IDRD

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficina de Transformación Digital y Tecnologías de la Información

2025

1. PRESENTACIÓN

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El plan estratégico de seguridad y privacidad de la información establece los objetivos necesarios para proteger los datos, garantizando su confidencialidad, integridad, disponibilidad, autenticidad y no repudio. Estos objetivos se alcanzan mediante diversas iniciativas y proyectos estratégicos orientados a fortalecer la gestión de la seguridad.

2. INTRODUCCIÓN

La información constituye un activo fundamental para la organización, al igual que otros recursos clave del negocio, y por ello requiere una protección adecuada. Esta necesidad se vuelve aún más crítica en un entorno cada vez más interconectado, donde el intercambio constante de datos incrementa la exposición a múltiples amenazas y vulnerabilidades.

La información puede presentarse en múltiples formatos: impresa o escrita en papel, almacenada en medios electrónicos, transmitida por correo o medios digitales, mostrada en imágenes o películas, o comunicada verbalmente. Independientemente de su forma o del canal utilizado para compartirla o almacenarla, debe contar siempre con una protección adecuada.

La seguridad de la información consiste en salvaguardar estos activos frente a diversas amenazas, con el objetivo de garantizar la continuidad operativa, reducir los riesgos y optimizar tanto el retorno de las inversiones como el aprovechamiento de oportunidades.

3. JUSTIFICACIÓN

Establecer, implementar y dar seguimiento al plan de seguridad y privacidad de la información en el Instituto Distrital de Recreación y Deportes IDRD, facilitará una toma de decisiones oportuna, orientada a garantizar la seguridad y privacidad de la información de forma adecuada.

4. OBJETIVOS

Este documento tiene como objetivo establecer el Plan de Seguridad y Privacidad de la Información del IDRD. Su finalidad es permitir el seguimiento continuo a la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG).

Asimismo, define las responsabilidades relacionadas con la formulación, ejecución, monitoreo y mejora de las políticas institucionales en materia de seguridad de la información. También proporciona orientación a funcionarios, contratistas y terceros sobre el uso responsable y seguro de los activos de información y de la infraestructura tecnológica que soporta la operación institucional.

El Plan de Seguridad y Privacidad de la Información busca preservar la confidencialidad, integridad y disponibilidad de la información, garantizando la protección de los datos y generando confianza en su gestión.

Objetivo General

Diseñar, desarrollar e implementar un conjunto de lineamientos y buenas prácticas en seguridad y privacidad de la información, alineados al MSPI y al plan institucional, con el fin de fortalecer el aseguramiento de los servicios de TI y salvaguardar los datos e información de los procesos y usuarios de la entidad para la vigencia 2025.

5. ALCANCE

El Plan de Seguridad y Privacidad de la Información es aplicable a la definición, implementación, mantenimiento y mejora de los lineamientos, directrices, políticas y controles necesarios para que el Instituto Distrital de Recreación y Deporte – IDRD mantenga niveles adecuados de seguridad sobre sus activos de información, para el año 2025.

6. DEFINICIONES

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, dentro de los cuales se puede mencionar:
  - Información.
  - Software.
  - Recursos físicos.
  - Servicios.
  - Personas y sus cualificaciones, habilidades y experiencias.
  - Elementos intangibles como la reputación y la imagen.

- **Activo de Información:** Es cualquier dato, documento, registro, conocimiento, sistema, medio tecnológico o recurso que almacena, procesa, transmite o soporta información y que tiene valor para la organización. Estos activos son fundamentales para el funcionamiento institucional y deben ser protegidos adecuadamente para garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Causas:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control:** Medida que permite reducir o mitigar un riesgo. Entiéndase por las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida.

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009) interacción entre usuarios.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos**: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Evaluación del Riesgo:** Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

- **Gestión del riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **Gestión de Incidentes de Seguridad de la Información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Identificación del riesgo:** Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las

necesidades de las partes involucradas.

- **Integridad:** Propiedad de exactitud y completitud

- **Impacto**: Son las consecuencias que genera un riesgo una vez se materialice.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **No repudio:** Es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos posibilidades:

  No repudio en Origen: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío.

  No Repudio en Destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. La posesión de un documento y su firma digital asociada será prueba efectiva del contenido y del autor del documento.

- **Política de Administración de Riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riego.

- **Plan de Tratamiento de Riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Probabilidad:** Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo

- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

- **Riesgo de Seguridad Digital**: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.

- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.

- **Tolerancia al Riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- **Tratamiento del Riesgo:** Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

- **Valoración de Riesgos:** Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

- **Vulnerabilidad:** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

7. RESPONSABILIDADES

La oficina de transformación digital y tecnologías de la información es responsable de realizar seguimiento, actualización, mantenimiento y mejora del plan de seguridad y privacidad de la información del IDRD.

7.1. ROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL IDRD

Dirección General

- Aprobar y respaldar el Plan de Seguridad de la Información.
- Asignar los recursos necesarios (humanos, financieros y tecnológicos).
- Fomentar la cultura de seguridad en todos los niveles de la organización.
- Garantizar el cumplimiento de los requisitos legales y normativos.

Oficial de Seguridad de la Información (CISO o equivalente)

- Liderar la formulación, implementación y mejora continua del Plan de Seguridad.
- Coordinar la gestión de riesgos de seguridad de la información.
- Definir políticas, estándares y procedimientos de seguridad.
- Realizar seguimiento al cumplimiento del SGSI (Sistema de Gestión de Seguridad de la Información).
- Reportar incidentes de seguridad de la información.

Responsables de Procesos / Líderes de Área

- Implementar las políticas de seguridad dentro de sus áreas.
- Asegurar que los controles de seguridad estén operativos y sean efectivos.
- Promover el uso seguro de los recursos de información por parte de sus equipos.
- Notificar cualquier incidente o vulnerabilidad detectada.

Usuarios (Colaboradores y Terceros)

- Cumplir con las políticas y procedimientos de seguridad de la entidad.
- Proteger la información y los recursos tecnológicos que utilizan.
- Reportar comportamientos sospechosos, incidentes o brechas de seguridad.
- Participar en programas de capacitación y concientización sobre seguridad.

La Oficina de Transformación Digital y Tecnologías de la Información

- Aplicar controles técnicos (firewalls, antivirus, backups, cifrado, etc.).
- Asegurar la disponibilidad, integridad y confidencialidad de los sistemas y redes.
- Monitorear, registrar y responder a eventos e incidentes de seguridad.
- Coordinar la gestión de identidades y accesos.

Auditoría Interna

- Evaluar la efectividad del SGSI y el cumplimiento de políticas de seguridad.
- Recomendar mejoras para fortalecer la postura de seguridad de la entidad.
- Realizar auditorías periódicas a los procesos relacionados con la seguridad de la información.

Comité Institucional de Gestión y Desempeño del Instituto Distrital de Recreación y Deporte – IDRD

- Servir como órgano consultivo y de coordinación en materia de seguridad de la información.
- Apoyar en la priorización de acciones, gestión de riesgos y toma de decisiones estratégicas.
- Supervisar los planes de mejora y la gestión de incidentes relevantes.

7.1.1. Responsable del tratamiento de los datos personales

En cumplimiento de los lineamientos establecidos en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, y la Política de Tratamiento de Datos Personales, se define como responsable del tratamiento de datos personales el IDRD.

7.1.2. Equipo de Gestión

El equipo de gestión del proyecto se encarga de tomar las medidas para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad y Privacidad de la Información, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

7.2. Roles y Responsabilidades Equipo de Gestión

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes

de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal, y que no dependa exclusivamente de la Oficina de Transformación Digital de Tecnologías de la Información.

7.2.1. Administrador Infraestructura Tecnológica

Garantizar la continuidad en la prestación de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la entidad, a través de la administración (configuración, pruebas, puesta en operación, migración, actualización, mantenimiento), de la infraestructura tecnológica IT, que soportan la operación informática institucional.

Responsable: La oficina de transformación digital y tecnologías de la información
Apoyo: Proveedores y terceros

7.2.2. Seguridad Informática

Buscar el aseguramiento de la información institucional digital, creada, procesada, modificada y alojada en la infraestructura tecnológica de la entidad, a través de la definición e implementación del sistema de gestión de seguridad de la información SGSI, modelo de seguridad y privacidad de la información MSPI, seguimiento, monitoreo, mantenimiento y mejora continua de los controles, lineamientos y directrices de seguridad informática en concordancia con las normas técnicas internacionales como por ejemplo IEC NTC-ISO 27001:2022 y normatividad vigente y aplicable.

Responsable: La oficina de transformación digital y tecnologías de la información
Apoyo: Proveedores y terceros

7.2.3. Administrador Redes de Comunicaciones

Los servicios informáticos, red de datos y de comunicaciones deben contar con altos niveles de disponibilidad, que se reflejan en oportunidad de la información institucional de manera eficiente y efectiva, para lo cual se debe gestionar el recurso humano calificado para adelantar actividades de administración, configuración, mantenimiento y operación de los equipos de comunicaciones de la entidad. Es responsabilidad del administrador de las redes de datos (networking) y los equipos que la soportan, implementar, mantener y mejorar las mejores prácticas y estándares para la gestión de infraestructura tecnológica.

El administrador de redes debe ejecutar las acciones necesarias asociadas a la continuidad en la prestación de los servicios informáticos en la entidad, adelantando tareas de respaldo de la configuración de los equipos activos, así como gestionar garantías sobre los activos de infraestructura tecnológica clasificados y valorados como críticos.

Se deben proponer alternativas de operación en caso de materialización de incidentes de seguridad que comprometan total o parcialmente la operación informática.

Responsable: Profesional de la oficina de transformación digital y tecnologías de la información
Apoyo: Proveedores y terceros

7.2.4. DBA- Administrador de Bases de Datos

Garantizar la protección de los datos creados, procesados y/o modificados que se encuentran alojados en los sistemas de información de la entidad, a partir de la implementación, mantenimiento y mejora de controles de seguridad que permitan niveles apropiados de integridad y confiabilidad de la información resultado de la operación informática misional de la entidad.

La responsabilidad en la administración de las bases de datos misionales de la entidad es asumida desde la oficina de transformación digital y tecnologías de la información, considerando como críticos las tareas de procesamiento y manejo de la información institucional usada en la toma de decisiones encaminadas al cumplimiento de metas, objetivos y la misión del IDRD.

El administrador de las bases de datos debe garantizar que exista una única fuente de información institucional, para lo cual se establecerá un único sistema de reportes misional. La asignación de un único DBA en el IDRD, permite a la entidad contar con niveles de confiabilidad de la información reportada ante entes de control, reportes de metas y demás instancias que lo requieran.

Responsable: Profesional de la oficina de transformación digital y tecnologías de la información
Apoyo: Proveedores y terceros

7.2.5. Administración Sistema de Información Misional – SIM

Uno de los logros de la Política de Gobierno Digital, se relaciona con los sistemas de información y busca potenciar los procesos y servicios que presta la entidad a través de la gestión de los sistemas de información SIM (Sistema de información Misional).

Es responsabilidad del administrador de la herramienta misional SIM de registro y gestión de deportistas y escenarios, contar con la documentación debidamente actualizada y controlada, teniendo en cuenta los lineamientos de seguridad de la información para la publicación de documentos y requisitos del modelo integrado de planeación y gestión.

Responsable: Profesional de la oficina de transformación digital y tecnologías de la información

Apoyo: Proveedores y terceros

7.2.6. Administrador Sistemas de Información Administrativo

La oficina de transformación digital y tecnologías de la información designará a los responsables de la administración, configuración y puesta en operación (cuando sea requerido) de los aplicativos que apoyan los procesos administrativos de la entidad, como nómina, inventarios, almacén y tesorería entre otros.

El administrador de los sistemas de información administrativo es responsable de realizar seguimiento a la documentación requerida para su configuración, despliegue y puesta en operación, que permitan la oportuna recuperación frente a la materialización de un evento de seguridad informática que comprometa su operación.

Se deben aplicar procedimientos de copias de respaldo que permitan niveles apropiados de integridad de la información contenida en las bases de datos de los servicios informáticos administrativos, así como la ejecución de simulacros de restauración programados y controlados, que verifiquen la funcionalidad de las copias realizadas, para lo cual el administrador del sistema de información administrativa verificará los recursos (hardware, software y medios) necesarios y realizara la documentación de los resultados.

Importante:

- La oficina de transformación digital y tecnologías de la información es responsable de ejecutar acciones para preservar la disponibilidad de los sistemas de información administrativos, así como de velar por la protección de la información derivada de su uso.
- El uso de las funcionalidades de las herramientas informáticas de apoyo es responsabilidad de los usuarios autorizados.
- Los usuarios son responsables por el manejo que den a las contraseñas asignadas, en cumplimiento de los lineamientos de seguridad de los activos de información del IDRD, evitando exponerla a daño, modificación, destrucción accidental o intencional, robo o alteración.

Responsable: La oficina de transformación digital y tecnologías de la información

7.2.7. Responsable Gestión documental

Desde el proceso de Gestión Documental, se debe velar por la clasificación de la información institucional. El responsable del proceso debe gestionar la implementación de un sistema de gestión documental que permita contar con seguimiento y trazabilidad en el flujo de activos de la información.

Responsable Profesional de la oficina de transformación digital y tecnologías de la información

7.2.8. Control de Documentos – Sistema de Gestión

La Oficina Asesora de Planeación es responsable de garantizar el control de los documentos que consolidan el Sistema de Gestión del IDRD.
De igual forma deberá verificar la estructura y forma de los documentos allegados por las diferentes dependencias de la entidad, antes de avalar la publicación de los mismos.

Responsable: Oficina Asesora de Planeación

7.2.9. Responsable Plan de Sensibilización

Considerando la importancia de generar una cultura alrededor de la seguridad de la información en el Instituto Distrital de Recreación y Deporte - IDRD, desde La oficina de transformación digital y tecnologías de la información, la Oficina Asesora de Comunicaciones y demás áreas delegadas, se debe establecer, actualizar y ejecutar un plan de comunicación que permita a la entidad conocer los lineamientos y directrices relacionadas al SGSI.

Es responsabilidad de la oficina asesora de comunicaciones apoyar el desarrollo de los planes de comunicación del SGSI y MSPI, en el marco de las actividades del IDRD

8. CONDICIONES GENERALES

- Cumplimiento de los lineamientos para la administración de la seguridad y privacidad de la información de la Entidad.
- Cumplimiento a los lineamientos establecidos en la oficina de transformación digital y tecnologías de la información.

9. DESARROLLO DEL PLAN

PLAN MODELO MSPI & CIBERSEGURIDAD

Oficina de Transformación Digital y Tecnologías de la Información

Inicio del proyecto: sá., 2025-02-01

Semana para mostrar: 1

TAREA	ASIGNADO	Avance cuantitativo	Avance Cualitativo	Entregable	INICIO	FIN
MODELO MSPI & CIBERSEGURIDAD		0%				
1. Informe de autodiagnóstico de seguridad de la información		0		Instrumento MSPI	1-2-25	31-12-25
2. Análisis de vulnerabilidades y Pentesting		0		Informes	1-3-25	31-12-25
3. Actualizar manual de políticas de seguridad digital y de la información		0		Manual	1-5-25	31-12-25
4. Plan de Continuidad del Negocio TI y DRP TI		0		2 Planes	1-8-25	31-12-25
5. Capacitaciones y sensibilizaciones		0		Piezas y grabación	1-3-25	31-12-25
6. Actualización de documentación asociada a Seguridad de la Información		0		Isolucion y Documentos	1-2-25	30-9-25
7. Monitoreo de alertas e incidentes presentados		0		Reporte plataforma ZABBIX	1-8-25	31-12-25

10. DESARROLLO

10.1. COMPONENTES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se relacionan puntos críticos, en donde se pueden encontrar los componentes principales del Sistema de Gestión de Seguridad de la Información en la Entidad.

- **Estructura Organizacional de Seguridad de la Información:**

  El Comité Institucional de Gestión y Desempeño del cual hace parte el subcomité de seguridad de la información, El oficial o encargado de seguridad de la información y La oficina de transformación digital y tecnologías de la información, son los responsables de la gestión del sistema, y un conjunto de responsabilidades separadas entre las áreas usuarias para el apropiado apoyo a la gestión de la seguridad de la información en la entidad.

- **Clasificación de Información:**

  Desde La oficina de transformación digital y tecnologías de la información

11. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Política General del Sistema de Gestión de Seguridad de la Información

Política de Seguridad y Privacidad de la Información. Es la declaración general que representa la posición del Instituto Distrital de Recreación y Deporte IDRD respecto a la protección de los activos de información (los funcionarios, contratistas y terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del Instituto y apoyan la implementación del Modelo de Privacidad y Seguridad de la información, mediante la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información. La implementación del plan de Seguridad y Privacidad de la Información 2025, comprende las siguientes actividades:

a. **INFORME DE AUTODIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN**.

- ✓ Identificación de áreas involucradas.
- ✓ Levantamiento de información.
- ✓ Entrevistas.
- ✓ Informe.

b. ANÁLISIS DE VULNERABILIDADES Y PENTESTING.

- ✓ Análisis de vulnerabilidades Aplicativo ORFEO.
- ✓ Análisis de vulnerabilidades Página WEB.
- ✓ Análisis de vulnerabilidades Sistemas de Información.
- ✓ Análisis de vulnerabilidades SSL portales IDRD.

c. ACTUALIZAR MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y DE LA INFORMACIÓN.

- ✓ Actualización del Manual de Políticas.

d. PLAN DE CONTINUIDAD DEL NEGOCIO TI Y DRP TI.

- ✓ Inventario de servicios y aplicaciones de red y hardware.
- ✓ Identificación, Valoración y Clasificación de Activos.
- ✓ Gestión Documental DRP TI.
- ✓ Gestión Documental BCP TI.

e. CAPACITACIONES Y SENSIBILIZACIONES.

- ✓ Protección de datos personales y RNBD.
- ✓ Activos de información y clasificación.
- ✓ Gestión de incidentes, Ingeniería social y phishing.
- ✓ Actualizaciones políticas MSPI.

f. ACTUALIZACIÓN DE DOCUMENTACIÓN ASOCIADA A SEGURIDAD DE LA INFORMACIÓN.

- ✓ FORMATOS.
- ✓ INSTRUCTIVOS.
- ✓ MANUALES.
- ✓ PROCEDIMIENTOS.

- ✓ PLANES.

g. MONITOREO DE ALERTAS E INCIDENTES PRESENTADOS

- ✓ Monitoreo plataforma ZABBIX Alertas presentadas.

12. MEJORAMIENTO

Actualmente EL IDRD, cuenta con documentos para la gestión de la mejora donde se establecen metodologías para determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir los requisitos previstos en el Modelo de Seguridad y Privacidad de la Información. Las fuentes potenciales de oportunidades de mejora para el sistema de seguridad de la información son:

1. Revisión de Controles, políticas o procedimientos del sistema de seguridad de la información.
2. Incidentes de Seguridad de la Información
3. Nueva legislación o los cambios propuestos a la legislación vigente para el MSPI
4. Resultados de las auditorías internas
5. Evaluación y análisis de los resultados de seguimiento y medición
6. Opiniones de las partes interesadas
7. Resultados de la Revisión por la Dirección

13. MARCO NORMATIVO

MARCO NORMATIVO	DESCRIPCIÓN
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Manual de política de seguridad y privacidad de la información de función pública -2018.	Compendio de políticas aplican para todos los servidores públicos y contratistas de las entidades que procesan y/o manejan información de las entidades. Política pública de Seguridad Digital.
Decreto 103 de 2015.	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Decreto 338 de 2022	Por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.
Decreto 767 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.
Decreto 1263 de 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Ley estatutaria 1581 de 2012,	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República
Ley 1474 de 2011	“Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”. Disponible en Línea.
Decreto 4632 de 2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1474 de 2011	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.

Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Desarrollado por el Decreto 4487 de 2009 – Reglamentado parcialmente por el Decreto 1747 de 2000.
Resolución 746 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 500 de 2021.
Resolución 1978 de 2023	Por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones.
CONPES 3854 de 2016	Política Nacional de Seguridad digital
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.

ELABORÓ	REVISÓ	APROBÓ
Martha Mateus González Profesional Contratista Oficina de Transformación Digital y Tecnologías de la Información	**Norberto Ruiz Rodríguez** Profesional Contratista Oficina de Transformación Digital y Tecnologías de la Información **Martha Rodríguez Martínez** Jefe Oficina Asesora de Planeación	**Ángela Riveros Sierra** Jefe Oficina de Transformación Digital y Tecnología de la Información **Fecha de Aprobación:** 30/12/2025