



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



Documento de Seguridad.

IA-SGSDP-DS

TABLA DE AUTORIZACIÓN:

Elaboró:

M. en I. Liliana Hernández Cervantes
Tel. +(52) (55) 5622-3932
liliana@astro.unam.mx
Responsable de Seguridad de Datos Personales

Lic. Maria Elena Santos Morales
Tel. +(52) (55) 5622-3932
msantos@astro.unam.mx
Enlace de Transparencia

Aprobó:

Dr. José de Jesús González González
Tel. +(52) (55) 5622-3936
jesus@astro.unam.mx
Director del Instituto de Astronomía

Fecha de emisión: 31 de julio de 2022



**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



PÁGINA EN BLANCO



Contenido

1	Introducción	4
2	Objetivo.....	5
3	Términos, definiciones y abreviaturas.....	5
3.1	Términos y definiciones	5
3.2	Abreviaturas.....	10
4	Alcance.....	10
4.1	Funciones y Responsabilidades.....	10
4.2	Sistema de Gestión de Seguridad de Datos personales.....	11
5	Anexos.....	17
5.1	Anexo 1 Lineamientos.....	18
5.2	Anexo 2 Inventario, Estructura y Descripción de los Sistemas de Tratamiento de Datos Personales.....	20
5.3	Anexo 3 Análisis de Riesgo	33
5.4	Anexo 4 Análisis de Brecha	45
5.5	Anexo 5 Plan de Trabajo	51
5.6	Anexo 6 Formatos para el cumplimiento de las MST	64



1 Introducción

El presente documento de seguridad contiene las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales del Instituto de Astronomía con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

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

Específicamente los artículos 31, 32 y 33 de la Ley General, del 55 al 72 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, así como del 20 al 31 de los Lineamientos para la protección de datos personales en posesión de la Universidad Nacional Autónoma de México, publicados en la Gaceta UNAM el 25 de febrero de 2019, documento contenido en el Anexo 1.

El cimiento del formato de documento de seguridad es la aplicación de un enfoque basado en los riesgos de los activos universitarios, específicamente los datos personales y los soportes que los resguardan. Además, el formato considera el tamaño y estructura de la institución, objetivos, clasificación de la información, requerimientos de seguridad y procesos que se precisan en razón de los activos que posee esta Máxima Casa de Estudios, lo cual se encuentran contemplado en el estándar internacional en materia de seguridad de la información ISO/IEC27002:2013 "Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información"



2 Objetivo

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales del Instituto de Astronomía de la Universidad Nacional Autónoma de México (IA), desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante cualquiera de los siguientes tipos de soportes:

- a) En soportes físicos.
- b) En soportes electrónicos.
- c) En redes de datos.

3 Términos, definiciones y abreviaturas

3.1 *Términos y definiciones*

3.1.1 Activo: Todo elemento de valor para la Universidad, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos o los documentos en papel.

3.1.2 Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el Responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de éstos.

3.1.3 Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable condicionados a criterios determinados, con independencia de la rama o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.



3.1.4 Borrado seguro: Procedimiento para la eliminación en un dispositivo o medio de almacenamiento, conocido o por conocer, que impide la recuperación de los datos personales.

3.1.5 Ciclo vital del documento: Las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación hasta su conservación permanente o baja documental, a saber: archivo de trámite, archivo de concentración y archivo histórico.

3.1.6 Confidencialidad: Es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por el Área Universitaria respectiva.

3.1.7 Control de seguridad en la red: Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

3.1.8 Disponibilidad: Es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de personas o procesos autorizados por el Área Universitaria respectiva.

3.1.9 Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Responsable para garantizar la Confidencialidad, Integridad y Disponibilidad de los datos personales que posee.

3.1.10 Encargado: La persona física o jurídica distinta a las áreas, entidades o dependencias universitarias, que realizan el tratamiento de los datos personales a nombre de la Universidad, suscribiendo para tal efecto los instrumentos consensuales correspondientes acordes con la Legislación Universitaria aplicable.

3.1.11. Evaluación de impacto en la protección de datos personales (EIDP): Documento mediante el cual las Áreas Universitarias que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los Responsables y Encargados, previstos en la normativa aplicable.



3.1.12 Integridad: Es el principio de seguridad de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que éstos no puedan ser modificados sin autorización, ya sea accidental o intencionadamente.

3.1.13 Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales;

3.1.14 Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

3.1.15 Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

3.1.16 Medidas de seguridad técnicas: Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en formato digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Asegurar que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;



- b) Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo, mantenimiento del software y hardware;
- d) Gestionar las comunicaciones, operaciones y medios, de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

3.1.17 Red de datos: Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

3.1.18 Responsable: Las Áreas Universitarias que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

3.1.19 Seguridad de la información: La preservación de la confidencialidad, integridad y disponibilidad de la información, que puede abarcar además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

3.1.20 Servicios de nube privada. Modelo de servicio de tecnología de información proporcionados bajo demanda a las Áreas Universitarias, en infraestructura propiedad de la Universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

3.1.21 Servicios de nube pública: Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena a la Universidad.

3.1.22 Sistema de Gestión de Seguridad de Datos Personales: Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

3.1.23 Sistemas para el tratamiento: Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.



3.1.24 Soporte: Medio, ya sea electrónico o físico, en el que se registra y guarda información, como lo es: el papel, así como los audiovisuales, fotográficos, filmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

3.1.25 Soportes electrónicos: Son los medios de almacenamiento accesibles sólo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs, DVDs y Blue-rays), discos magneto ópticos, discos magnéticos (flexibles y duros) y demás medios para almacenamiento masivo no volátil.

3.1.26 Soportes físicos: Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos, oficios, formularios impresos, escritos autógrafos, documentos de máquina de escribir, fotografías, placas radiológicas, carpetas, expedientes, entre otros;

3.1.27 Supresión: La erradicación del registro de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el Responsable.

3.1.28 Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del Responsable o del Encargado.

3.1.29 Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

3.1.30 Vulneración de seguridad: En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.



3.2 Abreviaturas

2.2.1 IA

Instituto de Astronomía de la UNAM

2.2.2 SGSDP

Sistema de Gestión de Seguridad de Datos Personales

4 Alcance

Aplica a todas las áreas administrativas, académicas y de servicio que tienen en su poder datos personales y datos personales sensibles.

4.1 Funciones y Responsabilidades

En el SGSDP del IA, la responsabilidad e interrelaciones del personal que trata datos personales, se mantiene con el siguiente organigrama:



Las funciones y responsabilidades generales de los integrantes del SGSDP son:

Titular.

Supervisar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla de acuerdo a este Documento de Seguridad.



**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



Responsable.

Verificar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a este Documento de Seguridad.

Enlace de Transparencia

Mantener informados al Titular y Responsable sobre los requerimientos y solicitudes de la Unidad de Transparencia de la Universidad.

Encargados.

Mantener el Sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a este Documento de Seguridad.

Usuarios.

Utilizar el Sistema de Gestión de Seguridad de Datos Personales en sus áreas específicas (administrativas, académicas y/o de servicio) de acuerdo a este Documento de Seguridad.

En el Instituto de Astronomía los roles son:

Rol	Figura
Director	Dr. José de Jesús González González Director del Instituto de Astronomía
Responsable.	M. en I. Liliana Hernández Cervantes Responsable designado por el director del Instituto de Astronomía
Enlace de Transparencia	Lic. Maria Elena Santos Morales Enlace con la Unidad de Transparencia, designado por el Director del Instituto
Encargados	De acuerdo al uso de datos personales definido en el Anexo 2 Secretario Académico Secretario Administrativo Jefatura de la Unidad de Astrofísica Computacional
Usuarios	Definido en el Anexo 2, de acuerdo al uso de datos personales.

4.2 Sistema de Gestión de Seguridad de Datos personales

4.2.1 SGSDP, Política y Objetivo

El IA establece y mantiene un Sistema de Gestión de Seguridad de Datos Personales y documenta sus políticas, sistemas, programas, procedimientos e instrucciones necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, según el REGLAMENTO DE



TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO publicado el 26 de agosto de 2016 y a las NORMAS COMPLEMENTARIAS SOBRE MEDIDAS DE SEGURIDAD TÉCNICAS, ADMINISTRATIVAS Y FÍSICAS PARA LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LA UNIVERSIDAD publicadas el 10 de enero de 2020.

Política del Sistema de Seguridad de Datos Personales

El Instituto de Astronomía se compromete a cumplir con las medidas de seguridad para la protección de datos personales desde su obtención, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos personales sensibles que se recaben y de accesos no autorizados ni de tratamientos distintos a los fines para los que fueron recabados mediante soportes físicos, electrónicos o en redes de datos.

Objetivo del SGSDP.

El objetivo del SGSDP es asegurar la integridad, confidencialidad y disponibilidad de la información que contengan datos personales.

4.2.2 Inventario

El SGSDP cuenta con un inventario con información sobre el tratamiento de datos personales por área administrativa, académica o de servicio responsable, que se encuentra en el **Anexo 2** y que considera:

- I. El catálogo de recursos a través de los cuales se obtienen los datos personales;
- II. Las finalidades de cada tratamiento de datos personales;
- III. El catálogo de los tipos de datos personales que se traten;
- IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
- V. La lista de funcionarios o empleados universitarios que tienen acceso a los sistemas de tratamiento;
- VI. Los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.



4.2.3 Ciclo de Vida

En dicho inventario se incluye el ciclo de vida de los datos personales conforme a las siguientes etapas:

- La obtención de los datos personales;
- El almacenamiento de los datos personales;
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- El bloqueo de los datos personales, en su caso, y
- La cancelación, supresión o destrucción de los datos personales.

4.2.4 Anexo de inventario

Cada sistema de tratamiento sirve para realizar la obtención, uso, registro, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos. El detalle de cada sistema de tratamiento de datos personales por área administrativa, académica o de servicio responsable se encuentra en el **Anexo 2** de este documento.

4.3 Análisis de Riesgos

El IA realiza un análisis de riesgos del tratamiento de los datos personales que se encuentra en el **Anexo 3** y de acuerdo a la siguiente metodología:

- a) Los riesgos sobre el tratamiento de datos personales se detectan por área administrativa, académica o de servicio y por cualquier persona que dé tratamiento de, datos personales.
- b) Se realiza la Matriz de Riesgos Por Tratamiento de Datos Personales donde se identifica:
 - Tratamiento de datos personales. Clave de tratamiento de datos personales conforme al inventario.
 - Riesgo probable. Enunciado del riesgo identificado, tomando en cuenta:
 - i. Los requerimientos regulatorios, legales y reglamentarios.



- ii. El valor de los datos personales de acuerdo a si son sensibles o no y su ciclo de vida;
- iii. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- iv. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- v. Los siguientes factores:
 - El riesgo inherente a los datos personales tratados;
 - La sensibilidad de los datos personales tratados;
 - El desarrollo tecnológico.
 - Las posibles consecuencias de una vulneración para los titulares;
 - Las transferencias de datos personales que se realicen;
 - El número de titulares;
 - Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
 - El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
- Causa probable. La causa probable del riesgo. Pueden usarse las herramientas del análisis de causa es como los 5 por qué, diagrama de Ishikawa, entre otros.
- Probabilidad. La probabilidad subjetiva de que ocurra el riesgo. Es la posibilidad de que ocurra una vulneración de seguridad a los datos personales. Para determinar su probabilidad se toma en cuenta el número de áreas en las que se ha identificado el riesgo.

Criterio cuya escala es:

Probabilidad.	Escala.
De 1 a 3 áreas. **	Bajo
De 4 a 5 áreas,	Medio.
De 6 a 7 áreas.	Alto.

Tabla 1. Escala de probabilidad

*** en las medidas de seguridad*

- Impacto. El impacto de riesgo se refiere al impacto de las consecuencias negativas, daño o afectación para los titulares que pudieron derivar de una vulneración de seguridad ocurrida en los datos personales. Criterio cuya escala es:



**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



Impacto	Escala
No impacta a la integridad, confidencialidad ni disponibilidad de datos personales.	Bajo.
Impacta a la integridad, confidencialidad o disponibilidad de datos personales.	Medio.
Impacta a la integridad, confidencialidad y disponibilidad de datos personales.	Alto.

Tabla 2. Escala de impacto

- Cálculo de Nivel de valor de Riesgo. Para este caso, se asume que el Impacto y la Probabilidad tienen el mismo valor para la evaluación del riesgo. Se identifica en la gráfica Probabilidad vs Impacto la zona en la que se encuentra el riesgo identificado para asignarle su nivel de valor de riesgo, que definirá la prioridad con la que se tratarán los riesgos, de la siguiente manera:

Escala		Probabilidad		
		Bajo	Medio	Alto
Impacto	Bajo	Bajo	Medio	Medio
	Medio	Medio	Medio	Alto
	Alto	Medio	Alto	Alto

Grafica 1. Probabilidad vs. Impacto.

El nivel de riesgo determinará la prioridad de riesgo de la siguiente manera:

Nivel de Riesgo.	Prioridad.
Bajo.	Planificar acción y documentar en no más de 20 días hábiles desde su detección.
Medio.	Planificar acción y documentar en no más de 10 días hábiles desde su detección.
Alto.	Planificar acción y documentar inmediatamente.

Tabla 3. Nivel de prioridad de riesgo

- c) Una vez identificados los riesgos y su prioridad, se define el tratamiento del riesgo, el cual puede ser:



- Mitigar: acciones que minimicen los efectos que pudieran surgir por los riesgos.
 - Eliminar: acciones que desaparezcan los efectos del riesgo.
 - Transferir: acciones que trasladen el riesgo. Generalmente ocurre cuando no se tiene control total sobre la situación.
 - Aceptar: Generalmente ocurre cuando no se tiene control total sobre la situación.
- d) Una vez identificado el tratamiento del riesgo se plantean acciones para mitigar, eliminar, transferir o aceptar el riesgo, debiendo considerar los controles de seguridad física, administrativa y técnica para la protección de datos personales.
- e) Cuando se identifique algún riesgo se debe notificar a los responsables del SGDPD para que la integre a la Matriz de Riesgos.

4.4 Análisis de Brecha

El IA realiza un análisis de brecha que se encuentra en el **Anexo 4** considerando:

- Las medidas de seguridad existentes y efectivas;
- El nivel óptimo de medidas de seguridad y
- Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

4.5 Plan de trabajo.

4.5.1 Plan de Trabajo y Alcances

El IA cuenta con un plan de trabajo que define los controles de seguridad a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo detectado.

Lo anterior, considerando los recursos asignados, el personal interno y externo al área, así como las fechas establecidas para la implementación de los controles de seguridad nuevos o faltantes.

El Plan de Trabajo se encuentra en el **Anexo 5** de este documento.



4.6 Medidas de seguridad para la protección de datos personales.

El IA implementa medidas de seguridad técnicas, administrativas y físicas para asegurar la protección de los datos personales presentadas en el Anexo 2.

4.7 Capacitación.

Para capacitar a la comunidad del IA, se establece lo siguiente:

- Charlas informativas sobre temas de protección de datos personales
- Correos masivos con información del tema
- Generación de elementos gráficos con información de protección de datos personales

Esta capacitación debe de incluir los siguientes temas:

- I. Los requerimientos y actualizaciones del sistema de gestión;
- II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
- III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

5 Anexos

Anexo 1	Lineamientos
Anexo 2	Inventario, Estructura y Descripción de Sistemas de Tratamiento de Datos Personales
Anexo 3	Análisis de Riesgo
Anexo 4	Análisis de Brecha
Anexo 5	Plan de Trabajo
Anexo 6	Formatos para el cumplimiento de las MST



5.1 Anexo 1 Lineamientos



Lineamientos

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 26 de enero de 2017, URL <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>
- Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicados en el Diario Oficial de la Federación el 26 de enero de 2018, URL https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0
- Acuerdo por el que se establecen los lineamientos para la protección de datos personales en posesión de la universidad nacional Autónoma de México, URL https://www.red-tic.unam.mx/recursos/2019/2019_Acuerdo_Rectoria_02.pdf



5.2 Anexo 2 Inventario, Estructura y Descripción de los Sistemas de Tratamiento de Datos Personales



1. Inventario de los Sistemas de Tratamiento de Datos Personales

INSTITUTO DE ASTRONOMÍA	
Identificador	D1012a
Nombre del sistema	Sistema de Informes y Planes de Trabajo Anuales
Datos personales (sensibles o no) contenidos en el sistema:	Datos recabados del personal académico que labora en el Instituto de Astronomía: <ul style="list-style-type: none">• Nombre Completo• Email institucional• Número de Trabajador• Nombramiento• Nivel de PRIDE• Nivel de SNI• Antigüedad• Departamento• Usuario• Contraseña• Informes de trabajo Anuales• Planes de trabajo Anuales• Evaluación de los informes y planes de trabajo por el Consejo Interno
Responsable:	Secretaria Académica
Nombre:	María Magdalena González Sánchez
Cargo:	Secretaria Académica
Funciones:	<ul style="list-style-type: none">• Mantener actualizada la base de datos de los usuarios• Recabar y distribuir al Consejo Interno, los informes y planes de trabajo de los académicos, para su evaluación.• Consultar la base de datos.• Validar y actualizar los formatos de captura y de impresión del sistema.
Obligaciones:	<ul style="list-style-type: none">• Mantener actualizado el estatus del personal académico.• Indicar cuando de abre y cierra el sistema para la captura de los informes y planes.• Mantener la confidencialidad de la información.• Mantener actualizado el listado de los integrantes del Consejo Interno.
Encargados:	
Nombre:	Liliana Hernández Cervantes
Cargo:	Desarrolladora
Funciones:	<ul style="list-style-type: none">• Desarrollo del sistema, mantener la disponibilidad e integridad de los datos, hacer modificaciones y actualizaciones a la base de datos y los formatos, de acuerdo con los requerimientos de la Secretaría Académica.



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



	<ul style="list-style-type: none">• Generar los reportes electrónicos de los informes y planes de trabajo, para su evaluación ante el Consejo Interno.
Obligaciones:	<ul style="list-style-type: none">• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• Mantener en operación el sistema.• Realizar respaldos del sistema.• Mantener la seguridad e integridad de la información.• Hacer modificaciones al sistema cuando sean solicitados por la secretaría académica.
Nombre:	Francisco Ruiz Sala
Cargo:	Desarrollador
Funciones:	<ul style="list-style-type: none">• Desarrollo del sistema, mantener la disponibilidad e integridad de los datos, hacer modificaciones y actualizaciones a la base de datos y los formatos, de acuerdo con los requerimientos de la Secretaría Académica.• Generar los reportes electrónicos de los informes y planes de trabajo, para su evaluación ante el Consejo Interno.
Obligaciones:	<ul style="list-style-type: none">• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• Mantener en operación el sistema.• Realizar respaldos del sistema.• Mantener la seguridad e integridad de la información.• Hacer modificaciones al sistema cuando sean solicitados por la secretaría académica.
	Usuarios:
Nombre:	José de Jesús González González
Cargo:	Director
Funciones:	Coordinar la elaboración de los planes de desarrollo y los programas e informes anuales del Instituto, para su presentación ante el Consejo Técnico de la Investigación Científica y ante otras autoridades de la Universidad Nacional Autónoma de México, cuando así proceda.
Obligaciones:	<ul style="list-style-type: none">• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• No divulgar información de los académicos, fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.• Hacer uso de los datos únicamente para los fines para los que han sido recabados.
Nombre:	María Magdalena González Sánchez
Cargo:	Secretaría Académica
Funciones:	Consultar el sistema de los informes y planes de trabajo anuales del personal académico para trámites inherentes de la secretaría académica
Obligaciones:	<ul style="list-style-type: none">• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• No divulgar información de los académicos, fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



	<ul style="list-style-type: none">Hacer uso de los datos únicamente para los fines para los que han sido recabados.
Nombre:	Lourdes Margarita Pérez Carmona
Cargo:	Secretaría Auxiliar
Funciones:	Consultar el sistema de los informes y planes de trabajo anuales del personal académico para trámites inherentes de la secretaría académica
Obligaciones:	<ul style="list-style-type: none">Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.No divulgar información de los académicos, fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.Hacer uso de los datos únicamente para los fines para los que han sido recabados
Nombre:	<u>Consejeros Internos (Cuerpo Colegiado) del Instituto de Astronomía</u>
Cargo:	Consejeros Internos del Instituto de Astronomía
Funciones:	<ul style="list-style-type: none">Conocer, revisar y emitir recomendaciones sobre los informes y planes de trabajo del personal académico del Instituto
Obligaciones:	<ul style="list-style-type: none">Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información a cualquier persona externa al Consejo Interno
Nombre:	Maria Elena Santos Morales
Cargo:	Secretaría Técnica de Asuntos Externos
Funciones:	<ul style="list-style-type: none">Recabar información de los planes e informes del trabajo del personal académicos con fines estadísticos para los diferentes informes del Instituto ante las distintas instancias universitarias
Obligaciones:	<ul style="list-style-type: none">Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.No divulgar información de los académicos, fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.Hacer uso de los datos únicamente para los fines para los que han sido recabados.



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



INSTITUTO DE ASTRONOMÍA	
Identificador	D1012b
Nombre del sistema	Sistema COSE
Datos personales (sensibles o no) contenidos en el sistema:	Datos recabados de los estudiantes asociados al Instituto de Astronomía: <ul style="list-style-type: none">• Nombre Completo• Email personal• Email institucional• Teléfono particular• Teléfono de contacto• Nombre de contacto• Fotografía• Email asesor• Antecedentes académicos• Reportes semestrales estudiante• Reporte semestra del comité o tutor• Reporte de la Comisión de Servicios Estudiantiles
Responsables:	Comisión de Servicios Estudiantiles del Instituto de Astronomía (COSE)
Nombre:	<u>Integrantes de la Comisión de Servicios Estudiantiles en CU</u>
Cargo:	Integrantes de la Comisión de Servicios Estudiantiles del Instituto de Astronomía (COSE)
Funciones:	<ul style="list-style-type: none">• Dar de alta y baja a los estudiantes asociados al Instituto.• Cambiar el estatus del estudiante.• Gestionar los servicios que ofrece el Instituto de Astronomía a los estudiantes asociados.• Revisar y evaluar los informes de estudiantes asociados, de asesor o de comité según sea el caso• Consultar la base de datos
Obligaciones:	<ul style="list-style-type: none">• Mantener actualizado el estatus de los estudiantes asociados al Instituto de Astronomía en función de los estatutos de la COSE.• Dar seguimiento y evaluación a los reportes académicos los estudiantes.• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• No divulgar información de los estudiantes fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.• Hacer uso de los datos únicamente para los fines para los que han sido recabados.
	Encargados:
Nombre:	Liliana Hernández Cervantes
Cargo:	Desarrolladora



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



Funciones:	Desarrollar, programar y actualizar el sistema en función de los requerimientos de la COSE
Obligaciones:	<ul style="list-style-type: none">• Programar los cambios solicitados por los integrantes de la COSE.• Mantener el operación el sistema.• Realizar respaldos del sistema.• Mantener la seguridad e integridad de la información.• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.
Nombre:	Francisco Ruiz Sala
Cargo:	Desarrollador
Funciones*:	Desarrollar, programar y actualizar el sistema en función de los requerimientos de la COSE
Obligaciones*:	<ul style="list-style-type: none">• Programar los cambios solicitados por los integrantes de la COSE.• Mantener el operación el sistema.• Realizar respaldos del sistema.• Mantener la seguridad e integridad de la información.• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.
Usuarios:	
Nombre:	Integrantes de las comisiones de servicios estudiantiles del Instituto de Astronomía: <u>Integrantes de la Comisión de Servicios Estudiantiles en CU</u> Integrantes de la Comisión de Servicios Estudiantiles en Ensenada
Cargo:	Integrantes de la Comisión de Servicios Estudiantiles
Funciones:	<ul style="list-style-type: none">• Revisar los reportes de estudiantes, asesores o comité.• Evaluar los informes de los estudiantes para determinar la continuidad como estudiante asociado.• Mantener actualizado el estatus de los estudiantes.
Obligaciones*:	<ul style="list-style-type: none">• Mantener actualizado el estatus de los estudiantes asociados al Instituto de Astronomía en función de los estatutos de la COSE.• Dar seguimiento y evaluación a los reportes académicos los estudiantes.• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• No divulgar información de los estudiantes fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.• Hacer uso de los datos únicamente para los fines para los que han sido recabados.
Nombre:	Personal Académico del Instituto
Cargo:	Responsables de estudiantes asociados al Instituto
Funciones:	Evaluar el desempeño académico semestral de sus estudiantes asociados.



**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



Obligaciones:	<ul style="list-style-type: none">• Llenar el reporte semestral de los estudiantes asociados.• No divulgar la información de los estudiantes, fuera de las instancias relevantes dentro de la Universidad Nacional Autónoma de México.
Nombre:	Estudiantes Asociados el IA
Cargo:	Ninguno son estudiantes asociados
Funciones:	Capturar y mantener actualizada semestralmente su trabajo académico en el sistema
Obligaciones:	Capturar y mantener actualizada semestralmente su trabajo académico en el sistema



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



INSTITUTO DE ASTRONOMÍA	
Identificador	Regsol.3.70
Nombre del sistema	Registro de Solicitudes en Línea
Datos personales (sensibles o no) contenidos en el sistema*:	Datos del personal académico que labora en el Instituto de Astronomía: <ul style="list-style-type: none">• Nombre Completo• Email institucional• Número de Trabajador• Nombramiento• Usuario• Contraseña cifrada
Responsable:	Secretaría Académica
Nombre:	María Magdalena González Sánchez
Cargo:	Secretaría Académica
Funciones:	<ul style="list-style-type: none">• Mantener actualizada la base de datos de usuarios• Recabar y distribuir al Consejo Interno la información de todos los casos académicos a revisar.• Consultar la base de datos• Validar y actualizar los formatos de captura e impresión del sistema
Obligaciones:	<ul style="list-style-type: none">• Mantener actualizado el listado de los integrantes del Consejo Interno• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.• No divulgar información fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.• Hacer uso de los datos únicamente para los fines para los que han sido recabados.
	Encargados:
Nombre:	Urania Ceseña Borbon
Cargo:	Jefa de Cómputo, sede Ensenada
Funciones:	Mantener disponibilidad e integridad de los datos del sistema, hacer modificaciones y actualizaciones de los formatos de acuerdo a los requerimientos de la Secretaría Académica
Obligaciones:	<ul style="list-style-type: none">• Mantener en operación el sistema• Realizar respaldos del sistema• Mantener la seguridad e integridad de la información• Hacer modificaciones al sistema cuando sean solicitados por la secretaría académica• Conocer la privacidad de los datos que se manejan y mantener el secreto de dicha información.



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



	<ul style="list-style-type: none">No divulgar información fuera de las instancias relevantes de la Universidad Nacional Autónoma de México.
	Usuarios:
Nombre:	María Magdalena González Sánchez
Cargo:	Secretaria Académica
Funciones:	Recopilar las solicitudes del personal académico, para su revisión por los cuerpos colegiados CADE y CI. Generar solicitudes asociadas a la secretaria académica
Obligaciones:	No divulgar información de los académicos, fuera de las instancias relevantes de la UNAM.
Nombre:	Lourdes Margarita Pérez Cardona
Cargo:	Funcionario Secretaria Auxiliar
Funciones:	Recopilar las solicitudes del personal académico, para su revisión por los cuerpos colegiados CADE y CI. Generar solicitudes asociadas a la secretaria académica
Obligaciones:	No divulgar información de los académicos, fuera de las instancias relevantes de la UNAM.
Cargo:	Consejeros Internos (Cuerpo Colegiado) del Instituto de Astronomía
Funciones:	<ul style="list-style-type: none">Revisar y evaluar las solicitudes del personal académico del InstitutoEmitir recomendaciones sobre las solicitudes hechas al Consejo Interno
Obligaciones:	No divulgar información fuera del Consejo Interno
Nombre:	Miembros de la CADE (Comisión Académica de Ensenada)
Cargo:	Comisión Académica de Ensenada
Funciones:	<ul style="list-style-type: none">Revisar y emitir una opinión al Consejo Interno sobre las solicitudes del personal académico del Instituto de las sedes Ensenada y OAN-SPM
Obligaciones:	<ul style="list-style-type: none">No divulgar información fuera de la CADE



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



INSTITUTO DE ASTRONOMÍA	
Identificador único	SIP
Nombre del sistema	Sistema Integral de Personal
Datos personales (sensibles o no) contenidos en el sistema:	Datos personales, datos de reclutamiento y selección, nombramiento, incidencias, de capacitación, del puesto, correo electrónico, ingresos y egresos, cuentas bancarias, seguros, títulos, cédula profesional, certificados y reconocimientos, incapacidades médicas.
Responsable	
Nombre:	Carlos Alberto Téllez Esquivel
Cargo:	Jefe del departamento de Personal y Servicios Generales
Funciones:	Gestión de los trámites del personal académico, administrativo de base y de confianza.
Obligaciones:	Compromiso de confidencialidad, no divulgación de la información, reserva y resguardo de información y de datos personales.
	Encargados
Nombre:	José de Jesús González González
Cargo:	Director del IA
Funciones:	Relación de contratos para firma del Titular
Obligaciones:	Firmar el sistema, mantener la confidencialidad de los datos personales
Nombre:	Angelina Salmerón Godoy
Cargo:	Secretaria Administrativa
Funciones:	Autorización de contratos y adendas, autorización de notificación, ropa de trabajo, trámite de solicitudes
Obligaciones:	Firmar el sistema, mantener la confidencialidad de los datos personales
	Usuarios:
Nombre del Usuario:	Carlos Alberto Téllez Esquivel
Cargo:	Jefe del departamento de Personal y Servicios Generales
Funciones:	Gestión de los trámites del personal académico, administrativo de base y de confianza.
Obligaciones:	Compromiso de confidencialidad, no divulgación de la información, reserva y resguardo de información y de datos personales.
Nombre del Usuario	Marcela Margarita López González
Cargo:	Secretaria
Funciones:	Efectuar los trámites necesarios para el descuento por inasistencias y retardos del personal, ajustándose a las políticas establecidas.
Obligaciones:	Capturar las inasistencias del personal administrativo de base.



Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad



INSTITUTO DE ASTRONOMÍA	
Identificador único	Videovigilancia
Nombre del sistema	Videovigilancia
Datos personales (sensibles o no) contenidos en el sistema:	De incidencia
Responsable	
Nombre:	Fernando Garfias Macedo
Cargo:	Secretario Técnico
Funciones:	Mantener en operación el sistema de videovigilancia
Obligaciones:	Compromiso de confidencialidad, no divulgación de la información, reserva y resguardo de información y de datos personales.
	Encargados
Nombre:	Carmelo Jorge Guzmán Cerón
Cargo:	Responsable de los equipos de videovigilancia
Funciones:	Mantener en operación el sistema de videovigilancia en la sede Ciudad Universitaria, realizar respaldos de los videos, entregar videos solicitados por la unidad administrativa en caso de incidencias
Obligaciones:	Compromiso de confidencialidad, no divulgación de la información, reserva y resguardo de información y de datos personales.
	Usuarios:
Nombre del Usuario:	Vigilantes de la recepción
Cargo:	Vigilantes
Funciones:	Avisar en caso de una incidencia
Obligaciones:	Compromiso de confidencialidad, no divulgación de la información, reserva y resguardo de información y de datos personales.



2. Estructura y Descripción de los Sistemas de Tratamiento de Datos Personales

INSTITUTO DE ASTRONOMÍA	
Identificador	D1012a
Nombre del sistema	Sistema de Informes y Planes de Trabajo Anuales
Tipo de soporte:	Electrónico
Descripción:	Servidor de base de datos
Características del lugar donde se resguardan los soportes:	El servidor de base de datos se encuentra en un área de servidores con acceso restringido (sólo accede personal de cómputo), cuenta con energía regulada, red de alta velocidad y sistemas de enfriamiento.
Ubicación de respaldo de la base de datos del sistema:	Se encuentra localizado en un equipo de cómputo, en una oficina con acceso restringido, los respaldos son incrementales.

Identificador	D1012b
Nombre del sistema	Sistema COSE
Tipo de soporte:	Electrónico
Descripción:	Servidor de base de datos
Características del lugar donde se resguardan los soportes:	El servidor de base de datos se encuentra en un área para servidores con acceso restringido (sólo accede personal de cómputo), cuenta con energía regulada, red de alta velocidad y sistemas de enfriamiento.
Ubicación de respaldo de la base de datos del sistema:	Se encuentra localizado en un equipo de cómputo, en una oficina con acceso restringido, los respaldos son incrementales.

INSTITUTO DE ASTRONOMÍA	
Identificador	REGSOL.3.70a
Nombre del sistema	Registro de Solicitudes en Línea
Tipo de soporte:	Electrónico
Descripción:	Servidor de base de datos
Características del lugar donde se resguardan los soportes:	El servidor de base de datos se encuentra en un área para servidores con acceso restringido (sólo accede personal de cómputo), cuenta con energía regulada, red de alta velocidad y sistemas de enfriamiento.
Ubicación de respaldo de la base de datos del sistema	Se encuentra localizado en un equipo de cómputo, en una oficina con acceso restringido, los respaldos son incrementales.



**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



INSTITUTO DE ASTRONOMÍA	
Identificador	SIP
Nombre del sistema	Sistema Integral de Personal
Tipo de soporte:	Electrónico
Descripción:	Base de datos
Características del lugar donde se resguardan los soportes:	El departamento encargado del soporte del Sistema Integral de Personal es la Dirección General de Personal, Dirección de Sistemas
Ubicación de respaldo de la base de datos del sistema	No aplica

INSTITUTO DE ASTRONOMÍA	
Identificador	Videovigilancia
Nombre del sistema	Videovigilancia
Tipo de soporte:	Electrónico
Descripción:	Base de datos
Características del lugar donde se resguardan los soportes:	El servidor se encuentra en un área para servidores con acceso restringido (sólo accede personal de cómputo), cuenta con energía regulada, red de alta velocidad y sistemas de enfriamiento.
Ubicación de respaldo de la base de datos del sistema	No aplica

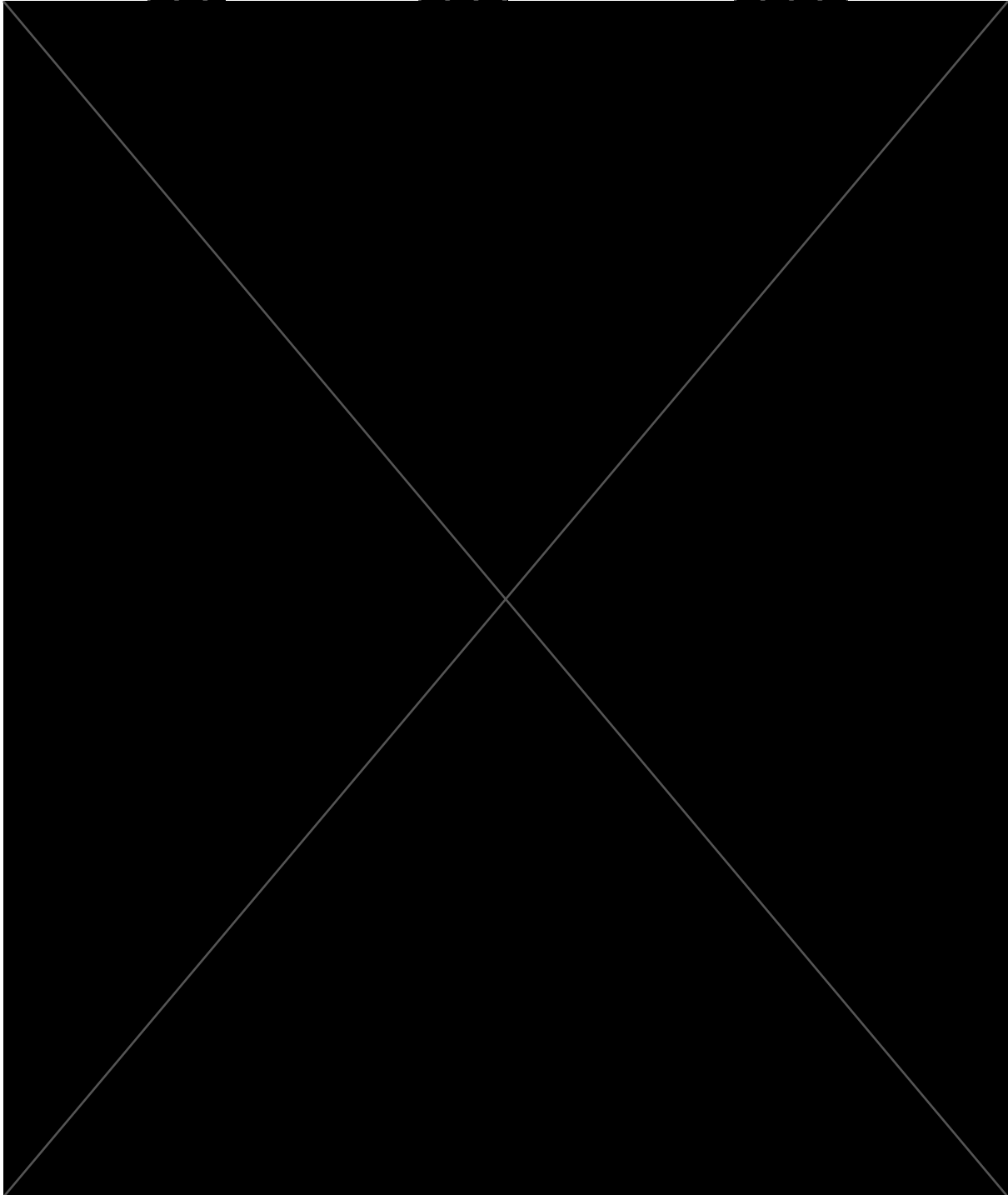


5.3 Anexo 3 Análisis de Riesgo



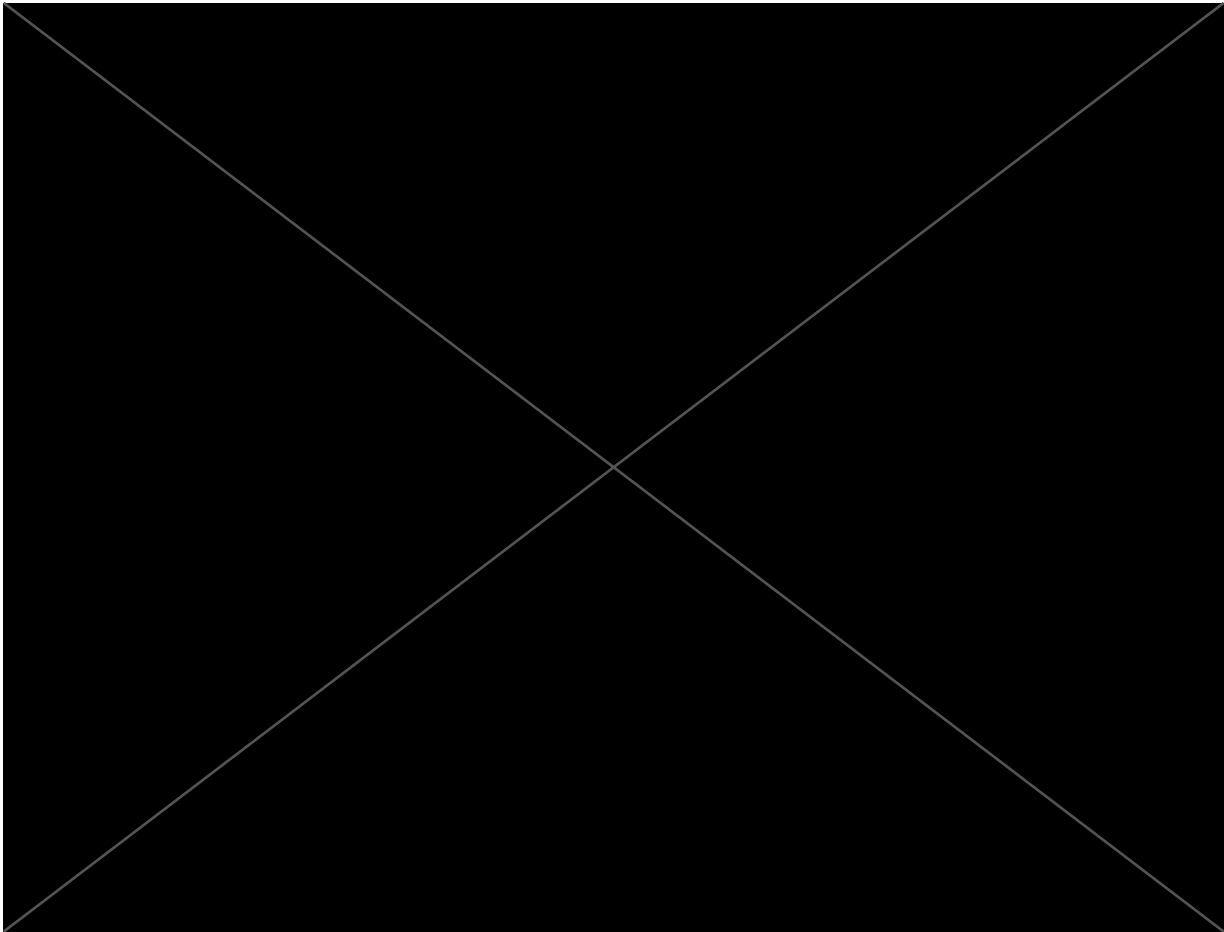
Análisis de Riesgo

INSTITUTO DE ASTRONOMÍA	
Identificador	D1012a
Nombre del sistema	Sistema de Informes y Planes de Trabajo Anuales





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

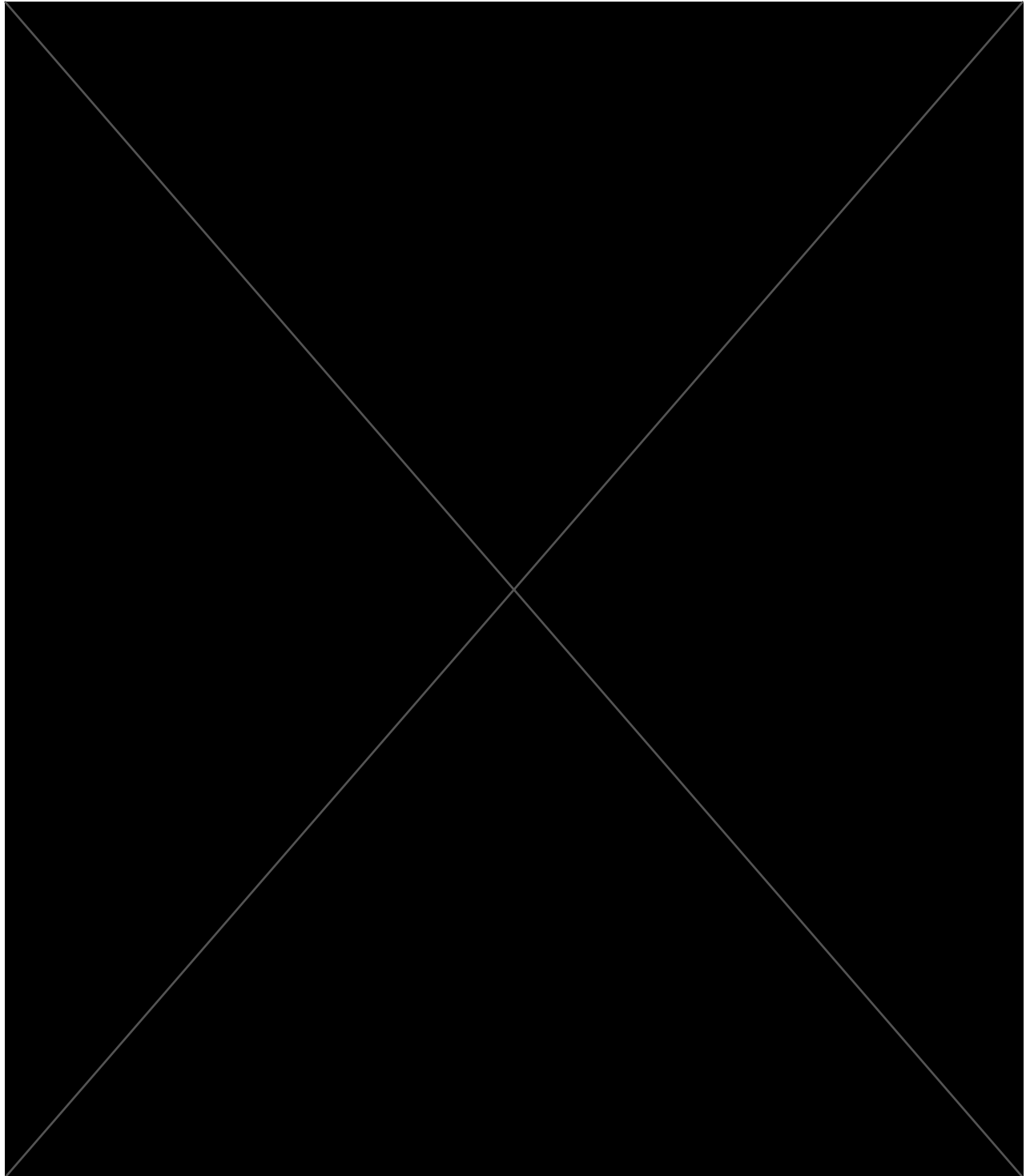


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



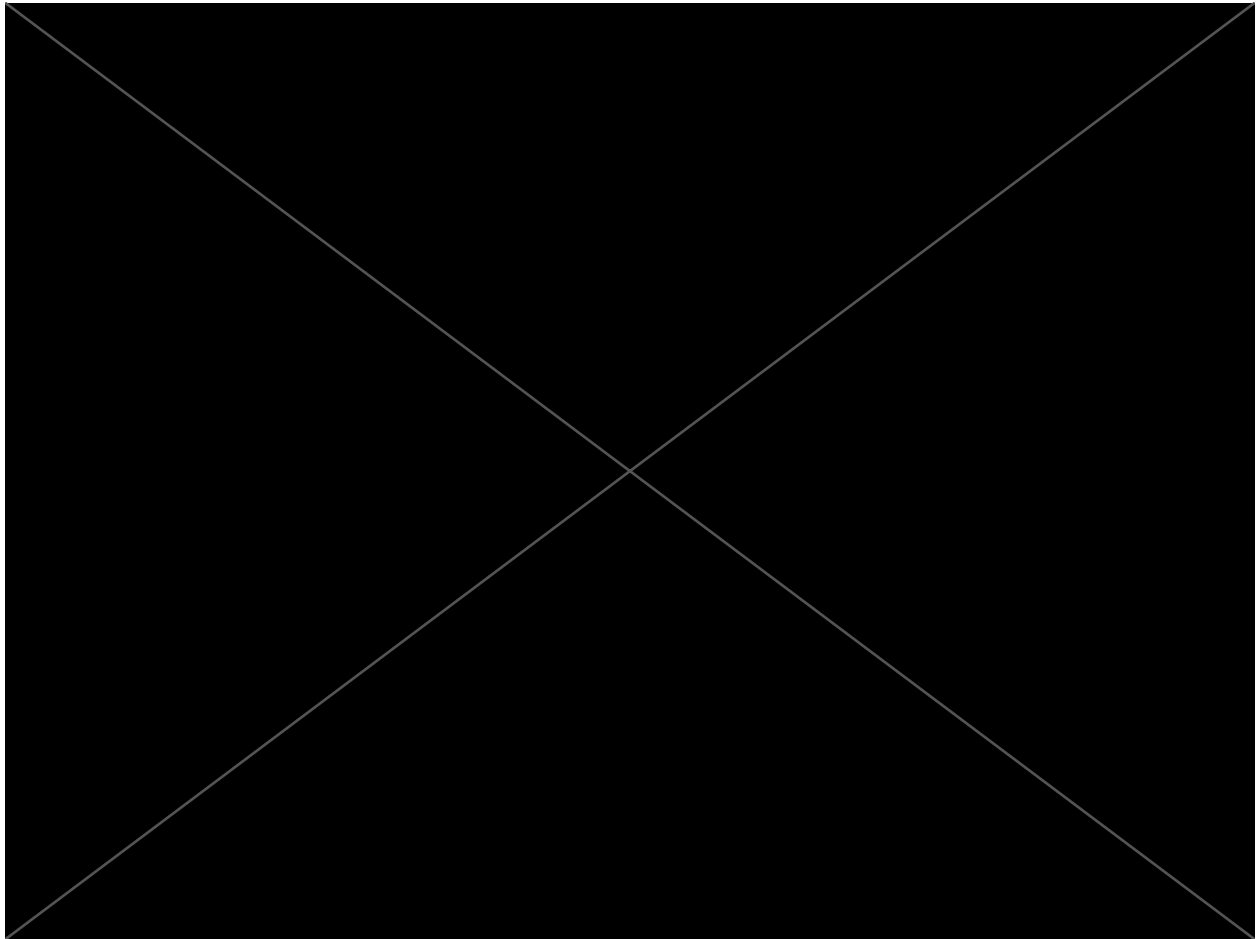
Análisis de Riesgo

INSTITUTO DE ASTRONOMÍA	
Identificador único	D1012b
Nombre del sistema	Sistema de la COSE





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

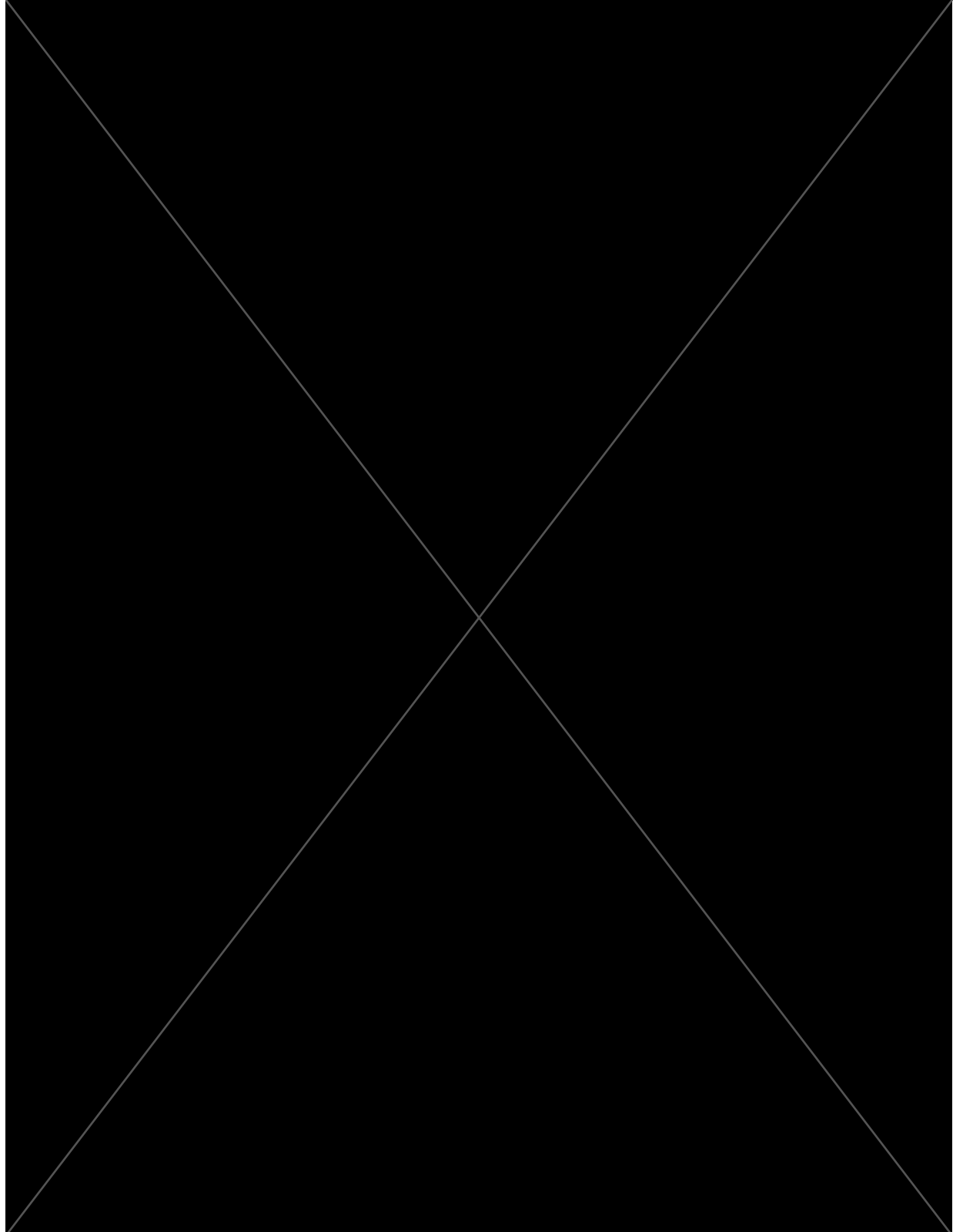


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



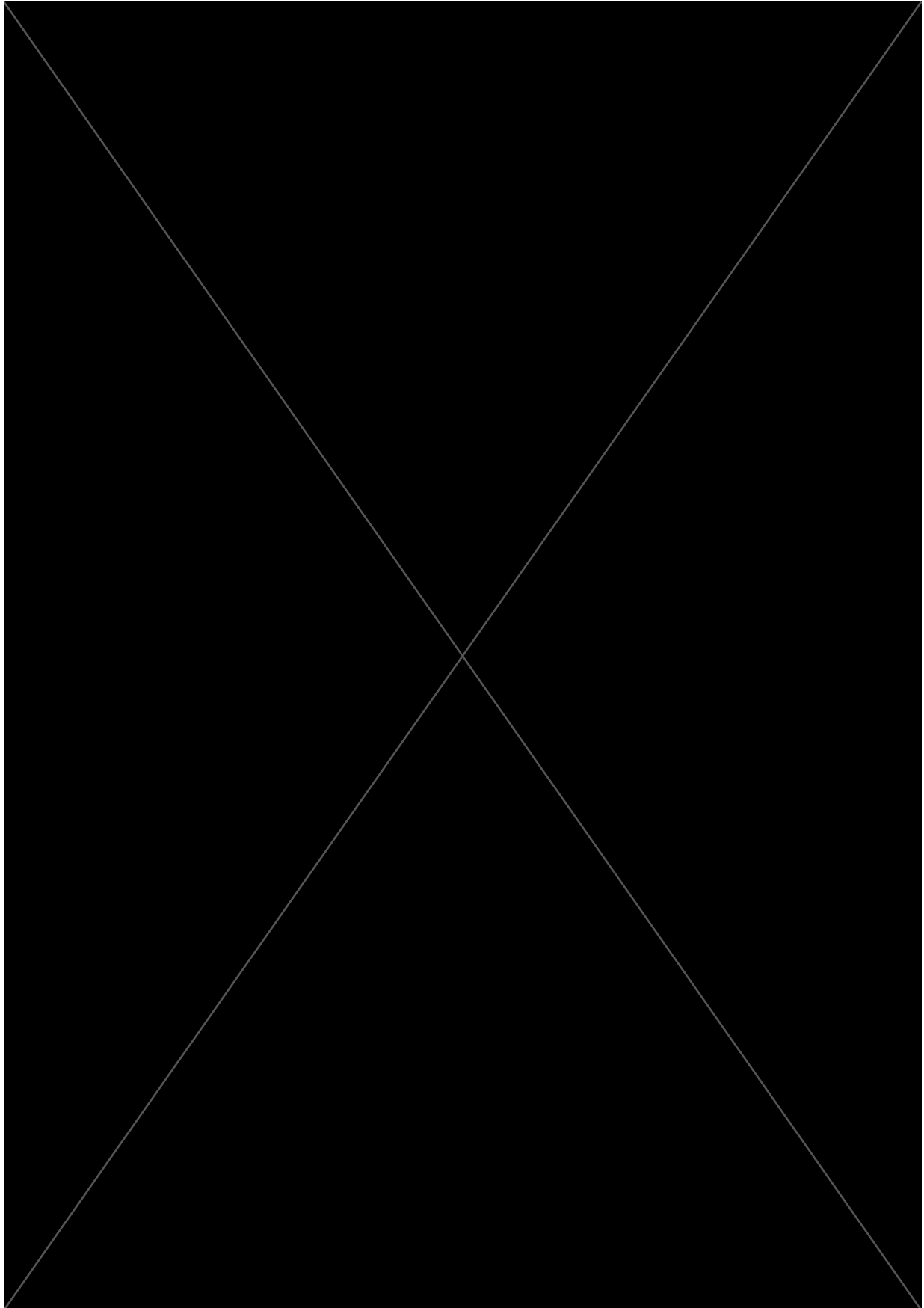
Análisis de Riesgo

INSTITUTO DE ASTRONOMÍA	
Identificador único	Re sol.3.70a



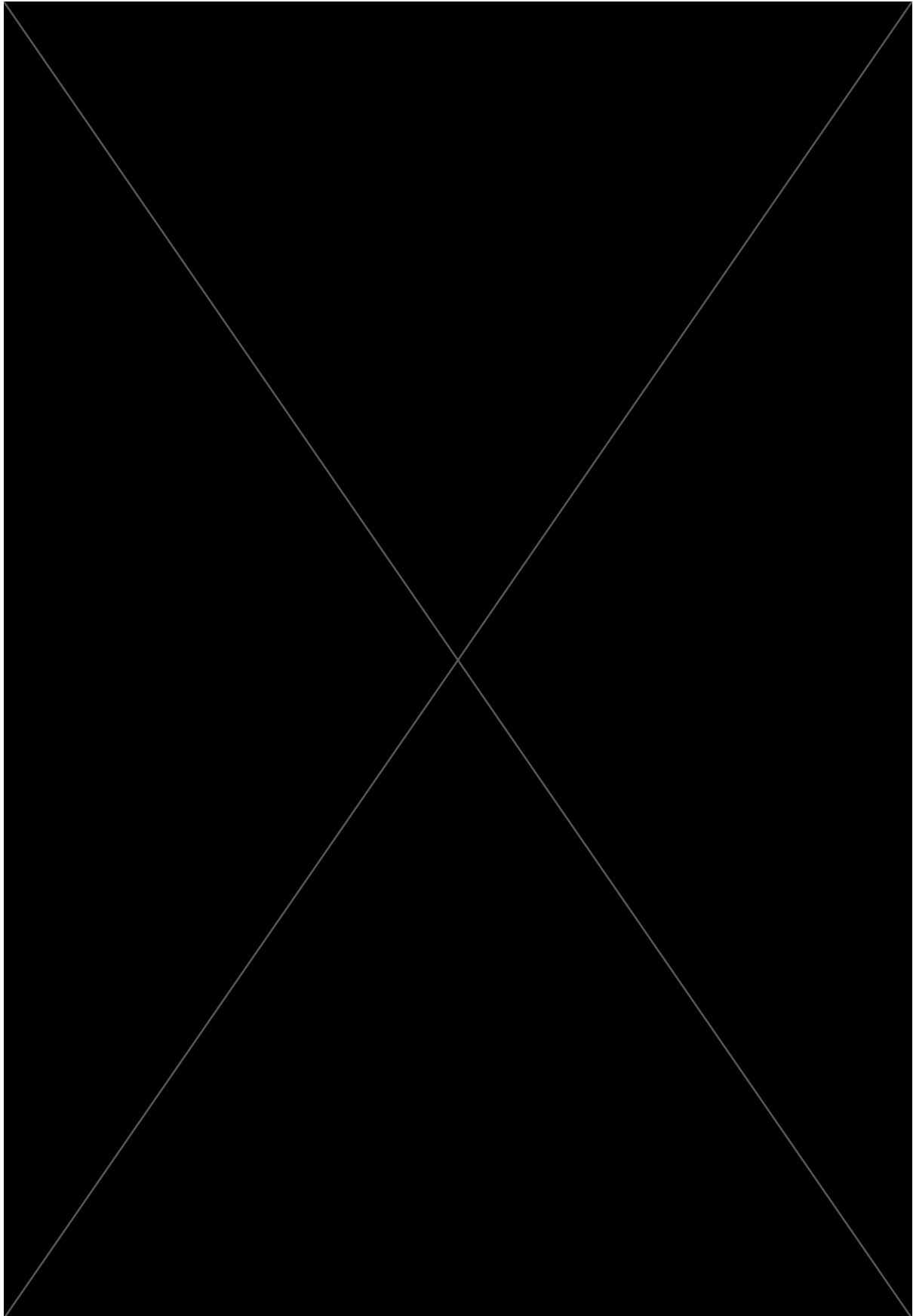


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



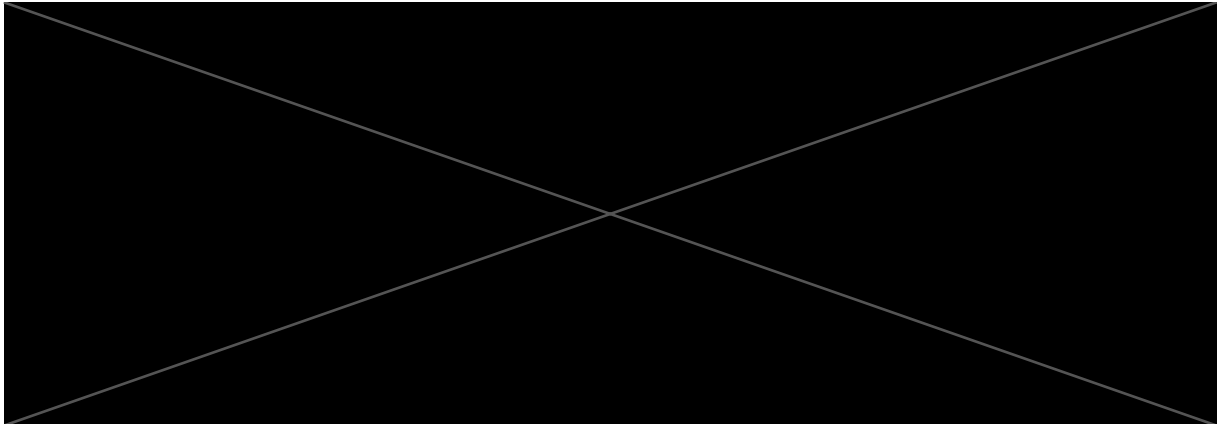


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

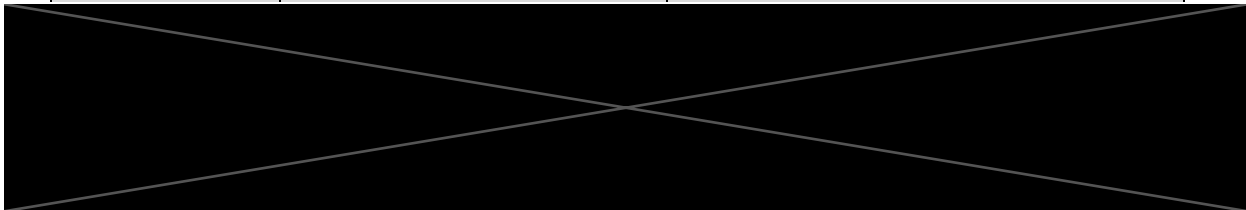


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Análisis de Riesgo

INSTITUTO DE ASTRONOMÍA	
Identificador único	SIP
Nombre del sistema	Sistema Integral de Personal

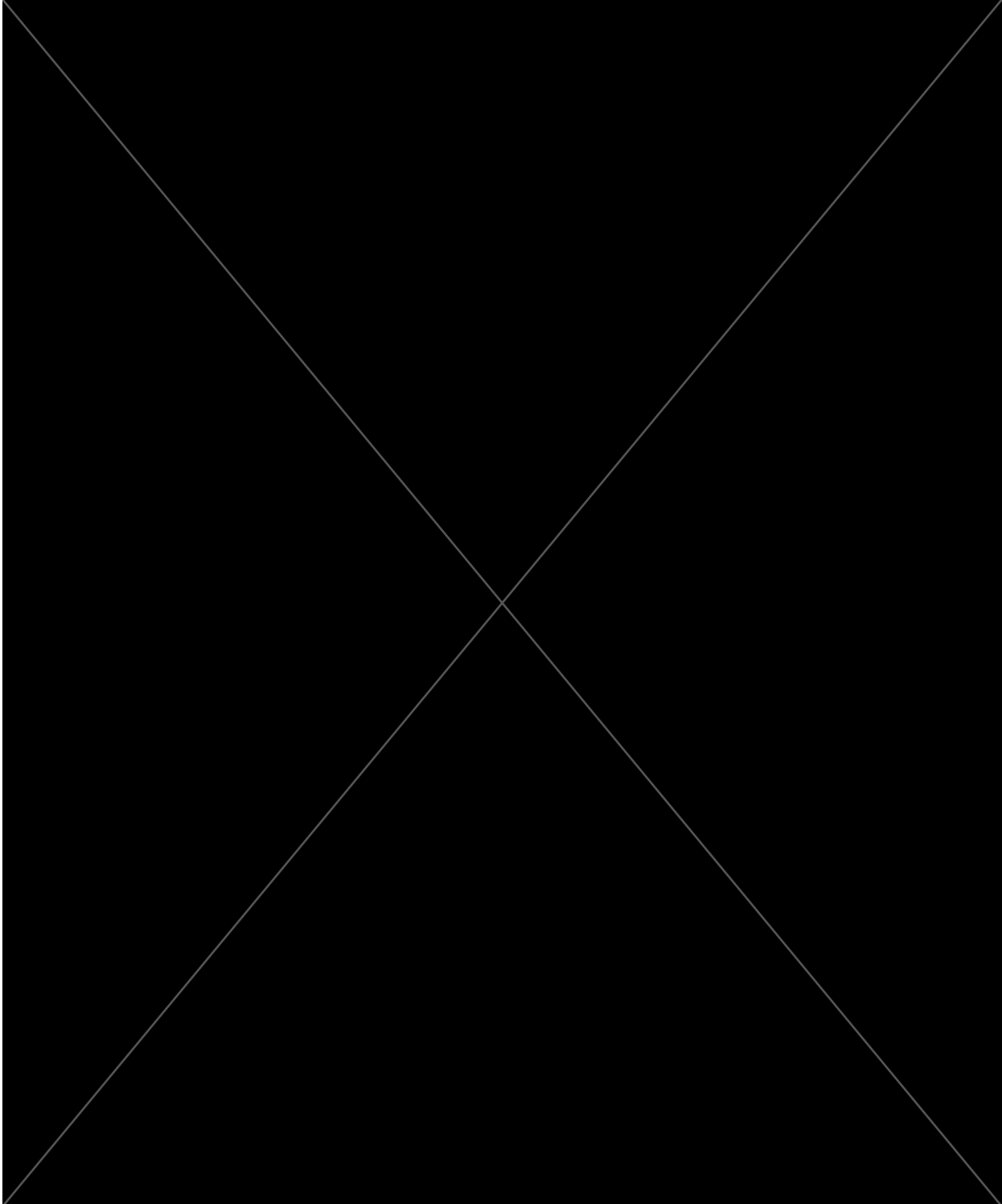


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



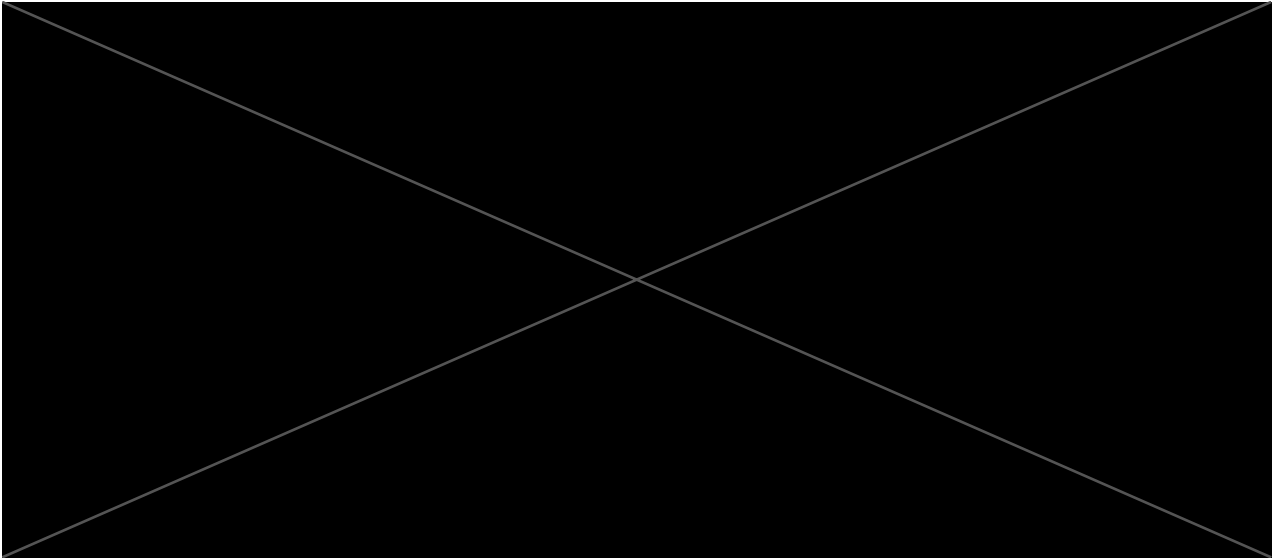
Análisis de Riesgo

INSTITUTO DE ASTRONOMÍA	
Identificador único	Videovigilancia
Nombre del sistema	Videovigilancia





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución

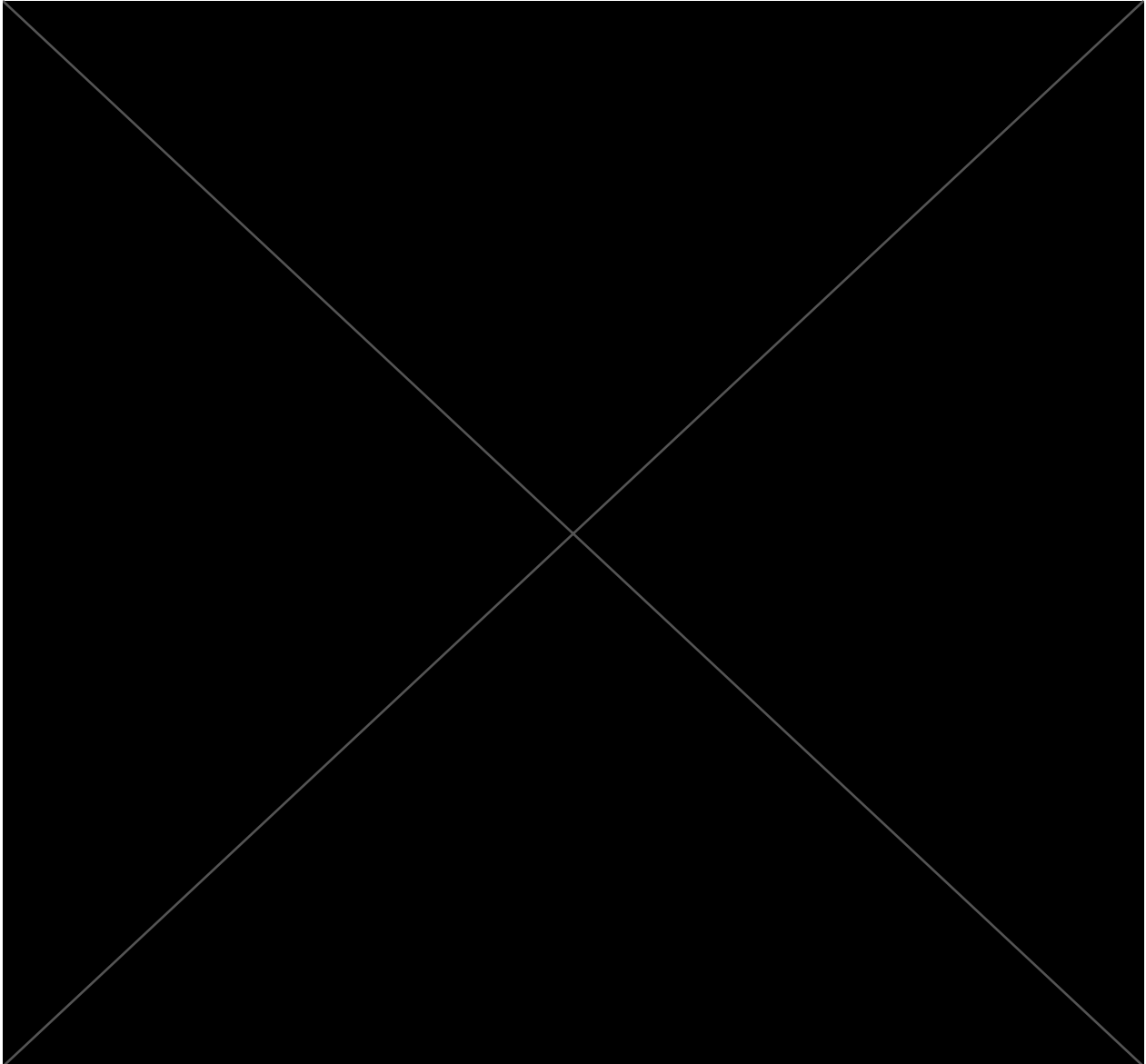


5.4 Anexo 4 Análisis de Brecha



Análisis de Brecha

INSTITUTO DE ASTRONOMÍA	
Identificador único	D1012a
Nombre del sistema	Sistema de Informes y Planes de Trabajo Anuales

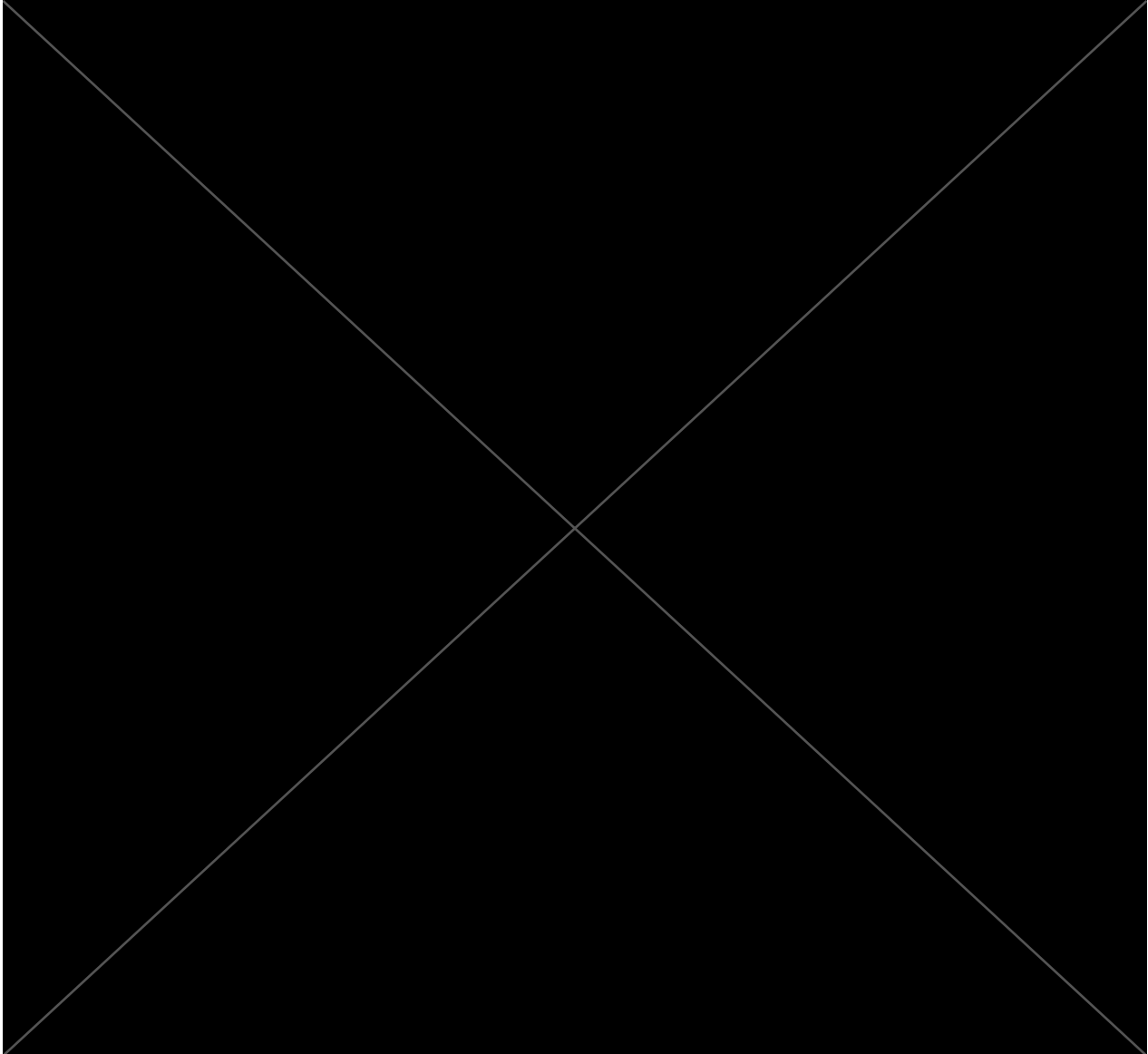


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Análisis de Brecha

INSTITUTO DE ASTRONOMÍA	
Identificador único	D1012b
Nombre del sistema	Sistema de la COSE

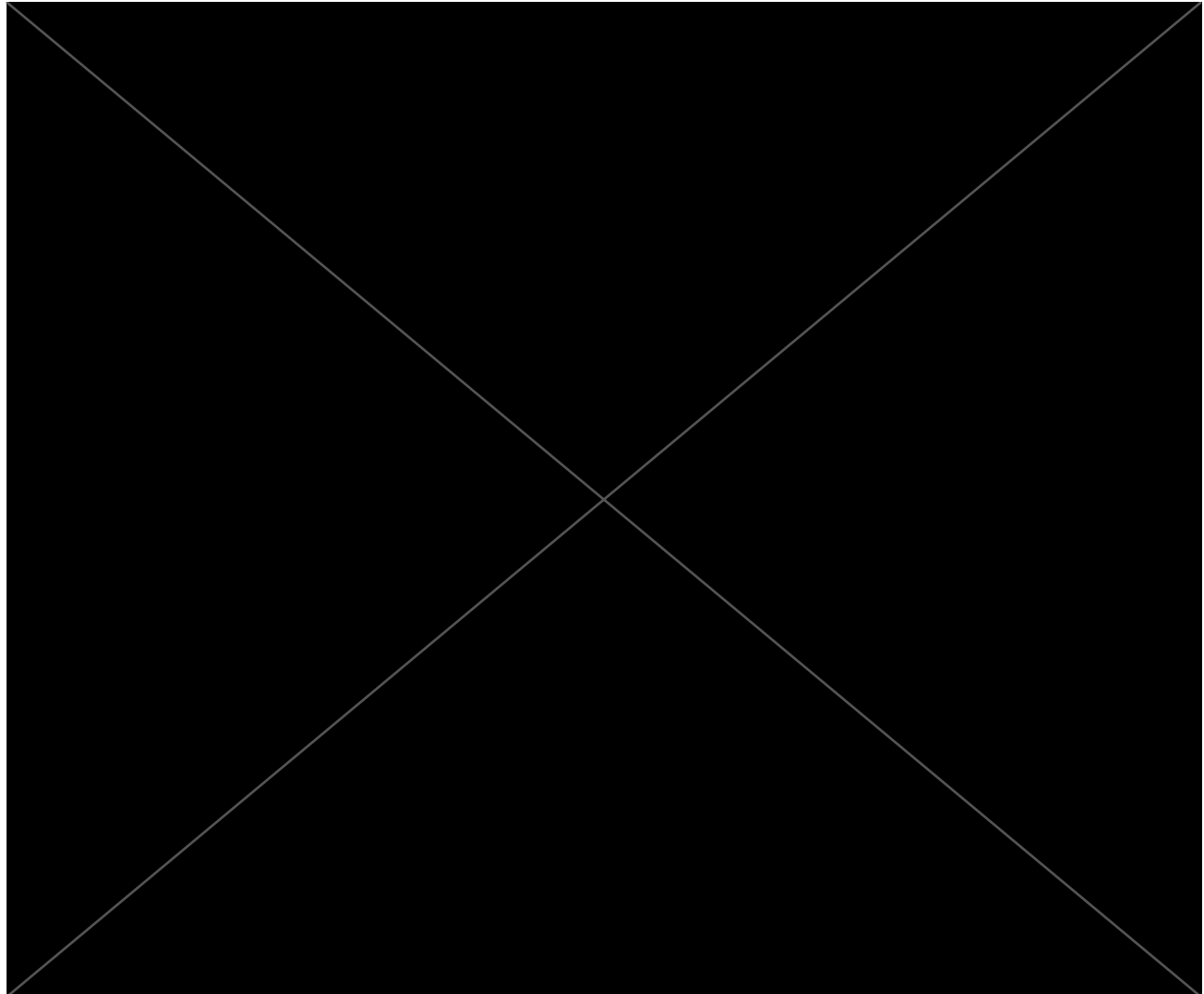


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Análisis de Brecha

INSTITUTO DE ASTRONOMÍA	
Identificador único	Regsol.3.70a
Nombre del sistema	Registro de Solicitudes en Línea

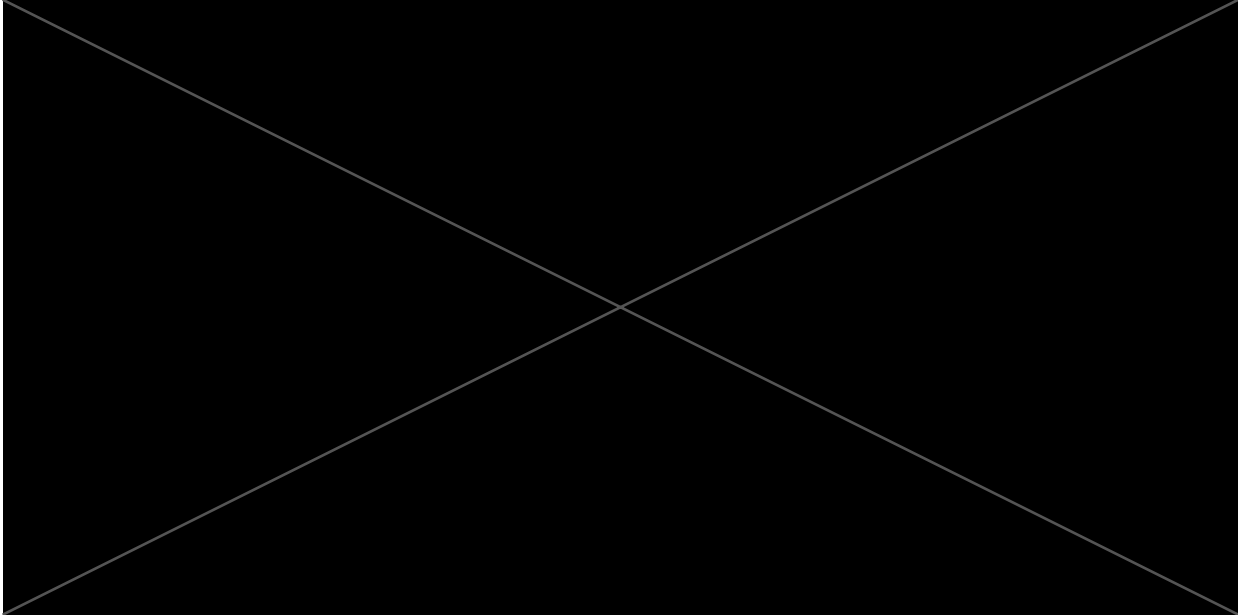


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Análisis de Brecha

INSTITUTO DE ASTRONOMÍA	
Identificador único	SIP
Nombre del sistema	SIP

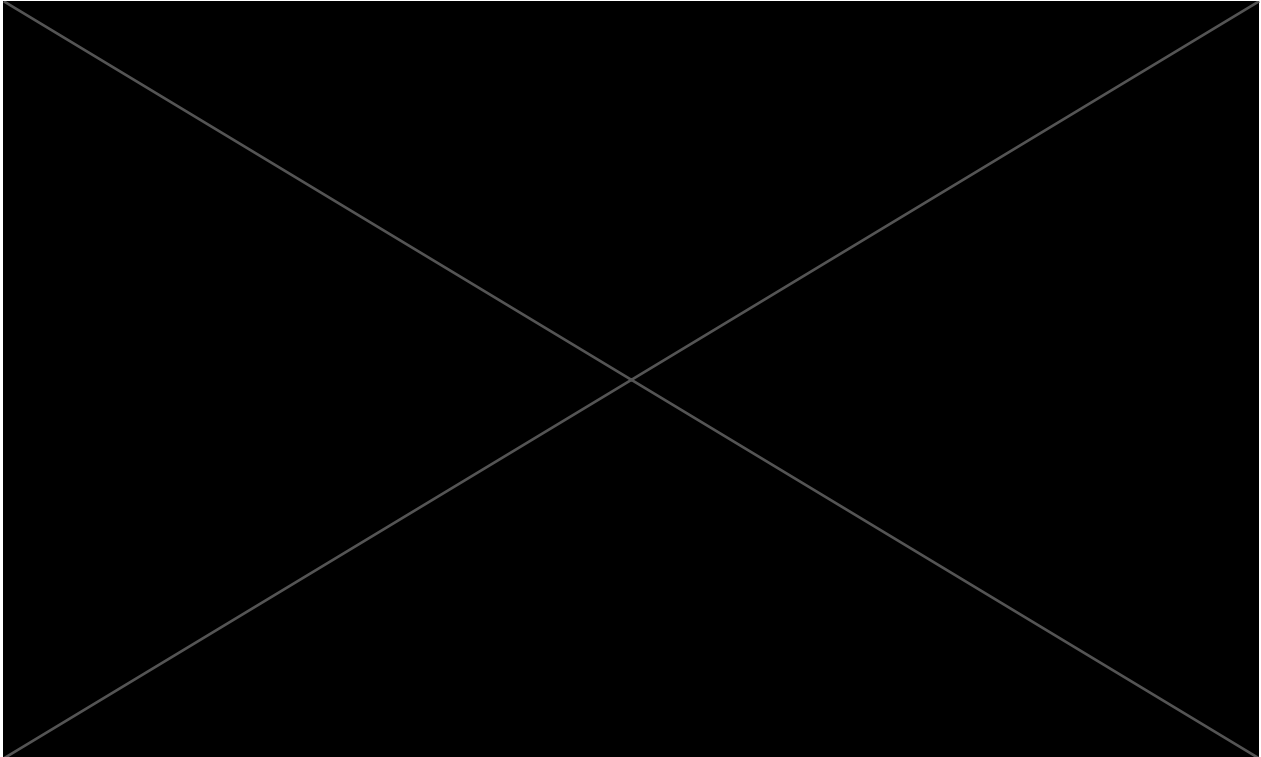


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Análisis de Brecha

INSTITUTO DE ASTRONOMÍA	
Identificador único	Videovigilancia
Nombre del sistema	Videovigilancia



Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución

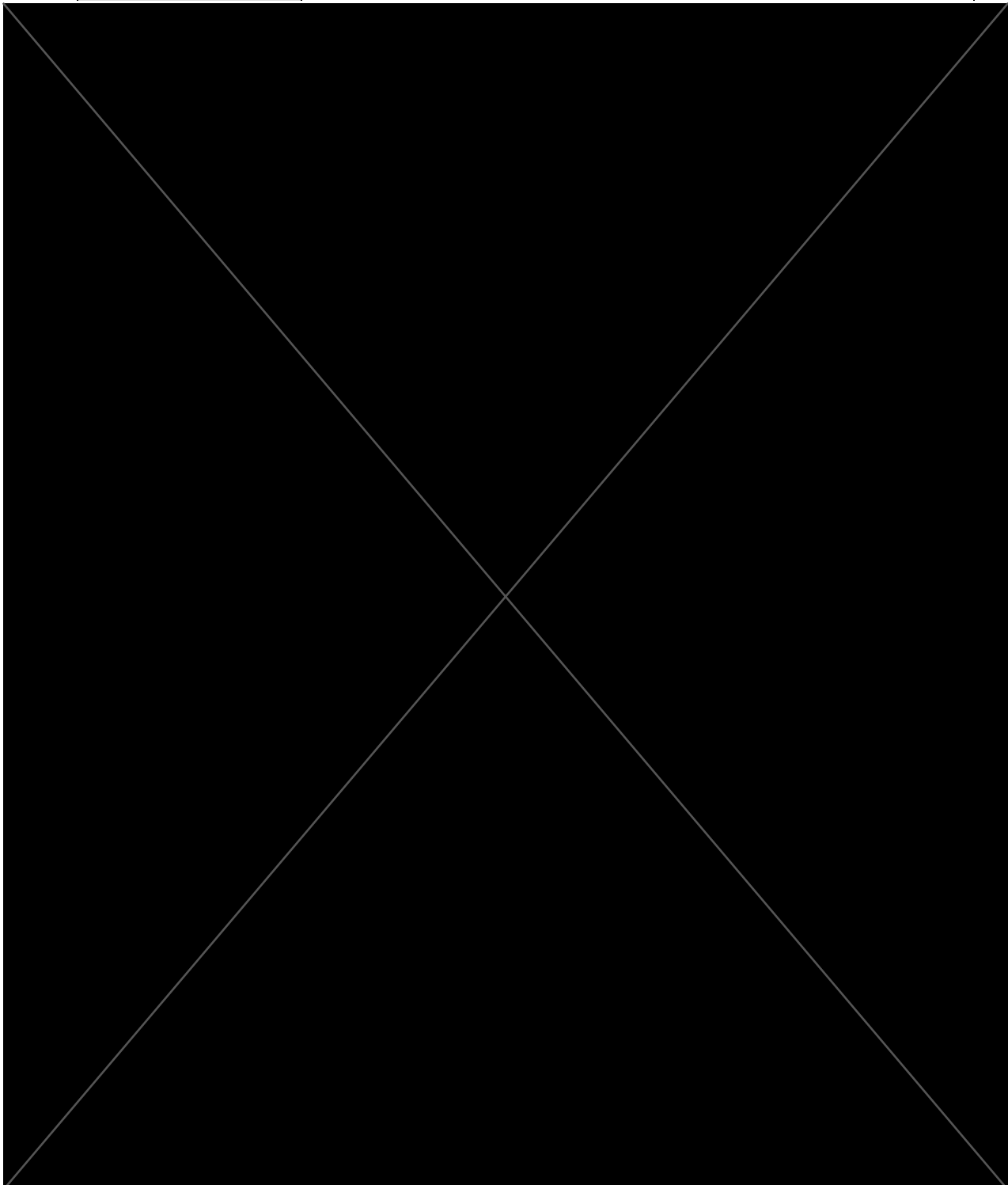


5.5 Anexo 5 Plan de Trabajo



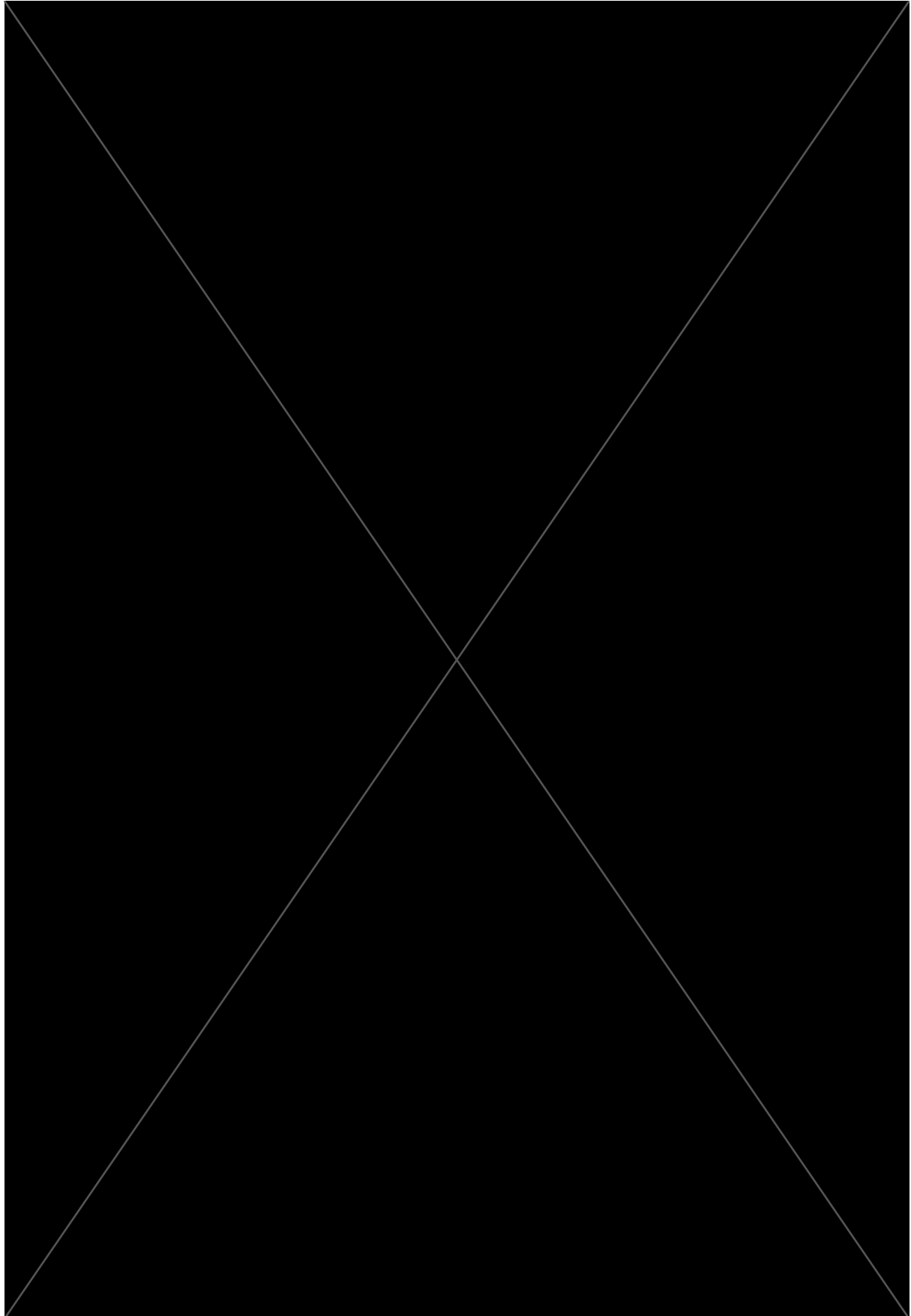
Plan de Trabajo

INSTITUTO DE ASTRONOMÍA	
Identificador único	D1012a
Nombre del sistema	Sistema de Informes y Planes de Trabajo Anuales



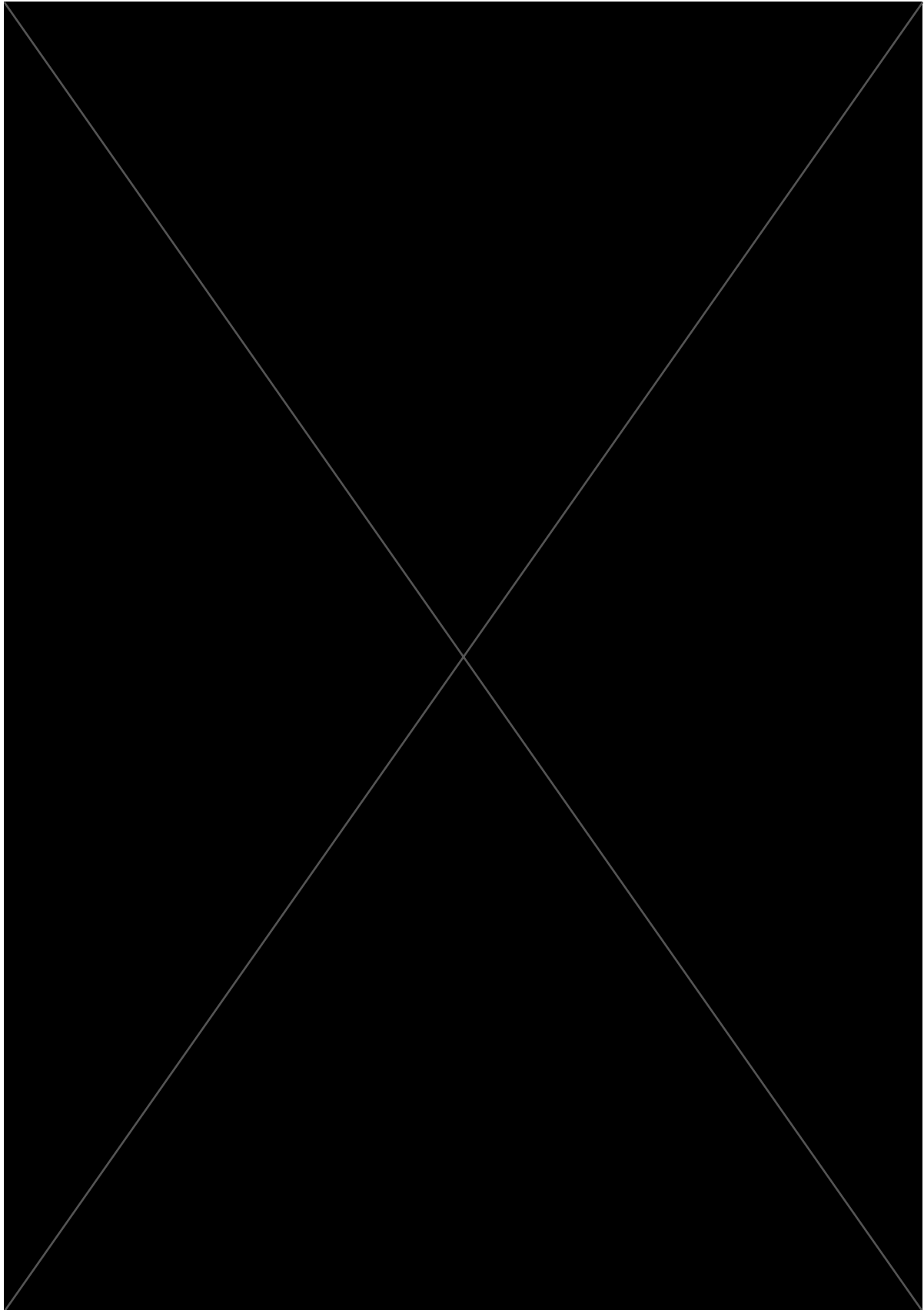


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



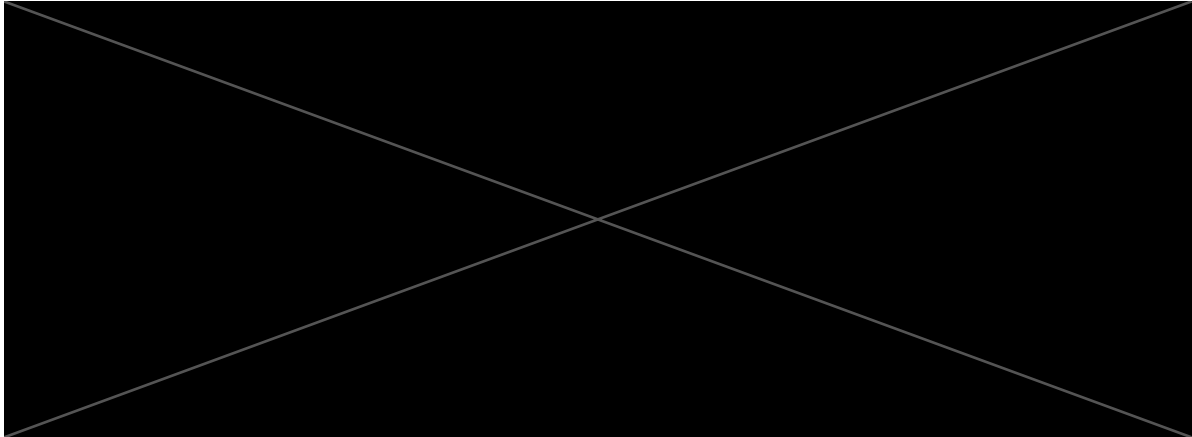


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

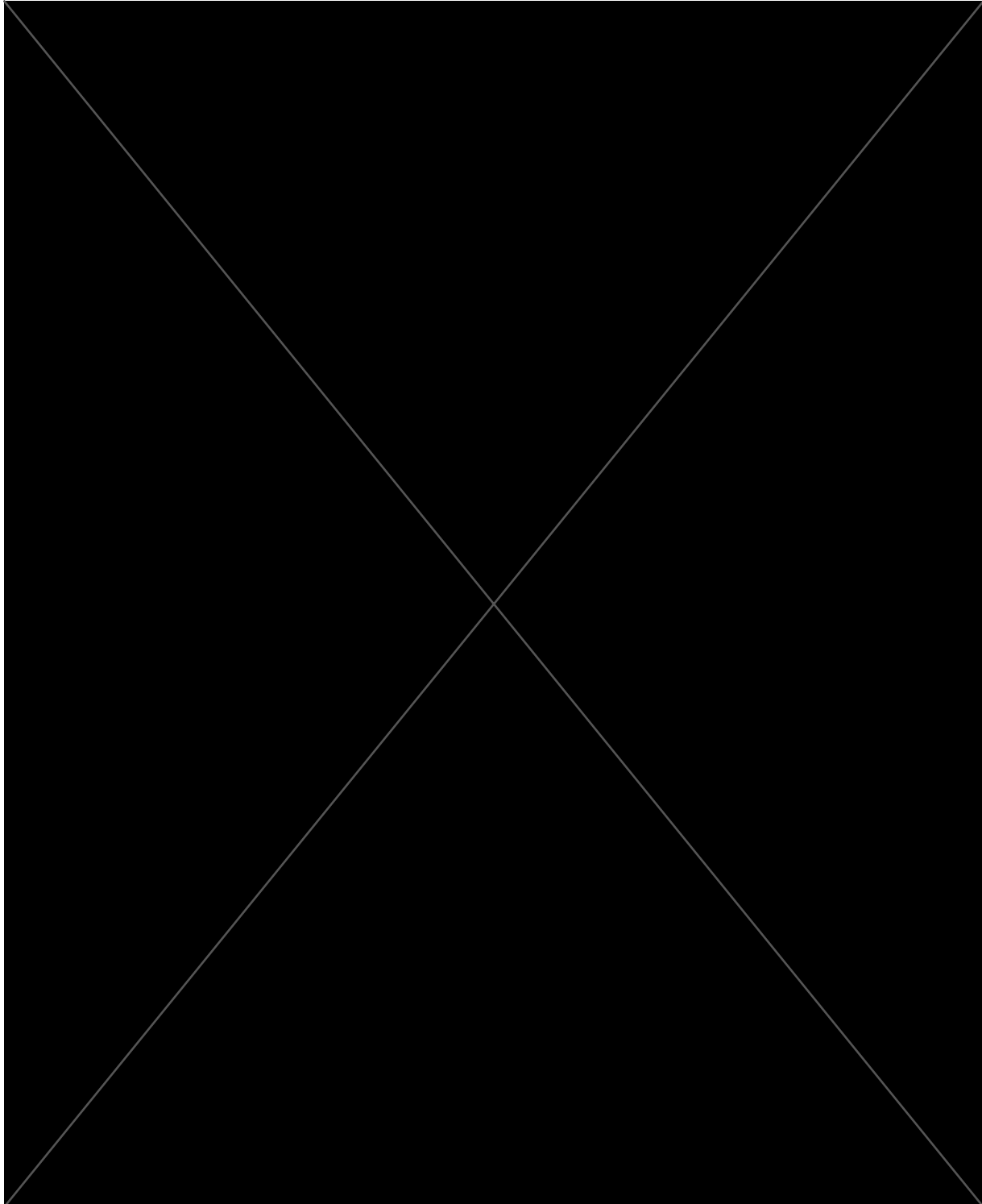


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



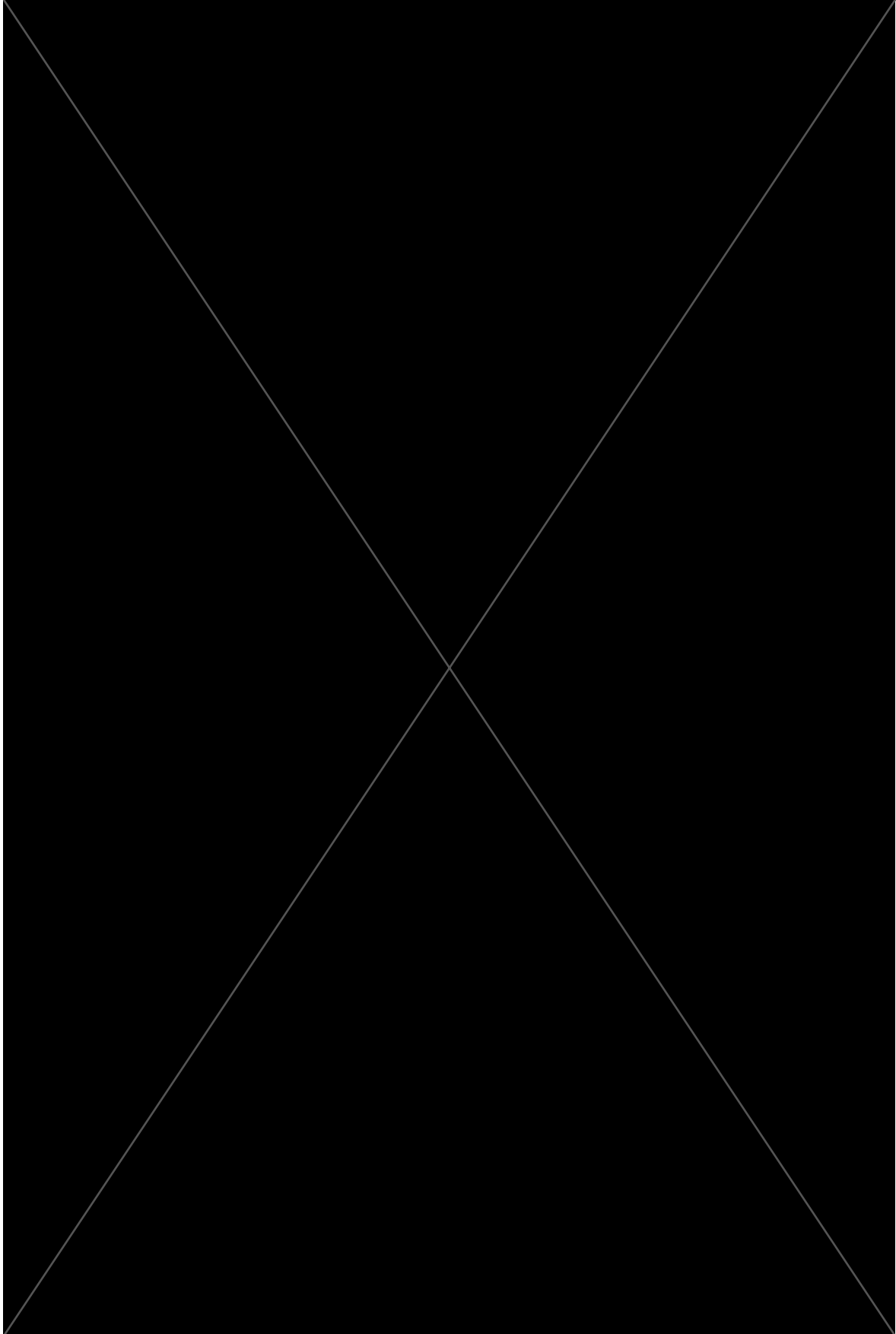
Plan de Trabajo

INSTITUTO DE ASTRONOMÍA	
Identificador único	D1012b
Nombre del sistema	Sistema de la COSE



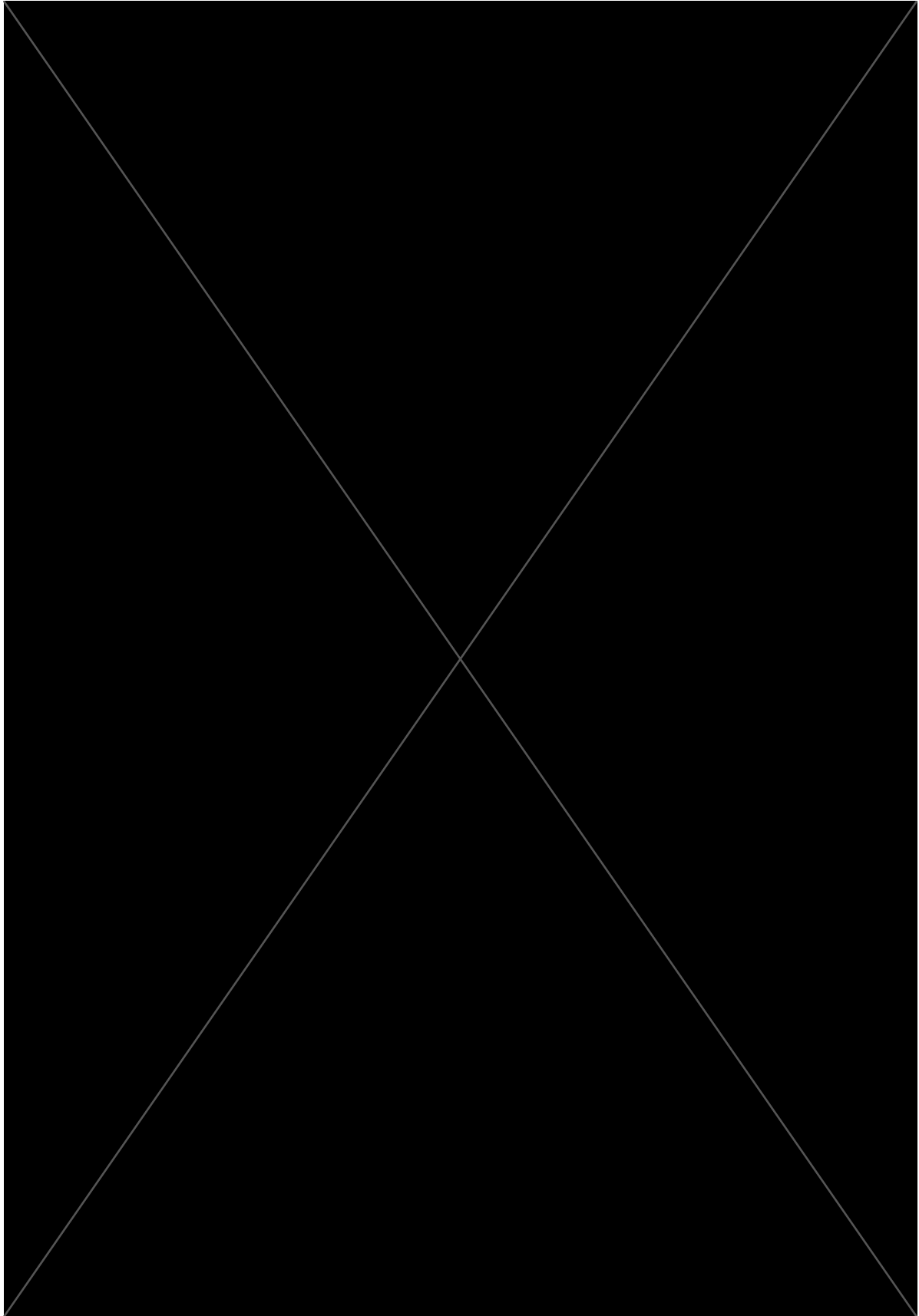


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**



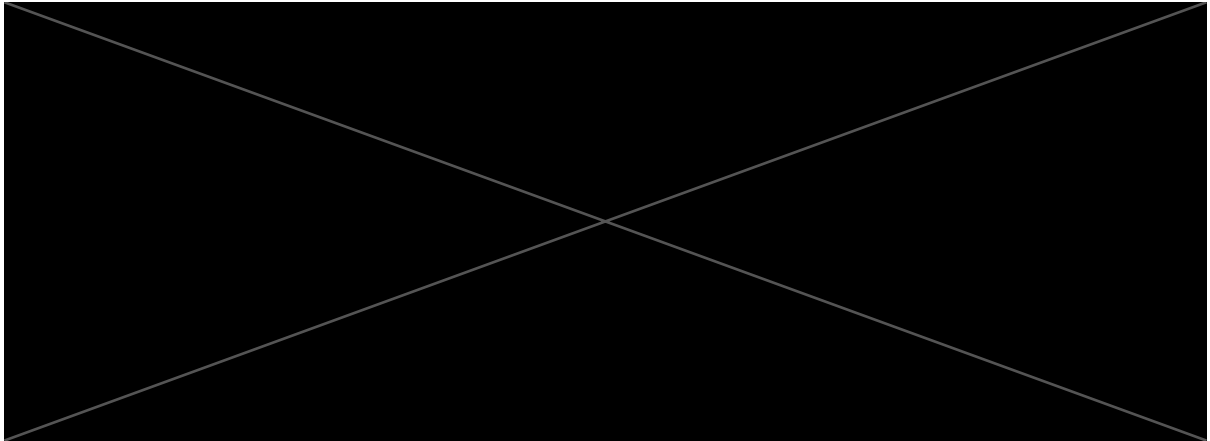


**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

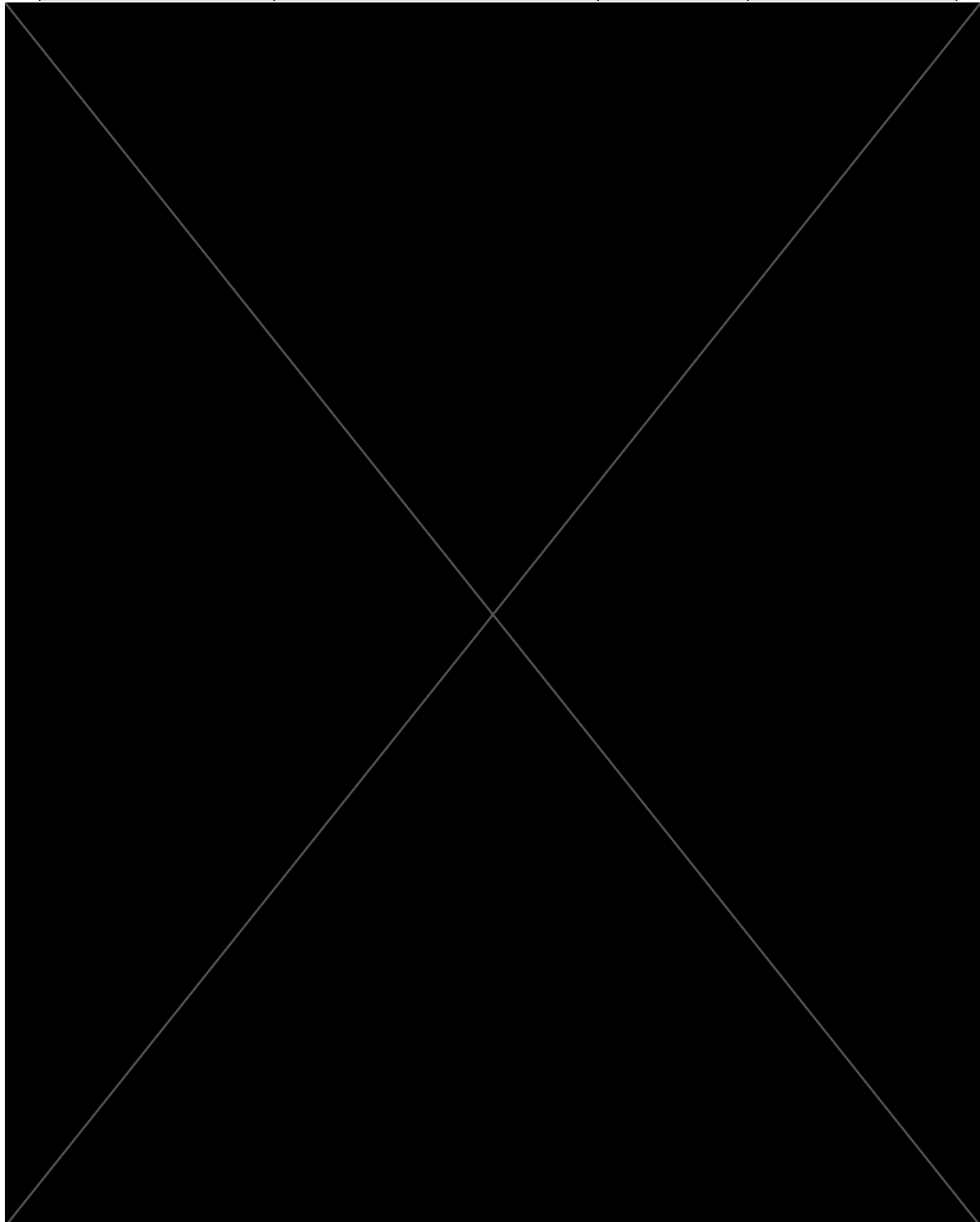


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



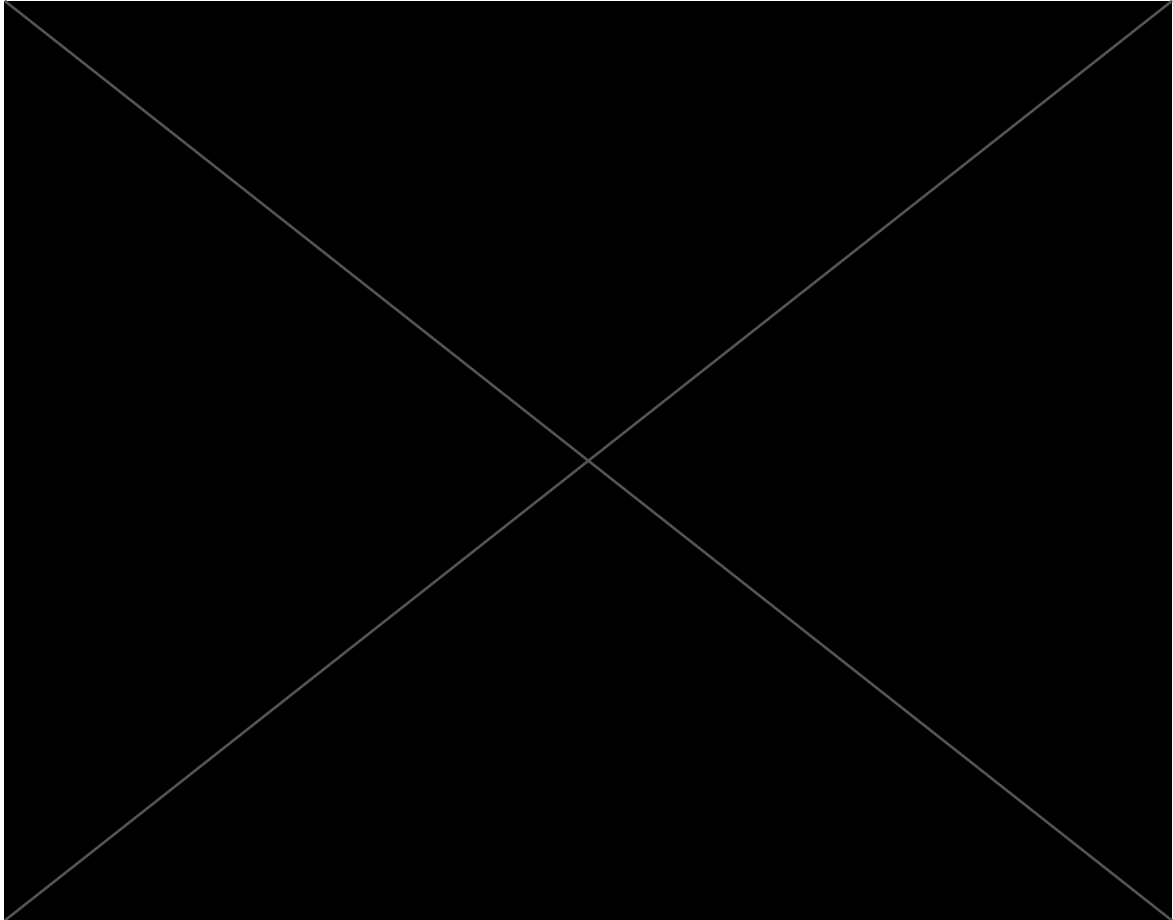
Plan de Trabajo

INSTITUTO DE ASTRONOMÍA	
Identificador único	Regsol.3.70
Nombre del sistema	REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)





**Instituto de Astronomía.
Sistema de Gestión de Datos Personales
Documento de Seguridad**

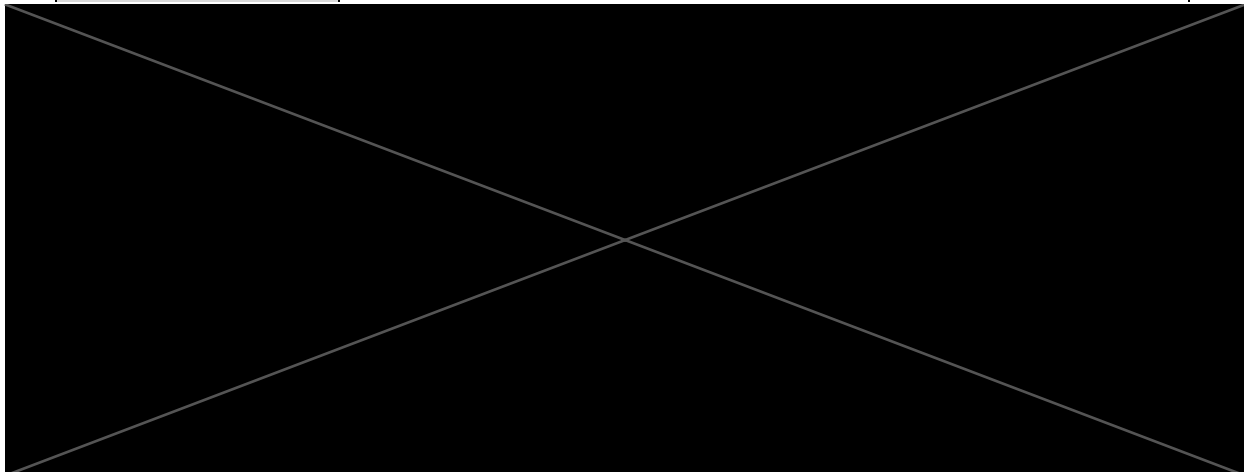


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Plan de Trabajo

INSTITUTO DE ASTRONOMÍA	
Identificador único	SIP
Nombre del sistema	SIP

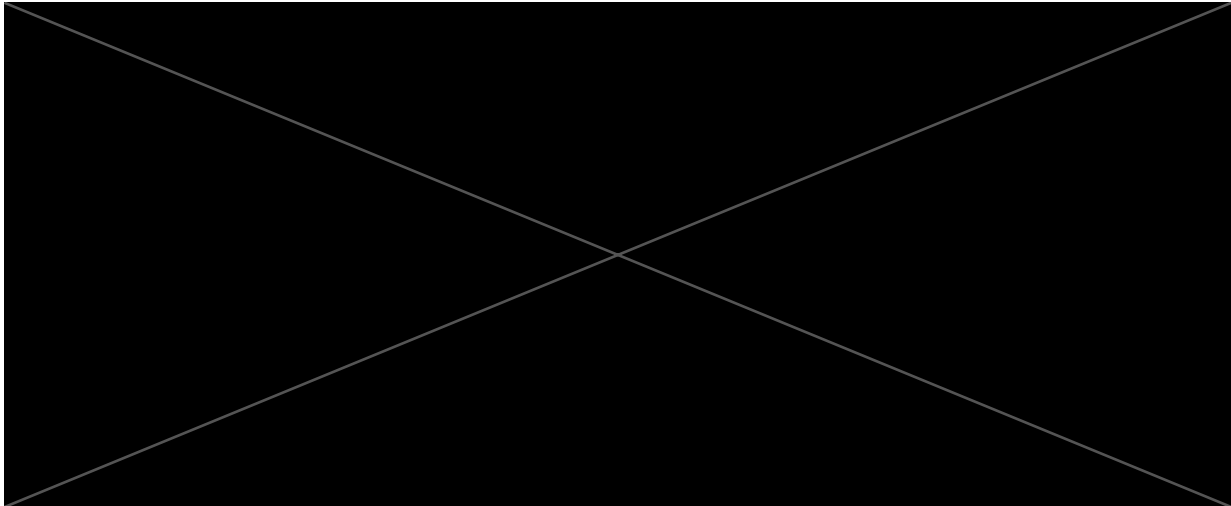


Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución



Plan de Trabajo



INSTITUTO DE ASTRONOMÍA	
Identificador único	Videovigilancia
Nombre del sistema	Videovigilancia






Se protege por tratarse de información reservada conforme a los artículos 113, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública y 110, fracción VII de la Ley Federal de Transparencia y Acceso a la Información Pública, y a lo aprobado por el Comité de Transparencia en la resolución




5.6 Anexo 6 Formatos para el cumplimiento de las MST

Sistema de la COSE		D1012b		
Formato	1	Verificación anual	Acción concluida	(SI)
Medida de seguridad técnica:	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información, por medio de formato o comandos.</p> <p>C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables.</p> <p>D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B.</p> <p>E) Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios.</p> <p>2.- Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha revisión
Programador, desarrollador o diseñador del sistema de información				09 agosto 2022
Observaciones / anotaciones	No se utilizan datos personales durante el desarrollo y pruebas del sistema			



Sistema de la COSE		D1012b		
Formato:	2	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.</p> <p>C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.</p> <p>D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.</p> <p>E) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Definir niveles de acceso adecuados para cada perfil o tipo de usuario.</p> <p>2.- Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
				
Francisco Ruiz Sala Administrador del sistema de información		Fecha revisión 09 de agosto de 2022		
Observaciones / anotaciones	Los privilegios de acceso al sistema son correctos para los usuarios			



Sistema de la COSE		D1012b		
Formato:	3	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.			
Proceso recomendado:	<p>A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación.</p> <p>B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo).</p> <p>C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx.</p> <p>D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.</p>			
Mejores prácticas, referencias:	<p>1.- Los certificados SSL deben tener una vigencia de al menos un año.</p> <p>2.- En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (<i>wildcard</i>).</p> <p>3.- Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.</p>			
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones	Se cuenta con un certificado SSL para el dominio @astro.unam.mx			

Sistema de la COSE		D1012b		
Formato:	4	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.			
Proceso recomendado:	<p>A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:</p> <ul style="list-style-type: none"> - Diario – incremental. - Semanal – incremental. - Mensual – total. <p>B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:</p> <ul style="list-style-type: none"> - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. <p>C) Incluir en el plan:</p> <ul style="list-style-type: none"> - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. - RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.			
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.			
Ejecución				
				
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022		
Observaciones / anotaciones				

Acciones realizadas:


- Se instalo y configuró un programa que realiza la copia de la información de manera automática en un directorio especializado para tal fin.
- Se configuro el respaldo diario de la base de datos y el directorio en donde se encuentra el sistema en un disco duro, con lo cual se tiene un respaldo diario durante un año.
- Cada 6 meses se realiza una copia de todos los directorios existentes en otro equipo y se realiza la copia en DVD o Blu-ray, los cuales se encuentran en una oficina con acceso restringido y bajo una gaveta con llave.
- El acceso a los respaldos es restringido a personal del departamento de cómputo de la sede de Ciudad Universitaria


Sistema de la COSE		D1012b		
Formato:	5	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.			
Proceso recomendado:	<p>A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.</p> <p>B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.</p> <p>C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.</p> <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<p>1.- Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf</p> <p>2.- Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar <i>DOD-5220.22-M</i>.</p>			
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones				



Sistema de la COSE		D1012b		
Formato:	6	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.			
Proceso recomendado:	<p>A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.</p> <p>B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <i>Por ejemplo</i>, en el caso del sistema operativo Linux:</p> <ul style="list-style-type: none"> - Verificar la existencia del archivo <code>/etc/ntp.conf</code> - Editar el archivo <code>ntp.conf</code> incluyendo en la primera línea: <code>server ntpdgtic.redunam.unam.mx ó</code> <code>server 132.247.169.17</code> - Reiniciar el demonio del cliente NTP con el comando <code>sudo service ntp reload</code>. <p>C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<p>1.- Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM.</p> <p>2.- No se deben usar otros servidores de NTP distintos al de UNAM.</p>			
Conocimientos requeridos:	Administración de sistema operativo.			
Ejecución			Fecha inicio	
				
Liliana Hernández Cervantes			Francisco Ruiz Sala	
Administrador del sistema de información o servidor			Fecha término	
Observaciones / anotaciones				


Acciones realizadas:



Activación y configuración del NTP en el sistema operativo.
Configuración del servidor de tiempo dirigido a *132.247.169.17*



Sistema de la COSE		D1012b	
Formato:	7	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de <i>malware</i> (<i>rootkits</i> , <i>backdoors</i> o códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:	<p>A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. <i>Por ejemplo</i>, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.</p> <p>B) Disponer de comandos para la localización de amenazas. <i>Por ejemplo</i>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>.</p> <p>C) Una vez instalada la solución, verificar periódicamente su actualización</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- UNAM-CERT puede asesorar en la selección de las herramientas <i>anti malware</i> más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones	Se instalo y configuro la herramienta chkrootkit en el equipo y se ejecutan las actualizaciones en el equipo		



Sistema de la COSE		D1012b	
Formato:	8	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:	<p>A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <i>Por ejemplo</i>, en el sistema operativo Linux ejecutar <i>apt-get update</i> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> de la respectiva distribución.</p> <p>B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.</p> <p>C) Instalar las actualizaciones en el sistema operativo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala		Fecha de revisión	
Administrador del sistema de información o servidor		9 de agosto de 2022	
Observaciones / anotaciones			


Sistema de la COSE		D1012b	
Formato:	9	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:	<p>A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema.</p> <p>B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. <i>Por ejemplo:</i> el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (<i>Active Directory</i>), <i>LDAP</i> u <i>OpenAIM</i>.</p> <p>2.- Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.</p>		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones			


Sistema de la COSE		D1012b	
Formato:	10	Verificación anual	Acción concluida (SI)
Medida de seguridad técnica:	Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:	<p>A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. <i>Por ejemplo:</i> en sistemas Linux desactivar la instalación de versiones <i>beta, test, debug, non-official</i>.</p> <p>B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. <i>Por ejemplo:</i> En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo.</p> <p>C) Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> no debe estar instalado.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE			D1012b	
Formato:	11	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	<p>A) Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos.</p> <p>B) En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.</p> <p>C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. <i>Por ejemplo</i>; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				9 de agosto de 2022
Observaciones / anotaciones				


Sistema de la COSE			D1012b	
Formato:	12	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	<p>A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades <i>flash</i>, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo.</p> <p>B) La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área.</p> <p>C) Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo.</p> <p>2.- En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.</p>			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			
Ejecución				
				
Liliana Hernández Cervantes			Fecha de revisión	
Administrador del sistema de información o servidor			09 de agosto de 2022	
Observaciones / anotaciones	Los equipos asociados al sistema no salen del Instituto			


Sistema de la COSE		D1012b	
Formato:	13	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:	<p>A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo: SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy).</i></p> <p>B) Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. <i>Por ejemplo, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando <code>apt-get install openssh-server</code>.</i></p> <p>C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo: en Linux con el comando <code>sudo systemctl enable ssh</code>.</i></p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad.</p> <p>2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			
			
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión	
Administrador del sistema de información o servidor		9 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE		D1012b	
Formato:	14	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.		
Aplicable en:	Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:	<p>A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> máquina virtual directorio temporal en el servidor.</p> <p>B) Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando.</p> <p>C) Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.</p> <p>D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. <i>Por ejemplo:</i> en Linux se dispone de <i>shred, wipe, secure-delete, srm, sfill, sswap, sdmem</i>, que se pueden instalar desde el administrador de aplicaciones.</p> <p>E) Llenar y firmar este formato.</p>		
Mejores prácticas, referencias:	1.- Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			


Sistema de la COSE		D1012b	
Formato:	15	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	<p>A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.</p> <p>B) Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.</p> <p>C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.</p> <p>D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo:</i> Webservices, transferencia SFTP.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
			
Liliana Hernández Cervantes Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto 2022	
Observaciones / anotaciones	No aplica la transferencia ni referencia de los datos a otras instancias		

Sistema de la COSE		D1012b		
Formato:	16	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	<p>A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles.</p> <p>B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).</p> <p>C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo</p> <p>D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo.</p> <p>E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales.</p> <p>F) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor		9 de agosto de 2022		
Observaciones / anotaciones				

Sistema de la COSE		D1012b	
Formato:	17	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:	<p>A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia).</p> <p>B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo.</p> <p>C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Liliana Hernández Cervantes		Revisión	
Administrador del sistema de información o servidor		9 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE		D1012b	
Formato:	18	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnica:	Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:	<p>A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos.</p> <p>B) Designar responsables de respaldos y responsables de verificación de respaldos.</p> <p>C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE		D1012b		
Formato:	19	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.			
Proceso recomendado:	<p>A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema.</p> <p>B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.</p> <p>C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Nombre y firma Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones				



Sistema de la COSE		D1012b	
Formato:	20	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:	<p>A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <i>Por ejemplo:</i> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo.</p> <p>B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <i>Por ejemplo:</i> diario, semanal, mensual.</p> <p>C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <i>Por ejemplo:</i> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			


Acciones realizadas:



Se comenzó a llevar el inventario de las bitácoras, las cuales se respaldan diariamente en el mismo esquema que la base de datos y el sistema



Sistema de la COSE		D1012b	
Formato:	21	Verificación anual	Acción concluida (SI)
Norma Complementaria Técnica	Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:	<p>A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.</p> <p>B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red.</p> <p>C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable.</p> <p>D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento.</p> <p>E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:	Administración de redes de datos.		
Ejecución			
			
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE		D1012b	
Formato:	22	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:	<p>A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <i>Por ejemplo</i>: para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales.</p> <p>B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <i>Por ejemplo</i>, en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo.</p> <p>C) Dejar activos solamente los puertos necesarios para la operación del sistema.</p> <p>D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <i>Por ejemplo</i>: Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión	
Administrador del sistema de información o servidor		09 de agosto de 2022	
Observaciones / anotaciones			

Sistema de la COSE		D1012b		
Formato:	23	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de estos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	<p>A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión.</p> <p>B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.</p> <p>C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar - equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución				
				
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión		
Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones				

Sistema de la COSE		D1012b	
Formato:	24	Verificación anual	Acción concluida (NO)
Medidas de seguridad técnicas:	Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:	<p>A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx .</p> <p>B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A.</p> <p>C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			
			
Francisco Ruiz Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de la COSE		D1012b		
Formato:	25	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.			
Proceso recomendado:	<p>A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información.</p> <p>B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática.</p> <p>C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico.</p> <p>D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico.</p> <p>E) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- El mantenimiento preventivo debe contar con medidas de verificación.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones				



Sistema de la COSE		D1012b		
Formato:	26	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. III. b) Definir el programa de mantenimiento preventivo.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.</p> <p>B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.</p> <p>C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
				
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión		
Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones				


Sistema de la COSE		D1012b		
Formato:	27	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.</p> <p>B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo.</p> <p>C) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones				



Acciones realizadas:


El Departamento de Cómputo tiene personal especializado que realiza el mantenimiento preventivo del equipo cada 6 meses o cuando la situación lo requiera por urgencia.

Sistema de la COSE		D1012b		
Formato:	28	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.			
Aplicable en:	Servicios en la nube pública.			
Tiempo estimado:	Hito.			
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el resguardo de archivos cifrados, no en producción.			
Proceso recomendado:	<p>A) Identificar los respaldos que se tengan resguardados en servicios de nube pública.</p> <p>B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.</p>			
Mejores prácticas, referencias:	1.- La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.			
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.			
Ejecución				
				
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión		
Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones	Es sistema se respalda y se tiene activo únicamente dentro de la dependencia y no se usan servicios en la Nube			

Sistema de Informes Anuales		D1012a		
Formato	1	Verificación anual	Acción concluida	(SI)
Medida de seguridad técnica:	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información, por medio de formato o comandos.</p> <p>C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables.</p> <p>D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B.</p> <p>E) Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios.</p> <p>2.- Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha revisión
Programador, desarrollador o diseñador del sistema de información				09 agosto 2022
Observaciones / anotaciones	No se utilizan datos personales durante el desarrollo y pruebas del sistema			



Sistema de Informes Anuales		D1012a		
Formato:	2	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.</p> <p>C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.</p> <p>D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.</p> <p>E) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Definir niveles de acceso adecuados para cada perfil o tipo de usuario.</p> <p>2.- Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
				
Francisco Ruiz Sala		Fecha revisión		
Administrador del sistema de información		09 de agosto de 2022		
Observaciones / anotaciones	Los privilegios de acceso al sistema son correctos para los usuarios			



Sistema de Informes Anuales		D1012a	
Formato:	3	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:	<p>A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación.</p> <p>B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo).</p> <p>C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx.</p> <p>D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.</p>		
Mejores prácticas, referencias:	<p>1.- Los certificados SSL deben tener una vigencia de al menos un año.</p> <p>2.- En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (<i>wildcard</i>).</p> <p>3.- Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones	Se cuenta con un certificado SSL para el dominio @astro.unam.mx		

Sistema de Informes Anuales		D1012a	
Formato:	4	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:	<p>A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:</p> <ul style="list-style-type: none"> - Diario – incremental. - Semanal – incremental. - Mensual – total. <p>B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:</p> <ul style="list-style-type: none"> - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. <p>C) Incluir en el plan:</p> <ul style="list-style-type: none"> - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. - RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			

Acciones realizadas:


- Se instalo y configuró un programa que realiza la copia de la información de manera automática en un directorio especializado para tal fin.
- Se configuro el respaldo diario de la base de datos y el directorio en donde se encuentra el sistema en un disco duro, con lo cual se tiene un respaldo diario durante un año.
- Cada 6 meses se realiza una copia de todos los directorios existentes en otro equipo y se realiza la copia en DVD o Blu-ray, los cuales se encuentran en una oficina con acceso restringido y bajo una gaveta con llave.
- El acceso a los respaldos es restringido a personal del departamento de cómputo de la sede de Ciudad Universitaria


Sistema de Informes Anuales		D1012a	
Formato:	5	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:	<p>A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.</p> <p>B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.</p> <p>C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.</p> <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf</p> <p>2.- Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar <i>DOD-5220.22-M</i>.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales		D1012a	
Formato:	6	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:	<p>A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.</p> <p>B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <i>Por ejemplo</i>, en el caso del sistema operativo Linux:</p> <ul style="list-style-type: none"> - Verificar la existencia del archivo <code>/etc/ntp.conf</code> - Editar el archivo <code>ntp.conf</code> incluyendo en la primera línea: <code>server ntpdgtic.redunam.unam.mx ó</code> <code>server 132.247.169.17</code> - Reiniciar el demonio del cliente NTP con el comando <code>sudo service ntp reload</code>. <p>C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM.</p> <p>2.- No se deben usar otros servidores de NTP distintos al de UNAM.</p>		
Conocimientos requeridos:	Administración de sistema operativo.		
Ejecución		Fecha inicio	
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha término	
Observaciones / anotaciones			


Acciones realizadas:



Activación y configuración del NTP en el sistema operativo.
Configuración del servidor de tiempo dirigido a *132.247.169.17*



Sistema de Informes Anuales		D1012a	
Formato:	7	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de <i>malware</i> (<i>rootkits</i> , <i>backdoors</i> o códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:	<p>A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. <i>Por ejemplo</i>, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.</p> <p>B) Disponer de comandos para la localización de amenazas. <i>Por ejemplo</i>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>.</p> <p>C) Una vez instalada la solución, verificar periódicamente su actualización</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- UNAM-CERT puede asesorar en la selección de las herramientas <i>anti malware</i> más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones	Se instalo y configuro la herramienta chkrootkit en el equipo y se ejecutan las actualizaciones en el equipo		



Sistema de Informes Anuales		D1012a	
Formato:	8	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:	<p>A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <i>Por ejemplo</i>, en el sistema operativo Linux ejecutar <code>apt-get update</code> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> de la respectiva distribución.</p> <p>B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.</p> <p>C) Instalar las actualizaciones en el sistema operativo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala		Fecha de revisión	
Administrador del sistema de información o servidor		9 de agosto de 2022	
Observaciones / anotaciones			


Sistema de Informes Anuales		D1012a	
Formato:	9	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:	<p>A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema.</p> <p>B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. <i>Por ejemplo:</i> el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (<i>Active Directory</i>), <i>LDAP</i> u <i>OpenAIM</i>.</p> <p>2.- Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.</p>		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones			


Sistema de Informes Anuales		D1012a	
Formato:	10	Verificación anual	Acción concluida (SI)
Medida de seguridad técnica:	Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:	<p>A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. <i>Por ejemplo:</i> en sistemas Linux desactivar la instalación de versiones <i>beta, test, debug, non-official</i>.</p> <p>B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. <i>Por ejemplo:</i> En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo.</p> <p>C) Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> no debe estar instalado.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales			D1012a	
Formato:	11	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.			
Proceso recomendado:	<p>A) Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos.</p> <p>B) En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.</p> <p>C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. <i>Por ejemplo</i>; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				9 de agosto de 2022
Observaciones / anotaciones				


Sistema de Informes Anuales			D1012a	
Formato:	12	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.			
Aplicable en:	III. Equipo de cómputo.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.			
Proceso recomendado:	<p>A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades <i>flash</i>, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo.</p> <p>B) La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área.</p> <p>C) Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo.</p> <p>2.- En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.</p>			
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones	Los equipos asociados al sistema no salen del Instituto			


Sistema de Informes Anuales			D1012a	
Formato:	13	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Tres días hábiles.			
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.			
Proceso recomendado:	<p>A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo: SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy).</i></p> <p>B) Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. <i>Por ejemplo,</i> en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando <i>apt-get install openssh-server.</i></p> <p>C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo:</i> en Linux con el comando <i>sudo systemctl enable ssh.</i></p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	<p>1.- Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad.</p> <p>2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.</p>			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				9 de agosto de 2022
Observaciones / anotaciones				



Sistema de Informes Anuales		D1012a	
Formato:	14	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.		
Aplicable en:	Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:	<p>A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> máquina virtual directorio temporal en el servidor.</p> <p>B) Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando.</p> <p>C) Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.</p> <p>D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. <i>Por ejemplo:</i> en Linux se dispone de <i>shred, wipe, secure-delete, srm, sfill, sswap, sdmem</i>, que se pueden instalar desde el administrador de aplicaciones.</p> <p>E) Llenar y firmar este formato.</p>		
Mejores prácticas, referencias:	1.- Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión 09 de agosto de 2022	
Observaciones / anotaciones			


Sistema de Informes Anuales		D1012a	
Formato:	15	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	<p>A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.</p> <p>B) Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.</p> <p>C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.</p> <p>D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo:</i> Webservices, transferencia SFTP.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
			
Liliana Hernández Cervantes Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto 2022	
Observaciones / anotaciones	No aplica la transferencia ni referencia de los datos a otras instancias		

Sistema de Informes Anuales			D1012a	
Formato:	16	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.			
Proceso recomendado:	<p>A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles.</p> <p>B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).</p> <p>C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo</p> <p>D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo.</p> <p>E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales.</p> <p>F) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor			9 de agosto de 2022	
Observaciones / anotaciones				

Sistema de Informes Anuales		D1012a	
Formato:	17	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:	<p>A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia).</p> <p>B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo.</p> <p>C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Liliana Hernández Cervantes		Revisión	
Administrador del sistema de información o servidor		9 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales		D1012a	
Formato:	18	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnica:	Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:	<p>A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos.</p> <p>B) Designar responsables de respaldos y responsables de verificación de respaldos.</p> <p>C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Francisco Ruiz Sala Administrador del sistema de información o servidor		Fecha de revisión	
		9 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales		D1012a	
Formato:	19	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:	<p>A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema.</p> <p>B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.</p> <p>C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
			
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión	
Nombre y firma Administrador del sistema de información o servidor		09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales			D1012a	
Formato:	20	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.			
Proceso recomendado:	<p>A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <i>Por ejemplo:</i> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo.</p> <p>B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <i>Por ejemplo:</i> diario, semanal, mensual.</p> <p>C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <i>Por ejemplo:</i> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución				
				
Francisco Ruiz Sala Administrador del sistema de información o servidor			Fecha de revisión	
			09 de agosto de 2022	
Observaciones / anotaciones				


Acciones realizadas:



Se comenzó a llevar el inventario de las bitácoras, las cuales se respaldan diariamente en el mismo esquema que la base de datos y el sistema



Sistema de Informes Anuales		D1012a	
Formato:	21	Verificación anual	Acción concluida (SI)
Norma Complementaria Técnica	Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:	<p>A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.</p> <p>B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red.</p> <p>C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable.</p> <p>D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento.</p> <p>E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:	Administración de redes de datos.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales		D1012a	
Formato:	22	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:	<p>A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <i>Por ejemplo:</i> para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales.</p> <p>B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <i>Por ejemplo,</i> en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo.</p> <p>C) Dejar activos solamente los puertos necesarios para la operación del sistema.</p> <p>D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <i>Por ejemplo:</i> Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			

Sistema de Informes Anuales		D1012a		
Formato:	23	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de estos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	<p>A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión.</p> <p>B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.</p> <p>C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar - equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución				
				
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión		
Administrador del sistema de información o servidor		09 de agosto de 2022		
Observaciones / anotaciones				

Sistema de Informes Anuales		D1012a	
Formato:	24	Verificación anual	Acción concluida (NO)
Medidas de seguridad técnicas:	Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:	<p>A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx .</p> <p>B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A.</p> <p>C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			
			
Francisco Ruiz		Fecha de revisión	
Administrador del sistema de información o servidor		09 de agosto de 2022	
Observaciones / anotaciones			



Sistema de Informes Anuales		D1012a	
Formato:	25	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:	<p>A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información.</p> <p>B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática.</p> <p>C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico.</p> <p>D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			
			
Liliana Hernández Cervantes		Francisco Ruiz Sala	
Administrador del sistema de información o servidor		Fecha de revisión	
		09 de agosto de 2022	
Observaciones / anotaciones			

Sistema de Informes Anuales		D1012a		
Formato:	26	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. III. b) Definir el programa de mantenimiento preventivo.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.</p> <p>B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.</p> <p>C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones				

Sistema de Informes Anuales		D1012a		
Formato:	27	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.</p> <p>B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo.</p> <p>C) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
				
Liliana Hernández Cervantes		Francisco Ruiz Sala		Fecha de revisión
Administrador del sistema de información o servidor				09 de agosto de 2022
Observaciones / anotaciones				

Acciones realizadas:

El Departamento de Cómputo tiene personal especializado que realiza el mantenimiento preventivo del equipo cada 6 meses o cuando la situación lo requiera por urgencia.

Sistema de Informes Anuales		D1012a	
Formato:	28	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.		
Aplicable en:	Servicios en la nube pública.		
Tiempo estimado:	Hito.		
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el resguardo de archivos cifrados, no en producción.		
Proceso recomendado:	<p>A) Identificar los respaldos que se tengan resguardados en servicios de nube pública.</p> <p>B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.</p>		
Mejores prácticas, referencias:	1.- La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.		
Ejecución			
			
Liliana Hernández Cervantes	Francisco Ruiz Sala	Fecha de revisión	
Administrador del sistema de información o servidor		09 de agosto de 2022	
Observaciones / anotaciones	Es sistema se respalda y se tiene activo únicamente dentro de la dependencia y no se usan servicios en la Nube		

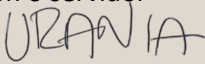
(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato	1	Verificación anual	Acción concluida	(SI)
Medida de seguridad técnica:	Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información, por medio de formato o comandos.</p> <p>C) Verificar que los datos usados en el desarrollo no correspondan a personas identificables.</p> <p>D) Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B.</p> <p>E) Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios.</p> <p>2.- Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de tablas.			
Ejecución				
M.C. Urania Ceseña Borbon Programador, desarrollador o diseñador del sistema de información		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	Se cumple con todos los puntos recomendados, el sistema de desarrollo tiene en su base de datos información ficticia. Se realizó el respaldo de la base de datos.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	2	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Un día hábil.			
Importancia de la acción:	No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.			
Proceso recomendado:	<p>A) Realizar respaldo completo de la base de datos.</p> <p>B) Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso.</p> <p>C) Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales.</p> <p>D) Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B.</p> <p>E) Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.</p>			
Mejores prácticas, referencias:	<p>1.- Definir niveles de acceso adecuados para cada perfil o tipo de usuario.</p> <p>2.- Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.</p>			
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información <i>URANIA</i>		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	En el sistema se asignan privilegios distintos a los usuarios dependiendo las tareas que deben de realizar.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	3	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:	<p>A) En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación.</p> <p>B) El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo).</p> <p>C) Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx.</p> <p>D) Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.</p>		
Mejores prácticas, referencias:	<p>1.- Los certificados SSL deben tener una vigencia de al menos un año.</p> <p>2.- En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (<i>wildcard</i>).</p> <p>3.- Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Administración de servicios Web.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Si se cumple con el certificado de seguridad en el servidor.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70	
Formato:	4	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:	<p>A) Elaborar documento con la secuencia de respaldos al menos con el siguiente orden:</p> <ul style="list-style-type: none"> - Diario – incremental. - Semanal – incremental. - Mensual – total. <p>B) Establecer en el plan los medios para resguardo del respaldo y su forma de identificación:</p> <ul style="list-style-type: none"> - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. <p>C) Incluir en el plan:</p> <ul style="list-style-type: none"> - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: <i>Recovery Time Objective</i>. Tiempo objetivo de recuperación. - RPO: <i>Recovery Point Objective</i>: Punto objetivo de recuperación. <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:	Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución		Fecha inicio	
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión	
		9/agosto/2022	

Observaciones / anotaciones	Se lleva a cabo el respaldo de la base de datos, de las tablas, de los programas semanalmente. El procedimiento se lleva a cabo manual, es necesario llevar a cabo el almacenamiento de manera automática.
------------------------------------	---

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70	
Formato:	5	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. i) Definir el procedimiento para el borrado seguro.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:	<p>A) Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos.</p> <p>B) Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo.</p> <p>C) El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores.</p> <p>D) Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_resp_onsiva_borrado_datos.pdf</p> <p>2.- Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar <i>DOD-5220.22-M</i>.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Comandos de borrado.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor 		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Solo se han hecho pruebas de borrado seguro de forma manual. Se debe automatizar el borrado seguro. Mejorar el plan de borrado seguro.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	6	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM		
Aplicable en:	II. Sistemas operativos y servicios.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:	<p>A) Realizar la verificación y configuración con privilegio de administrador del sistema operativo.</p> <p>B) En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. <i>Por ejemplo</i>, en el caso del sistema operativo Linux: - Verificar la existencia del archivo <code>/etc/ntp.conf</code> - Editar el archivo <code>ntp.conf</code> incluyendo en la primera línea: <code>server ntpdgtic.redunam.unam.mx ó</code> <code>server 132.247.169.17</code> - Reiniciar el demonio del cliente NTP con el comando <code>sudo service ntp reload</code>.</p> <p>C) En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM.</p> <p>2.- No se deben usar otros servidores de NTP distintos al de UNAM.</p>		
Conocimientos requeridos:	Administración de sistema operativo.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se tiene configurado el servidor de NTP-UNAM como servidor de tiempo de referencia.		

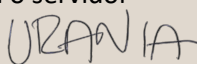
(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	7	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Dos días hábiles.			
Importancia de la acción:	El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de <i>malware</i> (<i>rootkits</i> , <i>backdoors</i> o códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.			
Proceso recomendado:	<p>A) En función del sistema operativo, instalar uno o varios programas para la contención de malware. <i>Por ejemplo</i>, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como <i>chkrootkit</i>, <i>rootkit hunter</i>, <i>bothunter</i>, <i>clamAV</i>, <i>avast</i>, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso.</p> <p>B) Disponer de comandos para la localización de amenazas. <i>Por ejemplo</i>, para el caso de Linux, se recomienda usar el comando <i>grep</i> para la detección de cadenas regulares de texto en las invocaciones al <i>shell</i>.</p> <p>C) Una vez instalada la solución, verificar periódicamente su actualización</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- UNAM-CERT puede asesorar en la selección de las herramientas <i>anti malware</i> más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	Se tiene instalado un firewall interno y además una herramienta de auditoría de seguridad y antimalware como lo es Lynis.			

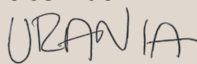
(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70		
Formato:	8	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.			
Aplicable en:	II. Sistemas operativos y servicios.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El servidor que hospeda el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.			
Proceso recomendado:	<p>A) En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. <i>Por ejemplo</i>, en el sistema operativo Linux ejecutar <i>apt-get update</i> para obtener la lista de actualizaciones, especialmente en el repositorio <i>security</i> de la respectiva distribución.</p> <p>B) Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad.</p> <p>C) Instalar las actualizaciones en el sistema operativo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.			
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	Se lleva a cabo mensualmente la actualización de todo el software instalado en el servidor, previamente se lleva a cabo la actualización en servidor de prueba de versiones.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	9	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:	<p>A) Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema.</p> <p>B) Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. <i>Por ejemplo:</i> el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (<i>Active Directory</i>), <i>LDAP</i> u <i>OpenAIM</i>.</p> <p>2.- Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.</p>		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se lleva a cabo la autenticación de los usuarios que tiene acceso al sistema. Y el usuario puede cambiar sus credenciales de entrada cuando lo requiera.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	10	Verificación anual	Acción concluida (SI)
Medida de seguridad técnica:	Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.		
Aplicable en:	II. Sistemas operativos.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:	<p>A) Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. <i>Por ejemplo:</i> en sistemas Linux desactivar la instalación de versiones <i>beta, test, debug, non-official.</i></p> <p>B) De la lista de software instalado, verificar el consumo de recursos de aplicaciones <i>TSR (Terminal and Stay Resident)</i>. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. <i>Por ejemplo:</i> En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo.</p> <p>C) Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. <i>Por ejemplo,</i> si el servidor Linux no proporcionará direcciones IP, el demonio o servicio <i>dchpd</i> no debe estar instalado.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	En el servidor sólo se encuentran disponibles los puertos necesarios para el sistema y el software necesario.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	11	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.		
Aplicable en:	III. Equipo de cómputo.		
Tiempo estimado:	Dos días hábiles.		
Importancia de la acción:	Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:	<p>A) Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos.</p> <p>B) En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar.</p> <p>C) Establecer y seguir un plan de mejoramiento de la protección física de equipos. <i>Por ejemplo:</i> cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:	Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión	
		9/agosto/2022	
Observaciones / anotaciones	Se tiene medidas físicas que limitan el acceso físico a equipos a personas no autorizadas.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	12	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.		
Aplicable en:	III. Equipo de cómputo.		
Tiempo estimado:	Un día hábil.		
Importancia de la acción:	Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:	<p>A) Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades <i>flash</i>, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo.</p> <p>B) La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área.</p> <p>C) Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo.</p> <p>2.- En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.</p>		
Conocimientos requeridos:	Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor 		Fecha término 9/agosto/2022	
Observaciones / anotaciones	Se tiene un formulario como mecanismo de control cuando se desea registrar una salida de equipo de las instalaciones.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	13	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.		
Aplicable en:	IV. Red de datos.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:	<p>A) Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. <i>Por ejemplo: SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy).</i></p> <p>B) Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. <i>Por ejemplo, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando <code>apt-get install openssh-server</code>.</i></p> <p>C) Activar los protocolos de comunicación encriptada en el servidor. <i>Por ejemplo: en Linux con el comando <code>sudo systemctl enable ssh</code>.</i></p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	<p>1.- Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad.</p> <p>2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.</p>		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor 		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Para tener acceso al servidor es necesario utilizar aplicaciones instalados para comunicación cifrada.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	14	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.		
Aplicable en:	Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Tres días hábiles.		
Importancia de la acción:	Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:	<p>A) Realizar una copia integral del sistema de información y colocarla en un servicio temporal. <i>Por ejemplo:</i> máquina virtual directorio temporal en el servidor.</p> <p>B) Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando.</p> <p>C) Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa.</p> <p>D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. <i>Por ejemplo:</i> en Linux se dispone de <i>shred, wipe, secure-delete, srm, sfill, sswap, sdmem</i>, que se pueden instalar desde el administrador de aplicaciones.</p> <p>E) Llenar y firmar este formato.</p>		
Mejores prácticas, referencias:	1.- Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:	Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se tiene el procedimiento para el borrado seguro de un subdirectorío ya se llevaron a cabo en un servidor de pruebas.		



(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resgol.3.70	
Formato:	15	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas	Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.		
Proceso recomendado:	<p>A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.</p> <p>B) Con el Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <i>Por ejemplo:</i> La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.</p> <p>C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.</p> <p>D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <i>Por ejemplo:</i> Webservices, transferencia SFTP.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se cuenta con un inventario de las tablas de la base de datos que maneja el sistema.		



(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	16	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Ocho días hábiles.		
Importancia de la acción:	Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:	<p>A) Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles.</p> <p>B) Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador).</p> <p>C) Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo</p> <p>D) Activar bitácoras de acceso (<i>log</i>) hacia el equipo central de desarrollo.</p> <p>E) Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales.</p> <p>F) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se tiene control de acceso al servidor y registro de acceso, y se centralizará el código fuente y documentación del sistema de información		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resgol.3.70	
Formato:	17	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Cuatro días hábiles.		
Importancia de la acción:	Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:	<p>A) Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia).</p> <p>B) Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo.</p> <p>C) Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo.</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).		
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha término 9/agosto/2022	
Observaciones / anotaciones	Se encuentra en desarrollo el plan DRP (Plan de recuperación de Desastres) para la recuperación del servidor donde se alberga el sistema. Este plan garantizará la continuidad de la operación y disponibilidad del servicio del sistema.		

v


(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	18	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnica:	Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Ocho días hábiles.			
Importancia de la acción:	Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.			
Proceso recomendado:	<p>A) De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos.</p> <p>B) Designar responsables de respaldos y responsables de verificación de respaldos.</p> <p>C) Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (DRP).			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones		Se lleva un respaldo manual de todo el sistema y la base de datos del sistema. El respaldo se lleva a cabo en un servidor virtual y se llena una bitácora.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	19	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.		
Aplicable en:	I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:	Veinte días hábiles.		
Importancia de la acción:	Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:	<p>A) Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. <i>Por ejemplo:</i> En caso de consultar vía un <i>Webservice</i> a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema.</p> <p>B) Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. <i>Por ejemplo:</i> Si la cuenta de acceso a un <i>Webservice</i> – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema.</p> <p>C) Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. <i>Por ejemplo:</i> si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx</p> <p>D) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:	Administración de sistema de información. Gestión de bases de datos.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Las cuentas de control para acceder al sistema son cuentas administradas por el administrador del sistema y son de personas de la universidad.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	20	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.			
Aplicable en:	II. Sistemas operativos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.			
Proceso recomendado:	<p>A) Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. <i>Por ejemplo:</i> En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (<i>logs</i>), de forma física las bitácoras de acceso al área donde está el equipo de cómputo.</p> <p>B) Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. <i>Por ejemplo:</i> diario, semanal, mensual.</p> <p>C) Establecer en el documento el procedimiento de resguardo de las bitácoras. <i>Por ejemplo:</i> respaldo y protección de <i>logs</i> en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión		
		9/agosto/2022		
Observaciones / anotaciones	Se cuenta con algunas bitácoras, pero es necesario revisar y mejorar. Las bitácoras se tienen en diferente lugar al servidor.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70		
Formato:	21	Verificación anual	Acción concluida	(SI)
Norma Complementaria Técnica	Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.			
Proceso recomendado:	<p>A) Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones.</p> <p>B) Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red.</p> <p>C) Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable.</p> <p>D) Mantener actualizados los equipos activos de red y con un programa de mantenimiento.</p> <p>E) Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.			
Conocimientos requeridos:	Administración de redes de datos.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión		
		9/agosto/2022		

Observaciones / anotaciones	El equipo de ruteo que dan servicio de red al servidor cuenta con IP que no es público y además el acceso al sitio es estrictamente controlado.
------------------------------------	--

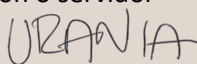
(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	22	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.			
Aplicable en:	IV. Red de datos.			
Tiempo estimado:	Cuatro días hábiles.			
Importancia de la acción:	Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.			
Proceso recomendado:	<p>A) Revisar los puertos de comunicación (<i>TCP</i> y <i>UDP</i>) que requiera el sistema de información para su operación. <i>Por ejemplo:</i> para servicios <i>Web</i> los puertos 80 y 8080 son los convencionales.</p> <p>B) Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. <i>Por ejemplo,</i> en Linux puede tratarse de un <i>firewall</i> a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo.</p> <p>C) Dejar activos solamente los puertos necesarios para la operación del sistema.</p> <p>D) Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. <i>Por ejemplo:</i> Permitir el acceso al puerto de <i>SSH</i> solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas.</p> <p>E) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- No se deben tener activos accesos que no son necesarios vía la red de datos.			
Conocimientos requeridos:	Administración de sistema de información. Administración de sistema operativo.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor 		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	En el servidor se tiene activo solo los puertos que se requiere. Se tiene instalado un firewall para filtrar los puertos.			



(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	23	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.			
Proceso recomendado:	<p>A) Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión.</p> <p>B) Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador.</p> <p>C) Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar - equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.			
Conocimientos requeridos:	Administración de sistema de información. Desarrollo de aplicaciones.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión		
		9/agosto/2022		
Observaciones / anotaciones	Se cuenta con varios servidores en total, uno donde se encuentra operando el sistema, otro donde se encuentran operando las versiones del SO para la actualización del mismo y otro donde se tiene el respaldo de las bases de datos y del programa y es el servidor de desarrollo y prueba.			



(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70		
Formato:	24	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.			
Aplicable en:	I. Bases de datos y sistemas de tratamiento.			
Tiempo estimado:	Veinte días hábiles.			
Importancia de la acción:	Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio.unam.mx.			
Proceso recomendado:	<p>A) Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx .</p> <p>B) Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A.</p> <p>C) Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.			
Conocimientos requeridos:	Administración de aplicaciones. Administración de sistema operativo.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión 9/agosto/2022		
Observaciones / anotaciones	Se tiene programado realizar pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Resol.3.70	
Formato:	25	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.		
Aplicable en:	III. Equipos de cómputo.		
Tiempo estimado:	Hito.		
Importancia de la acción:	Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:	<p>A) Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información.</p> <p>B) Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática.</p> <p>C) Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico.</p> <p>D) Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico.</p> <p>E) Llenar y firmar formato.</p>		
Mejores prácticas, referencias:	1.- El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:	Administración de infraestructura.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor 		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	Se tiene el inventario mínimo de requerimientos del servidor.		

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	26	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 18. III. b) Definir el programa de mantenimiento preventivo.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Hito.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.</p> <p>B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.</p> <p>C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.</p> <p>D) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión		
		9/agosto/2022		
Observaciones / anotaciones	Se pretende hacer un mantenimiento preventivo cada año y tener un equipo de respaldo.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70		
Formato:	27	Verificación anual	Acción concluida	(SI)
Medidas de seguridad técnicas:	Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.			
Aplicable en:	III. Equipos de cómputo.			
Tiempo estimado:	Seis días hábiles.			
Importancia de la acción:	Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.			
Proceso recomendado:	<p>A) En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad.</p> <p>B) En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo.</p> <p>C) Llenar y firmar formato.</p>			
Mejores prácticas, referencias:	1.- Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.			
Conocimientos requeridos:	Administración de infraestructura.			
Ejecución				
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor		Fecha revisión		
		9/agosto/2022		
Observaciones / anotaciones	Se tiene el plan de reemplazar el servidor cada 3 años. Reemplazar el hardware en su totalidad.			

(Nombre del sistema A1) REGISTRO DE SOLICITUDES EN LÍNEA (REGSOL)		Identificador único A1 Regsol.3.70	
Formato:	28	Verificación anual	Acción concluida (SI)
Medidas de seguridad técnicas:	Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.		
Aplicable en:	Servicios en la nube pública.		
Tiempo estimado:	Hito.		
Importancia de la acción:	No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:	A) Identificar los respaldos que se tengan resguardados en servicios de nube pública. B) Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:	1.- La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:	Administración de respaldos. Administración de sistema operativo.		
Ejecución			
M.C. Urania Ceseña Borbon Administrador del sistema de información o servidor <i>URANIA</i>		Fecha revisión 9/agosto/2022	
Observaciones / anotaciones	El sistema no utiliza los servicios de una nube pública.		