UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

SUBSISTEMA DE LA INVESTIGACIÓN CIENTÍFICA

INSTITUTO DE FÍSICA

Documento de Seguridad

IF-SGSDP-DS

TABLA DE AUTORIZACIÓN

Elaboró y Revisó:

Responsable de Seguridad de Datos Personales

Tel: 56225001
javier@fisica.unam.mx

Ing. Fernando Javier Martínez Mendoza

Fecha de Emisión: 19 de Enero del 2021

Coordinadora de la Unidad de Vinculación

Tel: 56225090
victoria@fisica.unam.mx

Mtra. Victoria Silva Domínguez

Aprobó:

Directora del Instituto de Física

Tel: 56225032
direccion-if@fisica.unam.mx

Dra. Cecilia Noguez Garrido

PÁGINA EN BLANCO

ÍNDICE

Contenido

0. 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 Física con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

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

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/IEC 27002:2013 "Tecnología de la información - Técnicas de seguridad - Código de práctica para los controles de seguridad de la información"

1. Objetivo

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales del Instituto de Física de la Universidad Nacional Autónoma de México (IF), 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.

2. Términos, definiciones y abreviaturas

2.1 Términos y definiciones

2.1.1 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.

2.1.2 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.

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

2.1.4 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.

2.1.5 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.

2.1.6 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.

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

2.1.8 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.

2.1.9 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.

2.1.10 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.

2.1.11. 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.

2.1.12 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.

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

2.1.14 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.

2.1.15 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.

2.1.16 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 y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

2.1.17 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.

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

2.1.19 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.

2.1.20 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.

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

2.1.22 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.

2.1.23 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.

2.1.24 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, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros, y los que produzca el avance de la tecnología.

2.1.25 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.

2.1.26 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; XXXVII. 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.

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

2.1.28 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.

2.1.29 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.

2.2 Abreviaturas

2.2.1 IF: Instituto de Física de la UNAM

2.2.2 SGSDP: Sistema de Gestión de Seguridad de Datos Personales

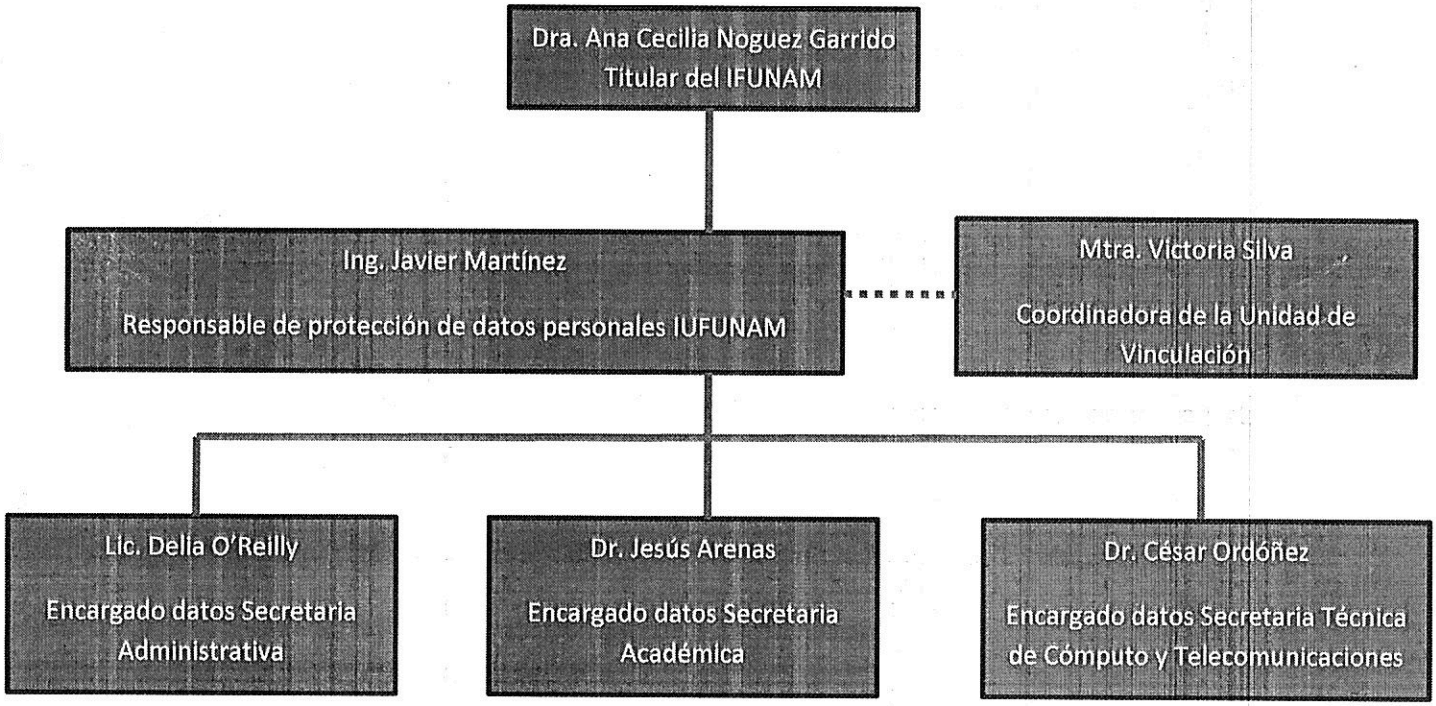
3. Alcance

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

3.1 Funciones y Responsabilidades

En el SGSDP del IF, la responsabilidad, autoridad e interrelaciones del personal que trata datos personales, se mantiene con la siguiente cadena de rendición de cuentas:

a) Organigrama del SGSDP



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 éste Documento de Seguridad.

Responsables

- 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 éste Documento de Seguridad.

Encargados:

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

En el Instituto de Física, los roles son:

Rol	**Figura**
Titular	Titular del Instituto de Física
Responsable	Responsable designado por el Titular del Instituto de Física
Encargado	De acuerdo al uso de los datos personales definidos en el Anexo 2: Secretario Académico Secratrio Administrativo Secretario Técnico de Cómputo y Telecomunicaciones
Usuarios	Definido en el Anexo 2 de acuerdo al uso de datos personales

3.2 Sistema de Gestión de Seguridad de Datos Personales

3.2.1 El IF 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 disponiblidad 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 Física se compromete a cumplir con las medidas de seguridad par ala 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 ó en redes de datos.

Objetivo del SGSDP

El objetivo del SGSDP son:

1. Asegurar la integridad, confidencialidad y disponiblidad de la información que contengan datos personales.

3.2.2 El SGSDP cuenta con un inventario con información sobre el tratamiento de datos personales por área administrativa, académica ó 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, indicando si son sensibles o no;
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.

3.2.3 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.

3.2.4 Cada Sistema de Tratamiento sirve 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. El detalle de cada sistema de tratamiento de datos personales por área administrativa, académica ó de servicio responsable se encuentra en el **ANEXO 2** de éste documento.

3.3 Análisis de Riesgos

3.3.1 El IF 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:

3.3.2 Los riesgos sobre el tratamiento de datos personales se detectan por área administrativa, académica ó de servicio y por cualquier persona que dé tratamiento de datos personales.

3.3.3 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:

- Los requerimientos regulatorios, legales y reglamentarios.
- El valor de los datos personales de acuerdo a si son sensibles o no y su ciclo de vida;
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- 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 raíz como los 5 por qué's, diagrama de Ishikawa, entre otros.

Probabilidad
La probabilidad subjetiva de que ocurra el riesgo. Es la posibilidad de que ocurra una vulneracion 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

Impacto

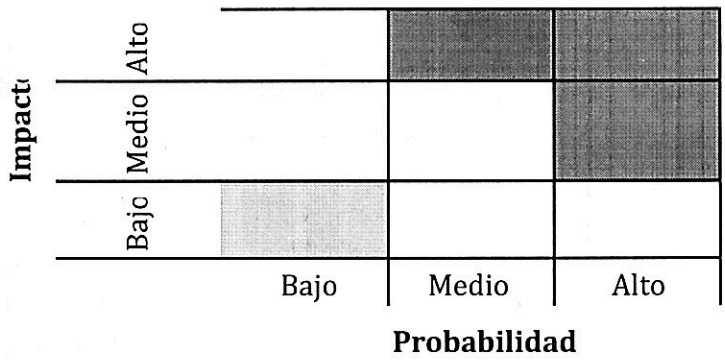
El impacto del riesgo se refiere al impacto a las consecuencias negativas, daño o afectación para los titulares que pudieran derivar de una vulneración de seguridad ocurrida en los datos personales. Criterio cuya escala es:

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

Cálculo de Nivel de valor de Riesgo

Para éste caso, se asume que el Impacto y la Probabilidad tienen el mismo valor para la valuación 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:



Gráfica 1. Probabilidad vs Impacto 1

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 del riesgo

3.3.3 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.

3.3.4. Una vez identificado el tratamiento del riesgo se plantean acciones para mitigar, eliminar, transferir ó aceptar el riesgo, debiendo considerar los controles de seguridad física, administrativa y técnica para la protección de datos personales.

3.3.5 Cuando se identifique algún riesgo se debe notificar a la RSGPDP para que la integre a la Matriz de Riesgos.

3.4 Análisis de Brecha

El IF 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.

3.5 Plan de Trabajo

3.5.1 El IF 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 éste documento.

3.6 Medidas de seguridad para la protección de datos personales

3.6.1 El IF implementa medidas de seguridad técnicas, administrativas y físicas para aegurar la protección de los datos personales presentadas en el **ANEXO 5.**

3.7 Capacitación

Dentro de la capacitacitación para la comunidad del IFUNAM, se estarán estableciendo:

- Charlas informativas sobre temas de protección de datos personales

- Corrreos masivos con información del tema

- Generación de elementos gráficos con información de protección de datos personales

Esta capacitación debe de incluír 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.

4. Anexos

ANEXO 1	Lineamientos
ANEXO 2	Inventario
ANEXO 3	Análisis de Riesgos
ANEXO 4	Análisis de Brecha
ANEXO 5	Planes de Trabajo

5. Identificación de los cambios

Fecha de revisión	Versión	Descripción de la modificación	Página/ Sección
19 de Enero del 2021	1	Versión inicial	