CUADRO CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción del Cambio**
01	17/07/2024	Creación del plan PETI para la vigencia 2024 - 2027

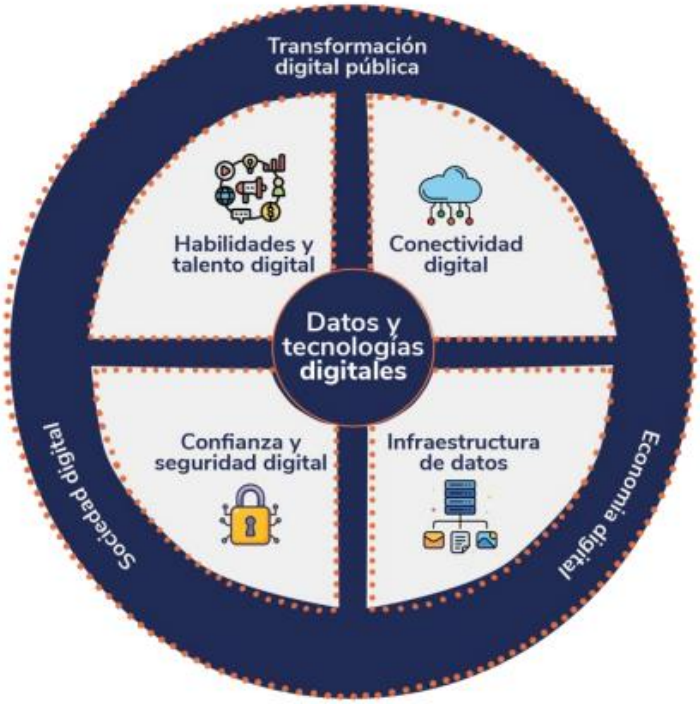
TABLA DE CONTENIDO

INTRODUICCIÓN

En la sociedad actual, el manejo de datos y el avance de tecnologías como la inteligencia artificial están transformando el entorno y la manera en que las personas, las entidades y la sociedad interactúan. Estas tecnologías ayudan a enfrentar retos y a incrementar la capacidad para abordar los múltiples desafíos que enfrentamos hoy en día. Según datos del DANE de 2022, tres cuartas partes de las personas mayores de cinco años utilizan internet en su vida diaria en cualquier lugar. Colombia es uno de los países en América Latina y el Caribe que más ha avanzado en la ruta hacia la digitalización.

Los gobiernos tienen un gran trabajo por delante en cuanto al acceso y uso de las tecnologías en la mayoría de los hogares, entidades y empresas, que deben avanzar para el desarrollo del país. Por ello, facilitar el acceso, uso y apropiación de los datos y las tecnologías digitales se plantea como un asunto central a lo largo de todo el Plan Nacional de Desarrollo 2022-2026 “Colombia, Potencia Mundial de la Vida”. Este plan destaca que la conectividad y la transformación digital son elementos clave para promover la seguridad humana y la justicia social, y lograr otras transformaciones relevantes para el país.

En el marco de este plan, el acceso a Internet se concibe como un derecho y no un privilegio, lo que constituye un avance fundamental para alcanzar las metas sociales y económicas propuestas por el gobierno. El Consejo Nacional de Política Económica y Social publicó el Documento CONPES 3995 sobre la Política Nacional de Confianza y Seguridad Digital, el cual resalta que “el entorno digital es un escenario en el que globalmente se desarrollan cada vez más todo tipo de actividades socioeconómicas. Esto expone tanto a las personas como a las organizaciones a amenazas cibernéticas por parte de delincuentes que aprovechan el creciente intercambio de información. Se debe apuntar a que existan medidas suficientes, tanto en el fortalecimiento de la seguridad como en la generación de confianza digital, respecto a una adecuada anticipación, gestión de riesgos, atención oportuna y defensa ante las amenazas existentes en el entorno digital, dentro de un marco de gobernanza nacional eficiente, acorde con las necesidades actuales y en constante desarrollo, en el que se pueda materializar rápidamente la confianza y la seguridad digital ante la aparición de nuevas tecnologías”.



Fuente: Elaboración DNP

Ilustración 1. Abordaje conceptual Estrategia Nacional Digital Colombia 2023-2026 fuente:
MINTIC Colombia Estrategia Nacional Digital de Colombia 2023 - 2026

Bajo este marco de trabajo INDERSANTANDER presenta su plan de tratamiento de riesgos de seguridad digital para la vigencia 2024.

1.OBJETIVOS

1.1. OBJETIVO GENERAL

Determinar las acciones necesarias para el tratamiento de riesgos de seguridad y privacidad de la información del Instituto Departamental de Recreación y Deportes de Santander. Esto se logrará mediante la identificación, análisis, valoración y tratamiento de los riesgos relacionados con la pérdida de confidencialidad, disponibilidad e integridad de la información, con el fin de

prevenir su materialización y/o reducir los impactos negativos en la gestión institucional.

1.2. OBJETIVOS ESPECÍFICOS

- Realizar un inventario exhaustivo de los activos de información y los posibles riesgos asociados a la confidencialidad, disponibilidad e integridad de estos activos.
- Evaluar la probabilidad y el impacto de los riesgos identificados, utilizando metodologías reconocidas para el análisis de riesgos de seguridad de la información.
- Priorizar los riesgos identificados en función de su probabilidad e impacto, para enfocar los esfuerzos de mitigación en los riesgos más críticos.
- Desarrollar e implementar medidas de control y mitigación para reducir la probabilidad y/o el impacto de los riesgos priorizados.
- Establecer un proceso continuo de monitoreo y revisión de los riesgos y las medidas de control implementadas, para asegurar su efectividad y realizar ajustes cuando sea necesario.
- Implementar programas de capacitación y concienciación para el personal del Instituto, con el fin de fomentar una cultura de seguridad y privacidad de la información.
- Mantener una documentación detallada de todos los procesos de gestión de riesgos y elaborar informes periódicos para la alta dirección sobre el estado de la seguridad y privacidad de la información.

2. RESPONSABILIDADES

INDERSANTANDER apoyará la implementación del plan de tratamientos de riesgos de Seguridad y Privacidad de Información como un proceso transversal incluido en el Comité Institucional de Gestión y Desempeño

Por lo anterior, se deben tener en cuenta al responsable de Tecnologías de la Información y Seguridad Digital de la Administración en las reuniones del Comité Institucional de Gestión y Desempeño.

3. TRATAMIENTO DE RIESGOS

3.1. Factores de riesgo

Para la vigencia 2025, se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

- **Nivel de conocimiento del personal:** Conocimiento insuficiente del personal en amenazas digitales, políticas y controles de seguridad.
- **Disponibilidad de servicios esenciales:** Garantizar la disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- **Protección de datos personales:** Identificación y protección adecuada de los datos de carácter personal.
- **Clasificación de la información:** Clasificación adecuada de la información bajo custodia de la Entidad, de acuerdo con el marco legal vigente.
- **Entorno digital inseguro:** Riesgos asociados a un entorno global digital inseguro.
- **Aislamiento del personal:** Impacto del aislamiento forzoso del personal en sus residencias.
- **Segregación de roles y privilegios:** Segregación apropiada de roles y privilegios en todos los sistemas de información.

	TIPOLOGIA DE ACTIVOS
TIPO DE ACTIVO	***DESCRIPCIÓN***
Informacion	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Activos informáticos lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A* Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	*SELECCIONE ESTA OPCIÓN SI EL ACTIVO IDENTIFICADO HACE REFERENCIA A Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa*
N/A	SELECCIONE ESTA OPCIÓN SI RIESGO ES DE GESTIÓN

3.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

3.2. Valoración del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer su nivel y las posibles acciones a implementar.

Dicho análisis incluye las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sean administrativos, técnicos y/o procedimientos implementados en la entidad. Por lo tanto, se analiza el riesgo combinando estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad).

La valoración de los riesgos se realizará conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, reglamentada por el DAFP, en versión 05 de 2020.

3.3. Estrategia de tratamiento de riesgo

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

Transferir: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.

Mitigar: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.

Evitar: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.

Aceptar: consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

La estrategia de control de riesgos para la vigencia 2025, contempla cuatro ejes que son: conocimiento, continuidad, control de acceso y controles tecnológicos, así:

.

3.3.1 Estrategias Orientadas al Conocimiento (Capacitación)

Mediante actividades de inducción, sensibilización y capacitación periódica se busca que todos los servidores y contratistas apropien conocimientos en materia de:

- Ley de protección de datos personales
- Ley de transparencia y acceso a la información
- Políticas institucionales de seguridad digital

- Modalidades y control de ataques informáticos
- Uso seguro de los recursos informáticos

3.3.2 Estrategias Orientadas al Conocimiento (Riesgos)

Para afrontar escenarios de riesgo asociados a la pérdida de continuidad, la Entidad adelantará en la vigencia 2025, acciones específicas en materia de:

- Fortalecimiento de su infraestructura de servicios básicos de energía
- Mejoramiento de sus capacidades de detección oportuna de eventos adversos de seguridad de la información.

3.3.3 Estrategias orientadas al conocimiento (Controles)

Con el fin de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados la Entidad emprenderá en la vigencia 2025 acciones específicas para:

- Actualizar los instrumentos de acceso a la información pública
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos.
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información

3.3.4 Estrategias de fortalecimiento de controles técnicos

Ante el aumento del tipo y complejidad de amenazas informáticas la entidad implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos
- Reforzamiento de controles de acceso a servicios en la nube
- Verificación y control de copias de respaldo
- Control de cambios en plataformas tecnológicas

4. Plan de Acción 2025

EJE	DESCRIPCIÓN	RESPONSABLE	ENTREGABLE	1 SEMESTRE						2 SEMESTRE					
				E	F	M	A	M	J	J	A	S	O	N	D
Riesgos	Actualización de los lineamientos de Riesgos de Seguridad de la Información en la Política de administración	P.U GESTION DE LA INFORMACIÓN CPS MIPG	Política Actualizada												

	del Riesgos institucional.													
	Incluir dentro del plan de capacitación-PIC 2025 los riesgos de Seguridad digital y privacidad de la información.	JEFE DE TALENTO HUMANO	Registro del PIC 2025											
	Establecer reuniones con los líderes de los procesos previamente identificando los Riesgos de Seguridad de la Información por proceso.	P.U GESTION DE LA INFORMACIÓN CPS MIPG	Riesgos de seguridad digital por proceso											
	Socializar los Riesgos de Seguridad de la Información ante el Comité Institucional de Gestión y Desempeño	P.U GESTION DE LA INFORMACIÓN CPS MIPG	Registro de asistencia del comité											
	Realizar monitoreo al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	P.U GESTION DE LA INFORMACIÓN CPS MIPG	Informe de monitoreo											
	Realizar informe de Seguimiento al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	Jefe de Control interno	Informe semestral de seguimiento											

BIBLIOGRAFÍA

- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 Ley de Transparencia.

- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, Protección de datos personales

- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.

- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.

- MINTIC COLOMBIA. articles-334120_recurso_1

	Funcionario/Contratista	Cargo/Contrato	Firma
Proyectó –Profesional	Freddy Angarita Pino	P.U. Gestión de la Información	
Revisó – Profesional	Hector Fabián Mantilla	Sub – director Administrativo y Financiero	
Aprobó- Asesor	Comité de Gestión y Desempeño - MIPG		