

**PLAN DE TRATAMIENTOS DE
RIESGOS Y SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
2021**

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



1. INTRODUCCIÓN	3
2. OBJETIVO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	4
3. CICLO DE OPERACIÓN MSIC	4
3.1 Fase de Diagnostico	5
3.2 Fase de Planificación	5
3.3 Fase de Implementación	6
3.4 Fase de Evaluación de Desempeño	6
3.5 Fase de Mejora Continua	7
4. PLAN DE IMPLEMENTACIÓN DEL MSIC	7

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



1. INTRODUCCIÓN

En este Plan de Seguridad y Privacidad de la Información, el IDEA establecerá las actividades que estarán contempladas en el Modelo de Seguridad de la Información y Ciberseguridad (MSIC), el cual encamina al Instituto a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo mantener la privacidad de los datos.

El Modelo opera a través de las siguientes 5 fases; diagnóstico, planificación, implementación, evaluación de desempeño y mejora continua.

Las fases incluirán objetivos, metas, procedimientos y seguimientos, permitiendo que la seguridad de la información y la ciberseguridad sean un sistema de gestión sostenible.

Adicionalmente, el Modelo de Seguridad de la Información y Ciberseguridad contiene toda la metodología para el tratamiento de riesgos, basado en la NTC/IEC ISO 27005:2008.

La Gestión de protección de datos tiene como propósito dar a conocer cuáles son los requisitos básicos de seguridad de la información para establecer controles efectivos sobre todas las actividades que se desarrollan en INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA, con el fin de que todos los involucrados en la operación o que prestan servicios garanticen el buen uso de los sistemas, herramientas, recursos e información a la que tienen acceso.

Así como, presentar los lineamientos de control para todos los empleados, terceros y entes que tengan acceso a la información de INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA, para garantizar su seguridad a través de los principios de confidencialidad, integridad y disponibilidad, estableciendo las políticas de seguridad que se aplican a todos los sistemas de información, la red, así como, a todas las instalaciones en las que procesan, almacenan, o transmiten información.

Teniendo en cuenta que la organización se enfrenta a amenazas relativas a la seguridad, en especial relacionados con el fraude asistido por computadores, como también a las acciones de personas, los cuales cada vez se han vuelto más comunes, ambiciosos y sofisticados. A continuación, se describen los principales objetivos específicos:

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



- Establecer y capacitar al personal de INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA en seguridad de la información, buscando el aumento en la cultura, así como en el compromiso con la adopción de buenas prácticas, el reporte de incidentes de seguridad y la identificación de riesgos.
- Minimizar los incidentes de seguridad de la información presentados en INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA.
- Mantener los sistemas y los recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
- Establecer los fundamentos para el desarrollo y la implantación de un Modelo de Seguridad de la información.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.

El presente Plan será actualizado con regularidad, dado que forma parte del Modelo Integrado de Planeación y Gestión -MIPG- y dando cumplimiento al Decreto 612 de 2018; por lo tanto, al identificar cambios en la normatividad en el negocio, en su estructura, objetivos o en general, deberá actualizarse y así asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

2. OBJETIVO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Establecer las actividades que están contempladas en el Modelo de Seguridad de la Información y Ciberseguridad alineadas con la NTC/IEC ISO 27001:2013, ISO 27032:2012, ISO 27005:2008 y las Circulares Externas de la Superintendencia Financiera de Colombia.

3. CICLO DE OPERACIÓN MSIC

El funcionamiento del Modelo de Seguridad de la Información Y Ciberseguridad se desarrollará en las siguientes 5 fases:

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

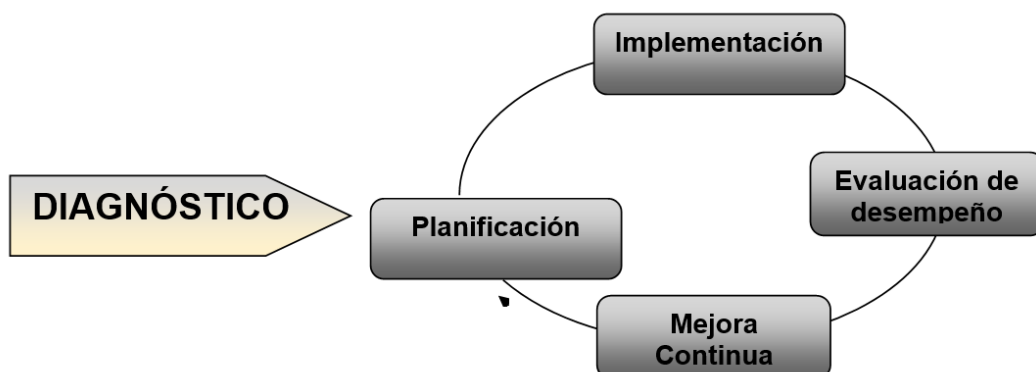


Figura 1. Ciclo de Operación

3.1 Fase de Diagnostico

En esta fase se pretende diagnosticar el estado del grado de madurez de los controles institucionales. Se identificará cual es el estado actual del IDEA frente a las seguridad de la información, privacidad de la información y ciberseguridad.

3.2 Fase de Planificación

Basados en los resultados obtenidos en la fase de diagnóstico, se procede a elaborar el Modelo de Seguridad de la Información y Ciberseguridad, con el propósito de definir acciones a implementar, a través de una metodología de gestión del riesgo.

La fase de planificación estará conformada por las siguientes procedimientos, planes y guías, los cuales deberán estar alineados con el objetivo misional del Instituto:

N°	INSTRUMENTO	RESPONSABLE
1	Modelo de Seguridad de la Información y Ciberseguridad (MSIC)	La Oficina Gestión del Riesgo, Comité de Seguridad de la Información y Ciberseguridad.
2	Política de Seguridad de la Información y Ciberseguridad	Comité de Seguridad de la Información y Ciberseguridad.
3	Guía de Roles y Responsabilidades de Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo y Dirección de Gestión Humana
4	Plan de Sensibilización para la Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo, Oficina Asesora de Comunicaciones y Comité de Seguridad de la Información.

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5	Procedimiento para la Gestión de Activos de Información	La Oficina Gestión del Riesgo y Centro de Atención Documental.
6	Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad	La Oficina Gestión del Riesgo y Dirección de Sistemas
7	Plan de Fuga de Información	La Oficina Gestión del Riesgo y Dirección de Sistemas
8	Guía para la Disposición Final de Información	La Oficina Gestión del Riesgo y Dirección de Sistemas
9	Procedimiento gestión de identidades y accesos	La Oficina Gestión del Riesgo y Dirección de Sistemas
10	Guía de Controles Criptográficos	La Oficina Gestión del Riesgo y Dirección de Sistemas
11	Procedimiento de Control de Acceso Físico	La Oficina Gestión del Riesgo, Dirección de Sistemas y Subgerencia Administrativa.
12	Procedimiento de Mantenimiento de Equipos	Dirección de Sistemas
13	Procedimiento de Gestión de Cambios	Oficina de Planeación
14	Procedimiento de Protección Contra Códigos Maliciosos	La Oficina Gestión del Riesgo y Dirección de Sistemas
15	Guía de Seguridad en la Nube	La Oficina Gestión del Riesgo y Dirección de Sistemas
16	Guía de Hardening (Endurecimiento)	La Oficina Gestión del Riesgo y Dirección de Sistemas
17	Procedimiento Seguridad en Proyectos críticos	La Oficina Gestión del Riesgo, Dirección de Sistemas y Dirección Técnica Contractual y Administrativa
18	Procedimiento de Gestión de Incidentes de Seguridad de la Información	La Oficina Gestión del Riesgo y Dirección de Sistemas
19	Plan de Continuidad del Negocio	Equipo de manejo de crisis

3.3 Fase de Implementación

En esta fase se llevará a cabo la implementación del Modelo de Seguridad de la Información y Ciberseguridad, el cual fue planeado en la fase de planificación.

3.4 Fase de Evaluación de Desempeño

Una vez implementados los instrumentos el Modelo de Seguridad de la Información y Ciberseguridad se procede a evaluar para medir la efectividad de las acciones tomadas a través de indicadores, los cuales deberán ser definidos en la fase de implementación.

El proceso de seguimiento y monitoreo del MSIC se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



3.5 Fase de Mejora Continua

En esta fase el Instituto deberá consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad de la información y ciberseguridad, tomando las acciones oportunas para mitigar las debilidades identificadas.

4. PLAN DE IMPLEMENTACIÓN DEL MSIC Y PROTECCIÓN DE DATOS PERSONALES

Teniendo en cuenta que la organización se enfrenta a amenazas relativas a la seguridad, en especial relacionados con el fraude asistido por computadores, como también a las acciones de personas, los cuales cada vez se han vuelto más comunes, ambiciosos y sofisticados. A continuación, se describen los principales objetivos específicos:

5. Establecer y capacitar al personal de INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA en seguridad de la información, buscando el aumento en la cultura, así como en el compromiso con la adopción de buenas prácticas, el reporte de incidentes de seguridad y la identificación de riesgos.
6. Minimizar los incidentes de seguridad de la información presentados en INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA IDEA.
7. Mantener los sistemas y los recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
8. Establecer los fundamentos para el desarrollo y la implantación de un Modelo de Seguridad de la información.
9. Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
10. Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.
- 11.

Las siguientes son las acciones necesarias que se trazan para cumplir con los mecanismos para la gestión de protección de datos personales, que el IDEA desarrollará antes del 31 de diciembre del 2021:

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTIÓN	ACTIVIDAD	RESPONSABLE DE ACTIVIDAD	FECHA A CUMPLIR
Protección de Datos Personales	"Firmar los consentimientos y los contratos de confidencialidad	Gestión Humana	Marzo 30 de 2021
Gestión de Activos de Información	Implementar una herramienta tecnológica que permita etiquetar la información clasificada y reservada.	Oficina Gestión del Riesgo y Dirección de Sistemas	Abril de 2021
Protección de Datos Personales	Contar con ejemplar en medio impreso de la política de protección de datos personales al ingreso de la entidad, asegurando así la posibilidad de acceso a la misma por parte del público en cumplimiento al artículo 2.2.2.25.3.1 sección 3 Capítulo 25 de Decreto 1074 de 2015 (artículo 13 del Decreto 1377 de 2013).	Oficina de Comunicaciones	Abril de 2021
Gestión de Incidentes	Desarrollar un nuevo procedimiento de Gestión de Incidentes de seguridad de la información y ciberseguridad.	Oficina Gestión del Riesgo y Dirección de Sistemas	Abril 2021
Protección de Datos Personales	Realizar un ciclo de capacitaciones sobre el Sistema de Gestión en Protección de Datos Personales para compartir con todos los funcionarios las políticas y los procedimientos exigidos por la Ley 1581 de 2012 y conozcan a quien acudir en caso de consultas o reclamos de los Titulares, evitando así dar respuestas indebidas o no autorizadas que puedan desconocer el debido proceso	Oficina de Comunicaciones Oficial de Protección de Datos Oficina Gestión del Riesgo	Junio 30 de 2021
Protección de Datos Personales	Incluir en la capacitación de ingreso para los nuevos funcionarios la información sobre las políticas internas de protección de datos y medidas de seguridad establecidas por la empresa para la protección de la información y la documentación.	Dirección de Gestión Humana Oficial de Protección de Datos	Junio 30 de 2021
Seguridad de la Información y Ciberseguridad	Implementar un Centro de Operaciones de Seguridad que permita monitorizar los sistemas de información y la plataforma tecnológica.	Oficina Gestión del Riesgo y Dirección de Sistemas	Julio de 201
Plan de Sensibilización	Sensibilizar a todos los empleados del Instituto en temas relacionados con seguridad de la información y ciberseguridad.	Oficina Gestión del Riesgo	Agosto
Activos de Información	Actualizar el inventario de activos de información con cada dependencia y propietario de la información. Actualizar la criticidad de la información de acuerdo a la normatividad.	Centro de Administración Documental, Oficina Gestión del Riesgo y Oficial de Datos Personales	Septiembre de 2021
Protección de Datos Personales	Gestionar de carácter urgente la suscripción de los contratos de transmisión	Oficial de Protección de Datos	Octubre 30 de 2021

PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	de datos con los Encargados del Tratamiento (Terceros a los que se les suministra o tienen acceso a la información de la compañía para la prestación de un servicio, ejemplo, revisores fiscales o contadores cuando son externos, etc.). En este caso, se trata de una obligación legal contenida en el artículo 2.2.2.25.5.2. del Decreto compilatorio 1074 de 2015 (Artículo 25 del Decreto reglamentario 1377 de 2013).	Subgerencia Administrativa Centro Administrativo Documental	
Política de Seguridad de la Información y Ciberseguridad	Actualizar la Política de Seguridad de la Información y Ciberseguridad.	Oficina Gestión del Riesgo y la Dirección de Sistemas	Noviembre de 2021
Protección de Datos Personales	Tener presente el procedimiento establecido en el Documento Interno de Políticas de Seguridad para reportar los incidentes que sobre la información personal ocurran, toda vez que, los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de administrar las bases de datos o al Oficial de Protección de Datos, quienes se encargarán de su gestión y resolución.	"Oficial de Protección de Datos	Diciembre 30 2021
Protección de Datos Personales	Continuar realizando el registro de entradas y salidas de la documentación como control de trazabilidad para la información física.	Subgerencia Administrativa	Diciembre 30 2021
Comité de Seguridad de la Información y Ciberseguridad	Aprobar los procedimientos, guías y manuales del Modelo de Seguridad de la Información y Ciberseguridad, participar en la formulación y evaluación de planes para mitigar y/o eliminar riesgos.	Comité	Bimestral
Protección de Datos Personales	Estar atentos a cualquier requerimiento que realice la Superintendencia de Industria y Comercio en materia de protección de datos personales y Nueva Normatividad	"Oficial de Protección de Datos	Permanentemente
Protección de Datos Personales	Revisar de manera periódica el canal de atención electrónico que dispusieron para la recepción de consultas y reclamos en materia de protección de datos personales, tal como se viene haciendo actualmente.	Oficina de Comunicaciones Oficial de Protección de Datos Oficina Asesora de Planeación	Permanentemente