IDRD

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

Oficina de Transformación Digital y Tecnologías de la Información

2025

Tabla de contenido

1. INTRODUCCIÓN

Ante la creciente adopción de tecnologías en las organizaciones, el Instituto Distrital de Recreación y Deporte (IDRD) ha priorizado la definición e implementación de prácticas integradas en sus procesos y operaciones. Estas prácticas se establecen como estrategias fundamentales para reducir o mitigar los riesgos asociados a la seguridad digital que puedan afectar sus activos de información.

El Instituto IDRD mantiene la confidencialidad, integridad, y disponibilidad de los activos de información, mediante un enfoque basado en riesgos y cuyo proceso es tomado como un componente importante para el gobierno corporativo, toma de decisiones, logro de los objetivos estratégicos y cumplimiento de su misionalidad.

La planificación del Sistema de Gestión de Seguridad de la Información, así como la identificación, análisis y evaluación de los riesgos digitales, se fundamentan en la definición e implementación de un plan de tratamiento. Este plan contempla la adopción de herramientas, sistemas, políticas, procedimientos y mecanismos seguros y adaptables, orientados a proteger tanto la información como la infraestructura tecnológica que la respalda.

2. JUSTIFICACIÓN

La elaboración de un plan de tratamiento de riesgos en seguridad digital permite al Instituto Distrital de Recreación y Deporte (IDRD) planificar, implementar, mantener y fortalecer las medidas de protección de sus activos de información. Este proceso se apoya en la adopción de herramientas, sistemas, políticas, procedimientos y mecanismos seguros y flexibles, en cumplimiento con la normativa colombiana vigente (MSPI, Decreto 1008 de 2018) y alineado con las mejores prácticas internacionales, tales como las normas ISO/IEC 27001:2022, ISO 31000:2018.

3. OBJETIVO

Mantener la plataforma tecnológica existente y desarrollar proyectos de manera oportuna y eficaz, así como formular lineamientos relacionados con estándares y buenas prácticas para el manejo de la información a fin de contribuir a la eficiencia de los procesos del IDRD.

4. ALCANCE

El plan de tratamiento de riesgos propuesto tiene como objetivo gestionar de manera eficaz los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital. Para ello, integra buenas prácticas dentro de los procesos del IDRD, con el fin de facilitar la toma de decisiones y prevenir incidentes que puedan afectar el cumplimiento de sus objetivos institucionales.

5. RESPONSABILIDADES

5.1 La oficina de Transformación digital y tecnologías de la información, brindara asesoría en la identificación de activos, junto con su clasificación, para diferentes áreas analicen el tratamiento de riesgos de cada uno de sus activos en seguridad de la información, con la metodología dispuesta en el instituto por la Oficina de Transformación Digital y Tecnologías de la Información.

5.2 El equipo de seguimiento y evaluación está conformado por el/la Jefe de Control Interno, los servidores públicos y contratistas de su área, quienes velarán por la adecuada elaboración e implementación del mapa de riesgos de cada proceso,

promoviendo su apropiación, entendimiento y evaluación de este.

5.3 El plan de tratamiento de cada riesgo de seguridad especifica, será responsabilidad de cada dueño de proceso, y serán los responsables de implementar las acciones destinadas a tratar, reducir o mitigar dicho riesgo**.**

6. CONDICIONES GENERALES

- Cumplimiento de los lineamientos para la administración del riesgo de seguridad de la entidad.
- Utilizar la Herramienta definida por la entidad para el tratamiento de Riesgos de Seguridad de la Información.

7. 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. (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.

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.

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.

8. DESARROLLO DEL PLAN

METODOLOGÍA

- La implementación del plan de tratamiento de riesgos de seguridad de la Información 2025, comprende las siguientes actividades:

Proceso Responsable	Compromisos (actividades)	Producto	Programación											
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Oficina de Transformación Digital y Tecnologías de la Información	Realizar las acciones requeridas que contribuyan a la mitigación de las vulnerabilidades en la infraestructura tecnológica que soporta los sistemas de Información del IDRD	Informe con las acciones realizadas para remediar las vulnerabilidades en la infraestructura tecnológica de la IDRD												X
Oficina de Transformación Digital y Tecnologías de la Información	Realizar las acciones requeridas que contribuyan a la mitigación de las vulnerabilidades en la infraestructura tecnológica con la herramienta Zabbix en el IDRD	Informe con las acciones realizadas para remediar las vulnerabilidades dadas por la herramienta Zabbix en el IDRD								X	X	X	X	X
Oficina de Transformación Digital y Tecnologías de la Información	Efectuar las acciones de coordinación para el proceso de actualización y consolidación de los activos de información del IDRD	Memorandos de solicitud y/o activos de información										X		X

MONITOREO, SEGUIMIENTO Y EVALUACIÓN

El valor de los activos, así como los impactos, amenazas, vulnerabilidades y probabilidades asociadas, serán revisados de forma periódica, según lo establezca la segunda línea de defensa, con el fin de detectar posibles cambios que ameriten una reevaluación de los riesgos de seguridad de la información. Considerando la naturaleza dinámica de estos riesgos, y al igual que la propia Entidad, su evolución puede producirse de manera significativa y sin previo aviso.

9 MARCO NORMATIVO

- NTC-ISO/IEC 27001:2022
- NTC-ISO/IEC 27002:2022
- Ley 1712 de 2014 Ley de tratamiento de datos
- MSPI - Modelo de Seguridad y Privacidad de la Información
- Política de Gobierno 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