos los usuarios del sistema
c) Se desactiva el sistema para que no sea funcional y evitar posibles brechas de seguridad y acceso
d) El sistema queda resguardado en los servidores, aunque no es accesible ni funcional en espera de la política final para dar curso a su eliminación definitiva

11. APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

		Nombre y firma de quienes revisaron el presente documento:
Responsable del desarrollo:	Mtro. Romel Calero Ramos Responsable de seguridad de datos personales romel.calero@c3.unam.mx Lic. Adriana Cruz Cortés Delegada Administrativa yacortes@c3.unam.mx	
Revisó:		
Autorizó:		
Fecha de aprobación:		
Fecha de actualización:		