UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
INSTITUTO DE CIENCIAS FÍSICAS

Sistema de Gestión de Seguridad de Datos Personales

Documento de Seguridad

ICF-DS

Fecha de emisión: 17/08/2022

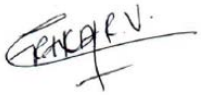
TABLA DE AUTORIZACIÓN

Elaboró y Revisó:

Responsable legal de la dependencia de Seguridad de Datos Personales

Ext. 27747

erika@icf.unam.mx



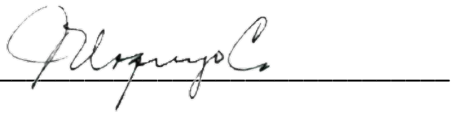
_____

Lic. Erika Ruiz Vázquez

Aprobó:

Director del Instituto de Ciencias Físicas
Ext. 27745

dirección@icf.unam.mx



_____

Dr. Jaime de Urquijo Carmona

Contenido

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 Ciencias Físicas con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que estos contiene.

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 del 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 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 Púbico, 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 anexo 1.

El origine de este 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 debido a los activos que posee esta máxima casa de estudios, basados en los estándares internacionales en materia de seguridad de la información ISO/IEC.

Objetivo

Describir las medidas de seguridad del Sistema de Gestión de la Seguridad de Datos Personales del Instituto de Ciencias Físicas de la Universidad Nacional Autónoma de México , desde su obtención registro, organización, conservación, elaboración, utilización, comunicación, difusión,

almacenamiento, tratamiento, posesión, acceso, resguardo, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, así como proteger todos los datos personales y datos sensibles, mediante cualquiera de los siguientes tipos de soporte:

- En soportes físicos.
- En soportes electrónicos.
- En soportes de datos.

Términos, definiciones

Definiciones previstas en el numeral 2 de los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México, para los efectos de las presentes Normas se entenderá por:

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.

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.

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.

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.

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.

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.

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

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación de este.

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.

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.

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.

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.

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.

Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos: Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México.

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

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.

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.

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.

Principio del menor privilegio: Otorgamiento de los permisos necesarios y suficientes a un usuario autorizado para acceder a un sistema de información para el desempeño de sus actividades.

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.

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

Responsable de Archivos: Persona designada por el titular de cada Área Universitaria, de entre la plantilla laboral existente, para contribuir al debido cumplimiento de los procedimientos, obligaciones, lineamientos y criterios emitidos por las figuras rectoras del Sistema Institucional de Archivos de la Universidad y funge como enlace entre el Área Universitaria y el Área Coordinadora de Archivos para la mejor organización, administración y conservación de los archivos universitarios.

Responsable de seguridad de datos personales: Encargado de las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales designado por cada Área Universitaria.

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

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.

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

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.

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.

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.

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.

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;

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.

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

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.

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.

Alcance

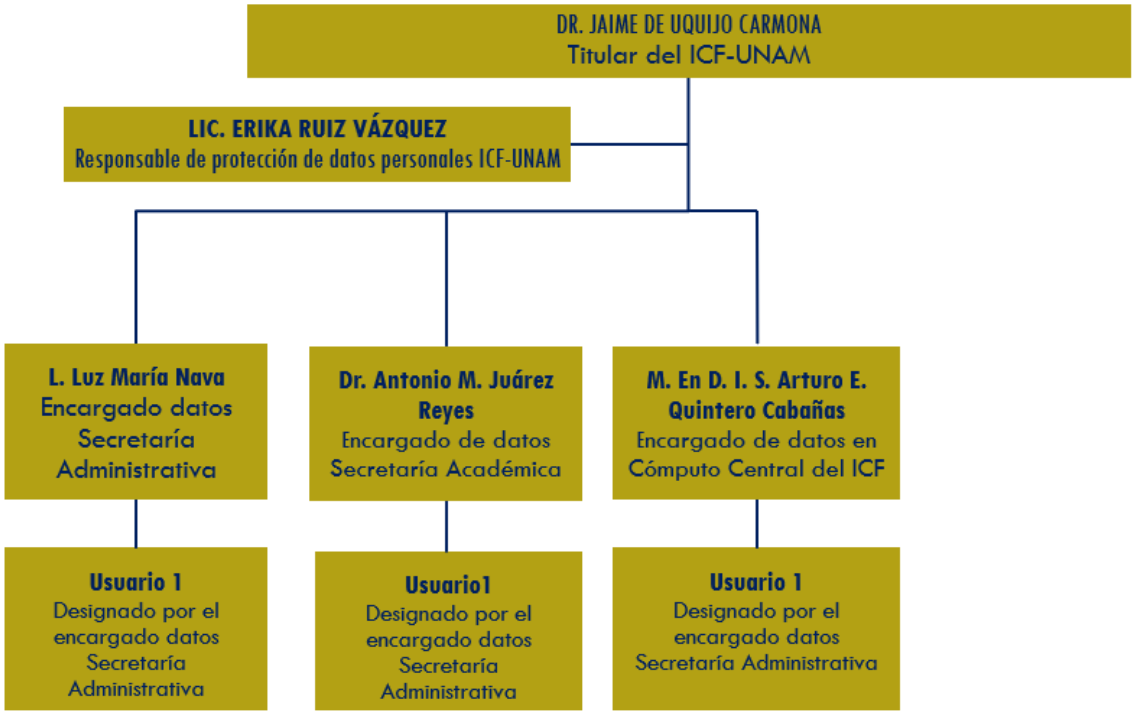
El desarrollo de este plan de seguridad aplica a todas las áreas administrativas, académicas y de servicio que tienen en su poder datos personales y daos personales sensibles.

Con el apoyo de las áreas administrativas se identificarán los sistemas de tratamiento de datos personales que posee esta área universitaria, el tipo de datos personales que contiene cada uno, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad concretas implementadas.

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

Funciones y Responsabilidades

El Sistema de Gestión de Seguridad de Datos Personales del ICF, presenta el siguiente organigrama de jerarquía y responsabilidades:



A continuación, se describen las actividades, responsabilidades y funciones de cada uno de los miembros del organigrama:

Titular

Su función es supervisar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla, acorde a lo establecido en el Documento de Seguridad.

Responsable

Persona designada por el titular de cada Área Universitaria, de entre la plantilla laboral existente, para contribuir al debido cumplimiento de los procedimientos, obligaciones, lineamientos y criterios emitidos por las figuras rectoras del Sistema Institucional de Archivos de la Universidad y funge como enlace entre el Área Universitaria y el Área Coordinadora de Archivos para la mejor organización, administración y conservación de los archivos universitarios.

Su función es verificar que el Sistema de Gestión de Seguridad de Datos Personales se cumpla en los distintos departamentos del área universitaria:

- Secretaría Administrativa.
- Secretaría Académica.
- Cómputo Central-ICF.

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.

Su función es mantener el Sistema de Gestión de Seguridad de Datos Personales de cada departamento del área universitaria:

- Secretaría Administrativa.
- Secretaría Académica.
- Cómputo Central-ICF.

Usuarios

Sus funciones es el tratamiento y uso de los datos personales, regidos por las norma, políticas y lineamiento establecidos en el Sistema de Gestión de Seguridad de Datos Personales y Documento de Seguridad, de cada departamento del área universitaria:

- Secretaría Administrativa.
- Secretaría Académica.
- Cómputo Central-ICF.

La definición de cada función la podemos observar en la imagen #

Sistema de Gestión de Seguridad de Datos Personales

El Instituto de Ciencias Físicas establece y mantiene un Sistema de Gestión de Seguridad de Datos Personales establece, procedimientos, políticas y sistemas, cada uno con instrucciones necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, acorde al reglamento de transparencia y acceso a la información pública de la Universidad Nacional Autónoma de México, publicada el 26 de agosto de 2016 y a las Normas Complementarias sobre las 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 por el pleno del Comité de Transparencia de la Universidad Nacional Autónoma de México.

Políticas del Sistema de Gestión de Seguridad de Datos Personales

El Instituto de Ciencias Físicas deberá implementar un sistema de gestión de seguridad de los datos personales para planificar, establecer, implementar, operar, monitorear, mantener, revisar y mejorar las medidas de seguridad de carácter administrativo, físico y técnico aplicadas a los datos personales; tomando en consideración los estándares nacionales e internacionales en materia de protección de datos personales y seguridad.

Objetivo del Sistema de Gestión de Seguridad de Datos Personales

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

Dentro del Sistema de Gestión de Seguridad de Datos Personales del Instituto de Ciencias Físicas, se establece lo siguiente:

- Inventario de sistemas que contengan Datos Personales.
- Roles y responsabilidades específicas de los involucrados en el tratamiento de datos personales.
- Ciclo de vida de los datos personales.
- Análisis de Riesgos
- Análisis de Brecha
- Plan de Trabajo
    - Evaluación de impacto en la protección de datos personales
    - Controles físicos de ingreso a las instalaciones, archivos y soportes físicos
- Medidas de Seguridad Técnicas para la Protección de datos Personales
- Medidas de Seguridad Administrativas para la Protección de Datos Personales.
- Capacitación.

Inventario de sistemas que contengan Datos Personales.

En el Sistema de Gestión de Seguridad de Datos Personales del Instituto de Ciencias Físicas 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, cada sistema identificado podremos observar sus características en el Anexo 2, encontraremos el inventario de sistemas que contienen datos personales, en el cual se recaba la siguiente información:

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;

Roles y responsabilidades específicas de los involucrados en el tratamiento de datos personales.

El Responsable de seguridad de datos personales documentará los roles y cadena de rendición de cuentas de las personas que traten datos personales en su Área Universitaria, conforme al sistema de gestión de seguridad implementado y materializado en el documento de seguridad a que se refieren los numerales 24 y 25 de los Lineamientos.

Cada Área Universitaria se asegurará de que todas las personas involucradas (Anexo 2) en el tratamiento de datos personales en el Área Universitaria conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión de seguridad, así como las consecuencias de su incumplimiento.

Ciclo de vida de los datos personales.

Dentro del Inventario de sistemas (Anexo 2), se incluye el tiempo de vida de los datos personales conforme a las siguientes etapas:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. 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;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales.

Análisis de Riesgos

En el Sistema de Gestión de Seguridad de Datos Personales del Instituto de Ciencias Físicas, se desarrolla un análisis de los riesgos de los datos personales tratados a partir de la evaluación de impacto por su probabilidad de ocurrencia, denominado riesgo real, considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo con su clasificación previamente definida 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:
   a. El riesgo inherente a los datos personales tratados;
   b. La sensibilidad de los datos personales tratados;
   c. El desarrollo tecnológico;
   d. Las posibles consecuencias de una vulneración para los titulares;
   e. Las transferencias de datos personales que se realicen;
   f. El número de titulares;
   g. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
   h. 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.

Se deben establecer controles de seguridad que mitiguen la ocurrencia del riesgo, se creará dicho control con el apoyo del análisis de riesgos y análisis de brecha de cada sistema, determinando en el plan de trabajo (Anexo 5)

Análisis de Brecha

El análisis de brecha está incluido dentro del Sistema de Gestión de Seguridad de Datos Personales del Instituto de Ciencias Físicas (anexo 4), en el cual se toman a consideración las siguientes recomendaciones:

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

Identificación y mitigación de riesgos

El Instituto de Ciencias Físicas determinará las opciones de tratamiento del riesgo con base en los resultados obtenidos en los análisis, tomará ayuda de los valores de impacto y probabilidad calculados, a continuación, se presentan los valores:

Aceptar: No tomar ninguna acción ante el riesgo y aceptar sus consecuencias. Los riesgos que se aceptan deben tener un impacto bajo para la organización

Mitigar: Desarrollar e implementar controles para contrarrestar la amenaza o minimizar el resultado del impacto, o ambos. Los riesgos que se mitigan tienen por lo general un impacto medio o alto para la organización.

Aplazar: Cuando el riesgo no se puede aceptar ni mitigar, es decisión de la organización el recopilar información adicional y realizar análisis adicionales. Estos riesgos son monitoreados y reevaluados en el futuro y generalmente no representan una amenaza inminente.

Estos valores se toman como referencia del análisis denominado “Allegro” sugerido por el CERT UNAM,

Plan de Trabajo

Los planes de trabajos están definidos por el resultado de los análisis de riesgos y análisis de brecha de cada sistema del inventario, dichos planes están definidos en el anexo 5.

Capacitación.

Para la capacitación sobre medidas de seguridad de datos personales a la comunidad del ICF se harán las siguientes acciones.

- Correos Informativos.
- Carteles sobre la protección de datos personales.
- Orientación sobre las buenas prácticas de datos personales.

La capacitación deberá 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.

Anexos

Anexo 1	Documento de Seguridad
Anexo 2	Inventario
Anexo 3	Análisis de Riesgos
Anexo 4	Análisis de Brecha
Anexo 5	Plan de Trabajo|