IDIPRON

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EL IDIPRON

Vr. 09; 13/03/2024

TABLA DE CONTENIDO

1. OBJETIVO

Establecer lineamientos, procedimientos y controles para salvaguardar la seguridad y privacidad de la información gestionada por EL IDIPRON, asegurando su disponibilidad, integridad, confidencialidad y trazabilidad. De esta manera, se busca mitigar riesgos asociados al manejo de activos de información y garantizar el cumplimiento normativo

2. ALCANCE

Este plan abarca todos los procesos, sistemas, recursos tecnológicos y humanos relacionados con la gestión de la información en el Instituto Distrital para la Protección de la Niñez y la Juventud (EL IDIPRON). Incluye la protección de datos almacenados, procesados y transmitidos en todos los entornos operativos, ya sean físicos o digitales.

2.2. El alcance comprende:

- **Procesos institucionales:** Todas las actividades relacionadas con la recolección, almacenamiento, procesamiento, transmisión, uso, y eliminación de la información, asegurando su integridad, confidencialidad, disponibilidad y trazabilidad.
- **Infraestructura tecnológica:** Los sistemas de información, bases de datos, redes, equipos tecnológicos y software utilizados para la gestión de datos en la entidad, así como su interconexión con sistemas externos.
- **Recursos humanos:** Los/ las funcionarios(as), contratistas, proveedores(as) y cualquier otra persona que tenga acceso a la información de EL IDIPRON, enfatizando su capacitación, sensibilización y compromiso con la seguridad y privacidad de la información.
- **Entornos operativos:** Todos los espacios en los que se maneje información, incluyendo oficinas administrativas, centros de datos, plataformas en la nube, y cualquier otra ubicación donde se almacene o procese información institucional.
- **Información sensible y confidencial:** Todos los datos relacionados con menores de edad, beneficiarios, expedientes, registros administrativos, y demás información crítica que sea manejada por EL IDIPRON en cumplimiento de su misión.

Este plan es aplicable a toda la entidad y a cualquier actividad o proyecto que implique la gestión de información, alineándose con la normativa vigente, las políticas internas de EL IDIPRON, y estándares internacionales de seguridad y privacidad de la información

3. CONDICIONES GENERALES

Desde la Oficina de TIC se Garantiza el cumplimiento normativo, alineándose con leyes como es la Ley 1581 de 2012 y promoviendo la actualización frente a cambios regulatorios. Es deber de los/las lideres de oficinas, subdirectores, gerentes y responsables de los procesos, como primera línea de defensa

garantizar la aplicación a toda la institución, incluyendo personal, contratistas y proveedores (as), bajo un esquema de roles claros y responsabilidad compartida. El plan asegura la confidencialidad, integridad y disponibilidad de la información, implementa una gestión activa de riesgos, fomenta la mejora continua mediante auditorías y actualizaciones tecnológicas, y prioriza la capacitación del personal para crear una cultura de seguridad. Asimismo, protege información sensible, especialmente de menores, y asegura una gobernanza alineada con políticas de Gobierno Digital, garantizando sostenibilidad y transparencia institucional.

4. GLOSARIO

Término	Definición
Acceso autorizado	Permiso otorgado a un usuario, sistema o proceso para utilizar recursos específicos de información según los lineamientos establecidos
Auditoría de seguridad	Proceso sistemático de revisión y evaluación de la efectividad de las políticas, controles y procedimientos de seguridad en la organización
Confidencialidad	Propiedad que garantiza que la información solo esté disponible para personas, entidades o procesos autorizados
Disponibilidad	Capacidad de la información de estar accesible y usable por los usuarios autorizados cuando se necesite
Gestión de riesgos	Proceso de identificar, evaluar y mitigar riesgos relacionados con la seguridad de la información para minimizar posibles impactos
Gobierno Digital	Conjunto de políticas y estrategias que buscan modernizar y transformar la gestión pública mediante el uso de tecnologías de la información
Integridad	Propiedad que asegura que la información se mantiene completa, precisa y sin alteraciones no autorizadas durante su ciclo de vida
Ley 1581 de 2012	Normativa colombiana que regula la protección de datos personales y establece derechos y obligaciones en el tratamiento de dicha información
Política de seguridad	Conjunto de directrices, principios y normas adoptadas para garantizar la protección y gestión adecuada de los activos de información de una organización
Riesgo	Posibilidad de que una amenaza aproveche una vulnerabilidad, causando un impacto negativo en la seguridad de la información

Vulnerabilidad	Debilidad o fallo en un sistema, proceso o control que puede ser explotado por una amenaza para comprometer la seguridad de la información

5. DESCRIPCIÓN O CONTEXTO DEL DOCUMENTO

Este documento expone el Plan de Seguridad y Privacidad de la Información del Instituto Distrital para la Protección de la Niñez y la Juventud (EL IDIPRON), que tiene como propósito principal definir un marco integral de lineamientos, estrategias y controles diseñados para proteger la información institucional contra posibles amenazas internas y externas. Este marco garantiza la confidencialidad, integridad, y disponibilidad de los datos, además de asegurar el cumplimiento de las obligaciones legales relacionadas con la privacidad de la información.

El plan busca fomentar una cultura organizacional orientada a la seguridad de la información, promoviendo buenas prácticas y el compromiso activo de todos los colaboradores de la entidad en la gestión segura de los activos de información. Así mismo, se asegura de alinear sus directrices con las normativas nacionales, como la Ley Estatutaria 1581 de 2012 sobre Protección de Datos Personales, el Decreto 1377 de 2013, y con estándares internacionales reconocidos, como la ISO/IEC 27001 de sistemas de gestión de seguridad de la información.

De esta manera, el presente plan se constituye en una herramienta clave para fortalecer la confianza en el manejo de la información sensible y asegurar la continuidad de las operaciones de EL IDIPRON en un entorno digital cada vez más complejo y desafiante.

6. NORMATIVIDAD

El Plan de Seguridad y Privacidad se fundamenta en las siguientes normativas:

- Ley 1581 de 2012: Ley de Protección de Datos Personales.
- Decreto 1377 de 2013: Reglamentación de la Ley 1581.
- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC.
- Resolución 500 de 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.”
- Decreto 338 marzo 8 de 2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y

se dictan otras disposiciones"

- Resolución 746 marzo 11 de 2022 "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
- Decreto 767 mayo 16 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- ISO/IEC 27001 e ISO/IEC 27701: Estándares internacionales sobre seguridad de la información y privacidad.

7. DOCUMENTOS ASOCIADOS

El Plan de Seguridad y Privacidad de la Información de EL IDIPRON se sustenta en un conjunto de documentos estratégicos y operativos que garantizan un enfoque integral para la gestión segura de la información institucional. Estos documentos reflejan el compromiso de la entidad con la protección de los datos, estableciendo directrices claras, procedimientos estandarizados y mecanismos efectivos de respuesta ante posibles riesgos y contingencias.

7.2. Principales documentos asociados

- **Manual de políticas de seguridad y ciberdefensa:** Define las directrices generales para proteger los activos tecnológicos de la entidad frente a amenazas cibernéticas, asegurando la integridad, disponibilidad y confidencialidad de la información.
- **Política de tratamiento de datos personales:** Establece reglas claras para el manejo responsable de los datos personales, en cumplimiento con las normativas vigentes y el respeto a los derechos de los titulares de la información.
- **Política de copia de seguridad y respaldo:** Detalla los procedimientos para la creación y gestión de copias de seguridad, garantizando la disponibilidad y recuperación de datos críticos en caso de incidentes.
- **Plan de contingencia TIC:** Proporciona las acciones preventivas, correctivas y estrategias de recuperación ante eventos que comprometan la continuidad operativa de los servicios tecnológicos.
- **Plan de contingencia para la no disponibilidad de la página Web:** Define las medidas para restaurar rápidamente el servicio de la página web en caso de caídas o ataques, asegurando el acceso continuo a la información pública.
- **Plan de tratamiento de riesgos de seguridad y privacidad de la información:** Identifica, evalúa y prioriza los riesgos asociados con la gestión de información, estableciendo estrategias para mitigar su impacto.

Estos documentos, actualizados periódicamente, constituyen el marco normativo y operativo del Plan de Seguridad y Privacidad de la Información, fortaleciendo la resiliencia de EL IDIPRON frente a los

desafíos tecnológicos.

8. ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EL IDIPRON ha avanzado en la consolidación de un sistema robusto para la gestión de seguridad y privacidad de la información, alineado con las normativas legales y estándares internacionales. Este sistema cuenta con herramientas clave que permiten:

- La implementación de buenas prácticas en seguridad informática.
- La capacitación continua del personal.
- La integración de nuevas tecnologías para responder a un entorno dinámico.

9. COMPONENTES DEL PLAN

Los principales componentes del Plan de Seguridad y Privacidad de la Información se basan en elementos claves que permiten una gestión integral de los riesgos asociados. Este sistema se sustenta en políticas y planes específicos que abarcan aspectos como la ciberseguridad, el tratamiento de datos personales, la gestión de copias de seguridad y las estrategias de contingencia. Estas acciones reflejan el compromiso institucional con la protección de la información y la garantía de la continuidad operativa.

9.2. Plan de contingencia tic y página WEB

Procedimientos detallados para garantizar la continuidad operativa de los servicios tecnológicos y la página web institucional en caso de fallos, ataques o desastres.

9.3. Políticas de seguridad y ciberdefensa

Directrices para prevenir, mitigar y responder a riesgos cibernéticos, protegiendo sistemas, redes y datos.

9.4. Política de tratamiento de datos personales

Lineamientos para la recolección, almacenamiento, uso y eliminación de datos personales, respetando las normativas legales.

9.5. Política de copia de seguridad y respaldo

Normas para la creación de copias de seguridad que garanticen la recuperación de datos críticos ante incidentes.

9.6. Plan de tratamiento de riesgos

Identificación y mitigación de riesgos prioritarios relacionados con la seguridad y privacidad de los activos de información.

La implementación eficiente de estos componentes, sumada al monitoreo constante y la actualización periódica, asegura que EL IDIPRON pueda enfrentar los retos de un entorno en constante evolución tecnológica.

10. ROLES Y RESPONSABILIDADES

- **Comité Institucional de Gestión y Desempeño:** Es responsable de apoyar la gestión de recursos financieros, administrativos, iniciativas y proyectos, revisar y aprobar el Plan de Seguridad de la Información y de promover el compromiso y participación de funcionarios(as) públicos(as) y contratistas del IDIPRON.
- **Jefe de la Oficina de Tecnologías de la Información:** Lidera la gestión de seguridad y privacidad, supervisando la implementación de controles, gestionando incidentes y promoviendo capacitaciones.
- **Equipo de Tecnologías de la Información:** Implementa medidas técnicas y operativas en línea con las políticas definidas.
- **Todos los servidores públicos:** Cumplen con las políticas establecidas y reportan incidentes de seguridad.

11. NORMATIVIDAD INTERNA

- Instalación y actualización de software y hardware.
- Desarrollo y mantenimiento de sistemas.
- Copia y respaldo de información crítica.
- Gestión de accesos y monitoreo de eventos.

12. CUMPLIMIENTO LEGAL

El cumplimiento de las normativas legales es fundamental para asegurar que IDIPRON gestione adecuadamente la seguridad y privacidad de la información. Para ello, se tomarán las siguientes acciones:

- **Identificación de normativas aplicables:** Se realizará un proceso de mapeo para identificar y garantizar el cumplimiento con las normativas nacionales e internacionales relevantes, como la Ley 1581 de 2012 y el Decreto 1377 de 2013, que regulan la protección de datos personales en Colombia. Además, se alineará la entidad con estándares internacionales como la ISO/IEC 27001 (gestión de seguridad de la información) y la ISO/IEC 27701 (gestión de privacidad de la información). En caso de operar con ciudadanos de la Unión Europea, también se tendrá en cuenta el cumplimiento con el Reglamento General de Protección de Datos (GDPR).
- **Auditorías de cumplimiento legal:** Se llevarán a cabo auditorías internas anuales y auditorías externas cuando sea necesario, para verificar que la entidad cumple con las normativas vigentes y para evaluar la eficacia de los controles implementados. Estas auditorías se enfocarán especialmente en la protección de datos personales y la seguridad de la información.
- **Actualización ante cambios regulatorios:** Se implementará un proceso de vigilancia

regulatoria, que permitirá detectar cualquier cambio normativo relevante. Esto garantizará que las políticas de seguridad y privacidad se actualicen de manera continua para cumplir con las nuevas disposiciones legales.

- **Mecanismos de transparencia:** Con el fin de fomentar la confianza y la transparencia, IDIPRON publicará informes periódicos sobre el cumplimiento de las normativas legales en materia de seguridad y privacidad. Estos informes serán accesibles para el público y proporcionarán detalles claros sobre cómo se gestionan los datos personales y cómo se protegen los derechos de los usuarios.
- **Gestión de incidentes de seguridad:** En caso de incidentes de seguridad, se cumplirán los plazos establecidos por las normativas legales, como los requeridos por la Ley 1581 de 2012 y las directrices del GDPR. Esto incluye la notificación oportuna de cualquier brecha de seguridad que afecte a los datos personales, así como la implementación de protocolos de respuesta y mitigación adecuados.

13. PLAN DE ACCIÓN

ACCIÓN	DESCRIPCIÓN	DETALLES ESPECÍFICOS
1. Actualizar políticas de seguridad	Revisión y actualización de las políticas actuales de seguridad.	Revisar aspectos críticos: gestión de acceso, uso de dispositivos personales y teletrabajo.
		Alinear con normativas nacionales (Ley 1581 de 2012, Decreto 1377 de 2013) y estándares internacionales (ISO/IEC 27001).
		Elaborar anexos específicos para temas emergentes (teletrabajo, ciberseguridad básica) sin rehacer completamente las políticas.
2. Implementar controles basados en el análisis de riesgos	Establecer controles para mitigar riesgos identificados.	Realizar evaluaciones de riesgos semestrales utilizando análisis FODA.
		Implementar controles básicos de alta prioridad, como contraseñas robustas, configuración de permisos, y cifrado básico.
		Establecer protocolos manuales para responder a riesgos críticos, como incidencias de malware.
3. Capacitar al personal regularmente	Diseñar e implementar un plan de capacitación sobre ciberseguridad y privacidad.	Capacitar sobre ciberseguridad, identificación de phishing y manejo responsable de datos personales.
		Realizar simulacros de incidentes cibernéticos, como phishing.
		Publicar boletines mensuales con consejos prácticos sobre seguridad.
4. Monitorear la eficacia de las medidas implementadas	Establecer un sistema de monitoreo para evaluar la	Realizar revisiones trimestrales de incidentes y alertas.
		Revisiones internas semestrales con listas de verificación simplificadas.

	efectividad de las políticas y controles.	Implementar métricas accesibles: número de incidentes reportados, tasa de cumplimiento de políticas, participación en capacitaciones.
		Documentar hallazgos y ajustar estrategias según prioridades identificadas.

14. PRIORIZACIÓN Y SEGUIMIENTO

Para maximizar el impacto se establecen las siguientes acciones:

- **A corto plazo:** Actualizar las políticas clave, capacitar al personal en conceptos básicos y establecer controles.
- **A mediano plazo:** Consolidar los protocolos de monitoreo y ajustar acciones según los riesgos emergentes y resultados obtenidos.

15. MONITOREO Y EVALUACIÓN

El monitoreo en el contexto de seguridad y privacidad de la información consiste en la supervisión constante de los sistemas, procesos y controles implementados para proteger los datos y activos tecnológicos de la entidad. Su objetivo es detectar incidentes de seguridad, evaluar la eficacia de las medidas adoptadas y asegurar el cumplimiento de las políticas establecidas. A través de indicadores clave de desempeño (KPIs), auditorías periódicas y análisis post-incidente, el monitoreo permite identificar vulnerabilidades y áreas de mejora. Además, facilita la toma de decisiones informadas para ajustar estrategias y políticas, garantizando la protección continua de la información.

KPI	Descripción	Alcance	Fórmula
Número de incidentes reportados	Mide la cantidad de incidentes de seguridad reportados durante un período determinado.	Evaluar la frecuencia y gravedad de los incidentes de seguridad en la entidad.	Número de incidentes / Período de tiempo.
Tiempo promedio de respuesta	Mide la eficiencia en la respuesta a los incidentes, desde su detección hasta su resolución.	Evaluar la rapidez en la resolución de incidentes de seguridad.	Suma de tiempos de resolución de incidentes / Número total de incidentes.
Cumplimiento de auditorías internas	Evalúa el nivel de conformidad con las políticas y procedimientos de seguridad durante las auditorías.	Verificar la adherencia a las políticas de seguridad de la información y normativas internas.	Número de auditorías conformes / Número total de auditorías.
Evaluación de impacto en la privacidad	Mide la aplicación de evaluaciones de impacto cuando se producen	Asegurar que los cambios en el manejo de datos personales	Número de PIAs realizadas / Número de cambios relevantes en el tratamiento de datos

(PIAs)	cambios significativos en el tratamiento de datos personales.	sean evaluados adecuadamente para prevenir riesgos.	personales.

16. DIVULGACIÓN Y COMUNICACIÓN DEL PLAN

La correcta divulgación y comunicación del plan de seguridad y privacidad es esencial para asegurar que todo el personal de IDIPRON esté informado y comprometido con las medidas establecidas. Para ello, se implementará una estrategia de comunicación interna que incluirá:

- **Capacitación presencial y virtual:** Se organizarán sesiones de formación tanto presenciales como en línea para todo el personal, con el objetivo de asegurar que cada empleado comprenda el contenido del plan, sus responsabilidades y las acciones que debe llevar a cabo para cumplir con las políticas de seguridad y privacidad. Las capacitaciones se adaptarán a los diferentes niveles de conocimiento y funciones del personal.
- **Boletines informativos internos:** Se enviarán boletines informativos periódicos que resuman las principales políticas, cambios normativos y buenas prácticas relacionadas con la seguridad y la privacidad de la información. Estos boletines serán un recurso accesible para todo el personal, promoviendo la actualización constante sobre el estado del plan y cualquier cambio relevante.
- **Publicaciones en canales oficiales de comunicación:** Se utilizarán los canales oficiales de comunicación interna (como el intranet institucional, correo electrónico y plataformas de colaboración) para mantener a todo el personal informado de manera continua. Las actualizaciones periódicas sobre el estado del plan de seguridad y privacidad serán compartidas de manera clara y accesible, promoviendo una cultura organizacional consciente de la importancia de la protección de datos.

17. INFORMES

El responsable de la gestión de seguridad tendrá la responsabilidad de presentar informes periódicos ante el nivel directivo, asegurando que la alta dirección esté constantemente informada sobre el avance del plan y los resultados obtenidos. Los informes incluirán los siguientes aspectos:

- **Avances en la implementación:** Se detallarán los progresos alcanzados en la implementación de las políticas de seguridad y privacidad, así como el cumplimiento de las metas establecidas en el plan de acción. Esto incluirá la implementación de controles, procesos de capacitación, y los resultados de las auditorías internas y externas realizadas.
- **Incidentes relevantes y su tratamiento:** El informe incluirá un resumen de los incidentes de seguridad más relevantes ocurridos durante el periodo de reporte, detallando las medidas adoptadas para su resolución y el impacto que estos pudieron haber tenido en la seguridad de la información. Así mismo, se indicará cómo se gestionaron dichos incidentes y qué medidas correctivas se implementaron para evitar su recurrencia.
- **Recomendaciones para la mejora continua:** Basado en el análisis de los resultados obtenidos y los incidentes registrados, se proporcionarán recomendaciones prácticas para la mejora continua

de las políticas y procedimientos de seguridad y privacidad. Estas recomendaciones podrán estar orientadas a la actualización de controles, refuerzo de la capacitación del personal o ajustes en las prácticas de monitoreo y respuesta ante incidentes.

Este informe no solo facilitará la toma de decisiones dentro de la alta dirección, sino que también permitirá ajustar las estrategias de seguridad y privacidad según las necesidades y retos identificados, contribuyendo al fortalecimiento continuo del sistema de protección de datos de la entidad.

18. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se crea el plan de seguridad y de la información del IDIPRON, con el objetivo de establecer lineamientos, procedimientos y controles que permitan salvaguardar la privacidad de la información gestionada por el Instituto Distrital para la Protección de la Niñez y la Juventud - IDIPRON, alineándolo a la estrategia tecnológica para el periodo 2025 -2027, al plan de desarrollo distrital (Bogotá Camina segura 2024 – 2027) y a la plataforma estratégica de la entidad.	27/12/2024	**SANDRA PATRICIA GUERRERO RAMIREZ** Ing. Gobierno Digital Oficina De Tic

19. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	WILSON ANDRES JIMENEZ RAMIREZ	ING. PROFESIONAL DE LA OFICINA DE TIC	27/12/2024
	YEIMMY ROCIO CARDENAS CRUZ	TÉCNICO OPERATIVO CÓDIGO 314 GRADO 03	27/12/2024
APROBACIÓN LÍDER DE PROCESO	LUIS CARLOS OCAMPO RAMOS	JEFE DE OFICINA DE TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES	27/12/2024