# Plan Estratégico de Seguridad de la Información

## Oficina de Sistemas e informática

2024 - 2027

Versión 2. 27/01/20

INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

# Introducción

INDEPORTES ANTIOQUIA considera:

1.Que los activos de información son fundamentales, dada la importancia en la operación y en la gestión de la Entidad, como medio para alcanzar los objetivos estratégicos propuestos y que por ende traen inmersas grandes amenazas que comprometan la información tanto física como digital.

2.Que se deben implementar mecanismos para garantizar el cumplimiento de la normatividad vigente, en materia de derechos de autor y de la protección de la información y los datos.

3.Que Indeportes Antioquia, debe adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

4. Que los cambios en la configuración de la plataforma tecnológica de la Entidad y el cambiante panorama de riesgos y amenazas del sector TIC, hacen necesario la actualización de estas políticas.

Así pues, con el fin de proteger la información y dar cumplimiento al decreto No. 1008 del 14 de junio 2018, por la cual se establecen los lineamientos generales de la Política de Gobierno Digital, la cual en su artículo 2.2.9.1.1.3. – Principios; tiene como prioridad la Seguridad de la Información: “Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades estatales, y de los servicios que prestan al ciudadano”; INDEPORTES ANTIOQUIA tiene definida bajo la resolución 2023001322 “LAS POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y USO DE RECURSOS INFORMÁTICOS EN INDEPORTES ANTIOQUIA”, la cual define las estrategias, guias y políticas a utilizar por parte de la entidad para salvagardar la seguridad de la información.

# Objetivo

Implementar el Sistema de Gestión de Seguridad de la Información en INDEPORTES ANTIOQUIA, determinando las políticas de seguridad de la información, con el fin de proteger la información contra una gran variedad de amenazas, minimizando el riesgo y asegurando la continuidad del servicio, acorde a los lineamientos definidos por el Departamento Administrativo de la FunciónPública, el Ministerio de las TIC y el programa de Gobierno Digital.

# Alcance

Este plan así como las políticas están dirigidas al personal interno de la Entidad (servidores públicos, contratistas, entrenadores, deportistas, así como también a los residentes de las Villas deportivas: Antonio Roldán Betancur, Villa Náutica, CEDEP Urabá, Neiva-80 y las demás sedes que sean administradas por el Instituto). El alcance de dichos lineamientos también aplica a personas externas (usuarios no frecuentes y visitantes).

Todo usuario de los recursos tecnológicos en INDEPORTES ANTIOQUIA tiene un grado de responsabilidad a partir del momento que tiene autorización de acceso a la información y a los equipos o a los canales de comunicación Institucionales de los que hace uso. Acorde a lo descrito, los usuarios deberán conocer y aceptar estas directrices, por lo que el desconocimiento de este documento no exonerará a la persona de las responsabilidades adquiridas.

Además de las políticas generales dispuestas a cumplir en INDEPORTES ANTIOQUIA, se adoptarán las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2015, y las que la Entidad disponga a partir del análisis de los riesgos de la seguridad de la Información.

# Objetivos Específicos

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores de la Entidad, practicantes, contratistas y demás actores participes de la operación de la Entidad.
- Velar por la continuidad de los procesos de la Entidad.
- Minimizar los riesgos asociados a la seguridad de la información.
- Cumplir con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y a la política de Gobierno en línea del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, y perdida de integridad, que respondan a la disponibilidad requerida por los usuarios o clientes externos de la Entidad.
- Proteger la información a la que se acceda y procese, para evitar su perdida, alteración, destrucción o uso indebido.
- Registrar y monitorear las violaciones a las políticas y controles de seguridad de la información, y a su vez reportarlas a la Oficina de Talento Humano, para que inicie las investigaciones pertinentes, de conformidad con el control disciplinario interno y con lo establecido en el Código Único Disciplinario.

# Marco normativo

- Ley 23 de 1982 - Derechos de Autor.

- Ley 599 de 2000 - Código Penal.

- Ley 1032 de 2006 - Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal: Artículo 257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Artículo 272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones.

- Ley 679 de 2001 - Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

- Ley 1273 de 2009 - Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

# Definiciones

- **Activo**: Buen que tiene valor para INDEPORTES ANTIOQUIA, se requiere para las actividades y requiere protección.

- **Activos de información:** Activo que dispone de información de INDEPORTES ANTIOQUIA, corresponde a elementos tales como infraestructura, sistemas de información, bases de datos, documentación, manuales de usuarios, planes de continuidad, etc.

- **Activos de software**: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

- **Activos físicos:** Se consideran activos físicos elementos tales como: Computadores, laptops, módems, impresoras, escáner, equipos de comunicaciones, teléfonos, cintas, discos extraíbles, UPS, swiches, apps, routers, etc.

- **Amenaza**: Potencialidad que puede provocar un evento/incidente en INDEPORTES ANTIOQUIA que podría producir daños o pérdidas materiales y/o inmateriales.

- **Disponibilidad**: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados 2.10 ISO 27000.

- **Confidencialidad**: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado 2.13 ISO 27000

- **Integridad**: Propiedad de salvaguardar la exactitud y el estado completo de los activos 2.36 ISO 27000.

- **Hardware**: Son los componentes físicos que forman parte de sistema informático como son: Servidores, impresoras, monitores, la CPU, teclados, mouse, etc.

# Definiciones

- **Software**: Son los programas y archivos que tiene un computador y que son necesarios para su funcionamiento.

- **Usuario**: Todas aquellas personas que utilicen sistemas software, equipos informáticos y los servicios de Red provistos por la Entidad.

- **Borrado seguro**: Procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.

- **Cifrado**: Que está escrito con letras, símbolos o números que sólo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.

- **Correo masivo**: Expresión usada en el presente documento para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que no formen parte de los dominios "@indeportesantioquia.gov.co".

- **Datos Sensibles**: Información catalogada como pública clasificada o pública reservada.

- **Derechos / Privilegios de acceso / Roles:** Conjunto de permisos otorgados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).

- **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y/o amenazar la seguridad de la información. Todo incidente es un evento, más no todo evento es un incidente.

# Definiciones

- **Mesa de servicios de INDEPORTES ANTIOQUIA:** Equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información y comunicaciones de la Entidad.

- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, trazabilidad, no repudio y confiabilidad pueden estar relacionadas.

- **Seguridad informática**: Mediciones y controles que garantizan la seguridad de la información en los dispositivos tecnológicos como equipos de cómputo, tales como servidores, equipos de escritorio, portátiles, tabletas, móviles, dispositivos de red, software aplicaciones y sistemas operativos.

- **Servidores públicos:** Término que se usa en el presente documento para identificar a empleados públicos, provisionales, de carrera, libre nombramiento, contratistas y practicantes de INDEPORTES ANTIOQUIA.

- **Software malicioso (código malicioso)**: Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario.

- **Usuario**: Persona, proceso o aplicación autorizada para acceder a la información de la Entidad o a los sistemas que se utilizan para habilitar los procesos.

- **VPN (Virtual Private Network):** Una Red Privada Virtual es una tecnología de red de computadores que permite tener una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

- **Hacking**: Es un conjunto de técnicas utilizadas para introducirse en un sistema informático vulnerando las medidas de seguridad, con independencia de la finalidad con la cual se realice, puede ser lícito y solicitado.

# Estado Actual

## RESULTADOS FURAG

De acuerdo con el Informe de Resultados Medición Desempeño Institucional MDI - FURAG 2024 que se realizó en 2024 con la gestión del 2023, a través de la plataforma disponible por la Función Pública.

Para el PESI son relevantes las Politicas de POL07 Gobierno Digital y POL 08 Seguridad Digital, sobre las cuales se obtuvieron los siguientes resultados:

**POL07: Gobierno Digital**

- **2023:** 68.9 puntos
- **2022:** 55.3 puntos

| Índice | Puntaje | Promedio |
|---|---|---|
| Arquitectura | 70.6 | 39.0 |
| Cultura y apropiación | 46.3 | 37.9 |
| Decisiones basadas en Datos | 54.3 | 40.4 |
| Estado Abierto | 88.3 | 68.7 |
| Gobernanza | 66.7 | 54.2 |
| Innovación pública digital | 66.7 | 32.5 |
| Proyectos de transformación digital | 88.9 | 74.2 |
| Seguridad y privacidad de la información | 53.9 | 50.3 |
| Servicios ciudadanos digitales | 0.0 | 7.0 |
| Servicios y procesos inteligentes | 50.0 | 32.9 |

# Estado Actual

## RESULTADOS FURAG

**POL08: Seguridad Digital**

- **2023:** 62.5 puntos
- **2022:** 71.6 puntos

| Índice | Puntaje | Promedio |
|---|---|---|
| Asignación de Recursos | 70 | 41.6 |
| Despliegue de controles | 75 | 65.7 |
| Implementación Lineamientos política | 56.7 | 58.4 |

Ahora bien, si en general os puntjaes están por encima de la media, se nota un retroceso en cuanto al 2023 frente al 2022, lo cual se pretende mejorar con el plan de acción derivado del presente PESI.

# MSPI

## MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con relación a la medición efectuada mediante la aplicación del instrumento del autodiagnóstico del Modelo de Seguridad de la Información (MSPI) en la entidad, se observa la evaluación de efectividad de controles implementados de acuerdo con la norma NTC-ISO-IEC 27001 como se detallan en la siguiente tabla:

| AVANCE PHVA | | |
|---|---|---|
| **COMPONENTE** | **% de Avance Actual Entidad** | **% Avance Esperado** |
| Planificación | 20% | 40% |
| Implementación | 9% | 20% |
| Evaluación de desempeño | 11% | 20% |
| Mejora continua | 14% | 20% |
| TOTAL | 54% | 100% |

# MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

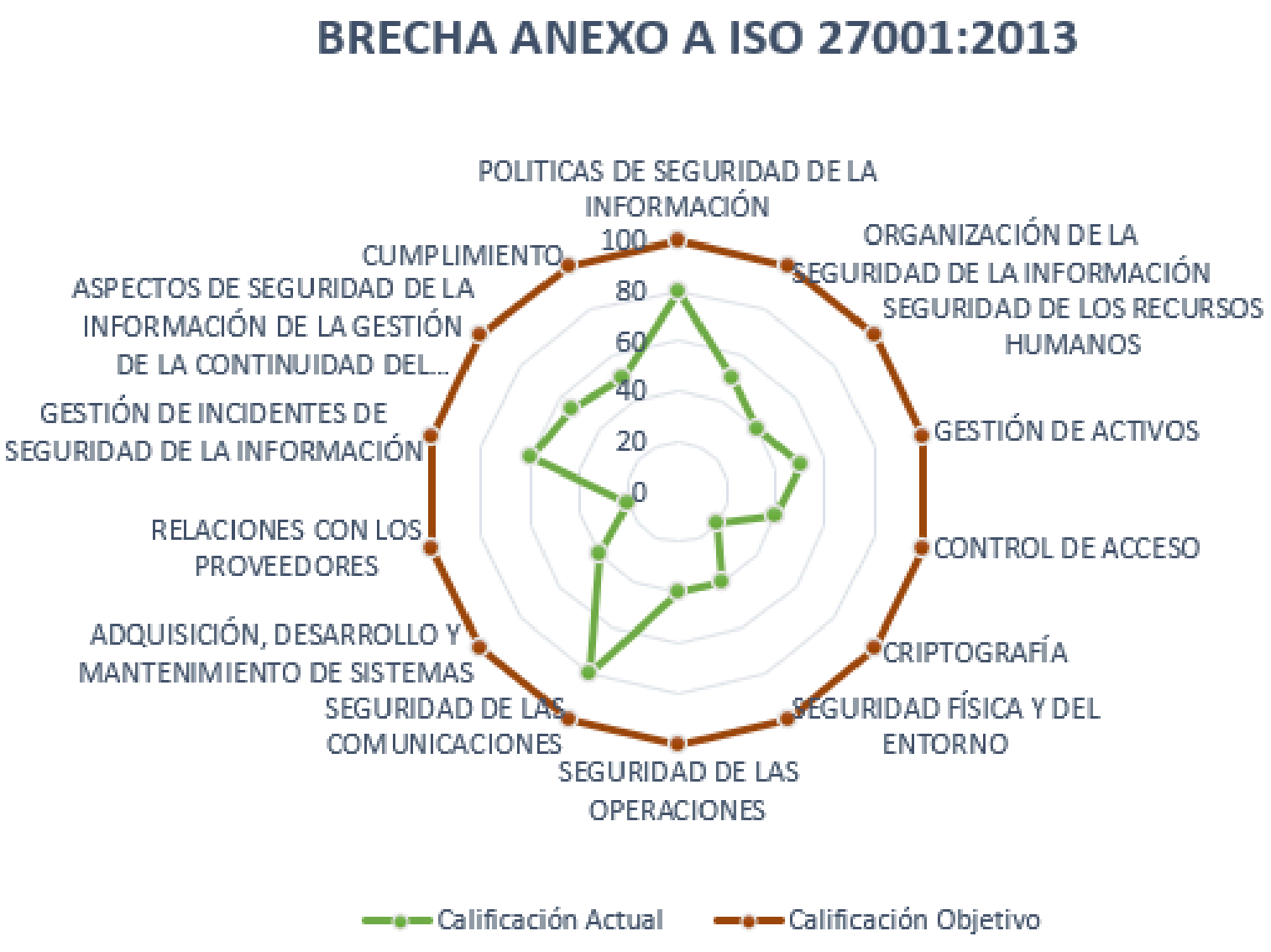
Se identifican algunos dominios que se encuentra por debajo del umbral del 60%, razón por la cual se requiere definir estrategias y proyecto que permita incrementar el % de implementación del MSPI en cada uno de los dominios y reducir la brecha de Seguridad Di

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 80 | 100 | GESTIONADO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 50 | 100 | EFECTIVO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 40 | 100 | REPETIBLE |
| A.8 | GESTIÓN DE ACTIVOS | 50 | 100 | EFECTIVO |
| A.9 | CONTROL DE ACCESO | 40 | 100 | REPETIBLE |
| A.10 | CRIPTOGRAFÍA | 20 | 100 | INICIAL |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 40 | 100 | REPETIBLE |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 40 | 100 | REPETIBLE |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 80 | 100 | GESTIONADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 40 | 100 | REPETIBLE |
| A.15 | RELACIONES CON LOS PROVEEDORES | 20 | 100 | INICIAL |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 60 | 100 | EFECTIVO |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 54 | 100 | EFECTIVO |
| A.18 | CUMPLIMIENTO | 50 | 100 | EFECTIVO |
| *PROMEDIO EVALUACIÓN DE CONTROLES* | | 47 | 100 | EFECTIVO |

# MSPI

## MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

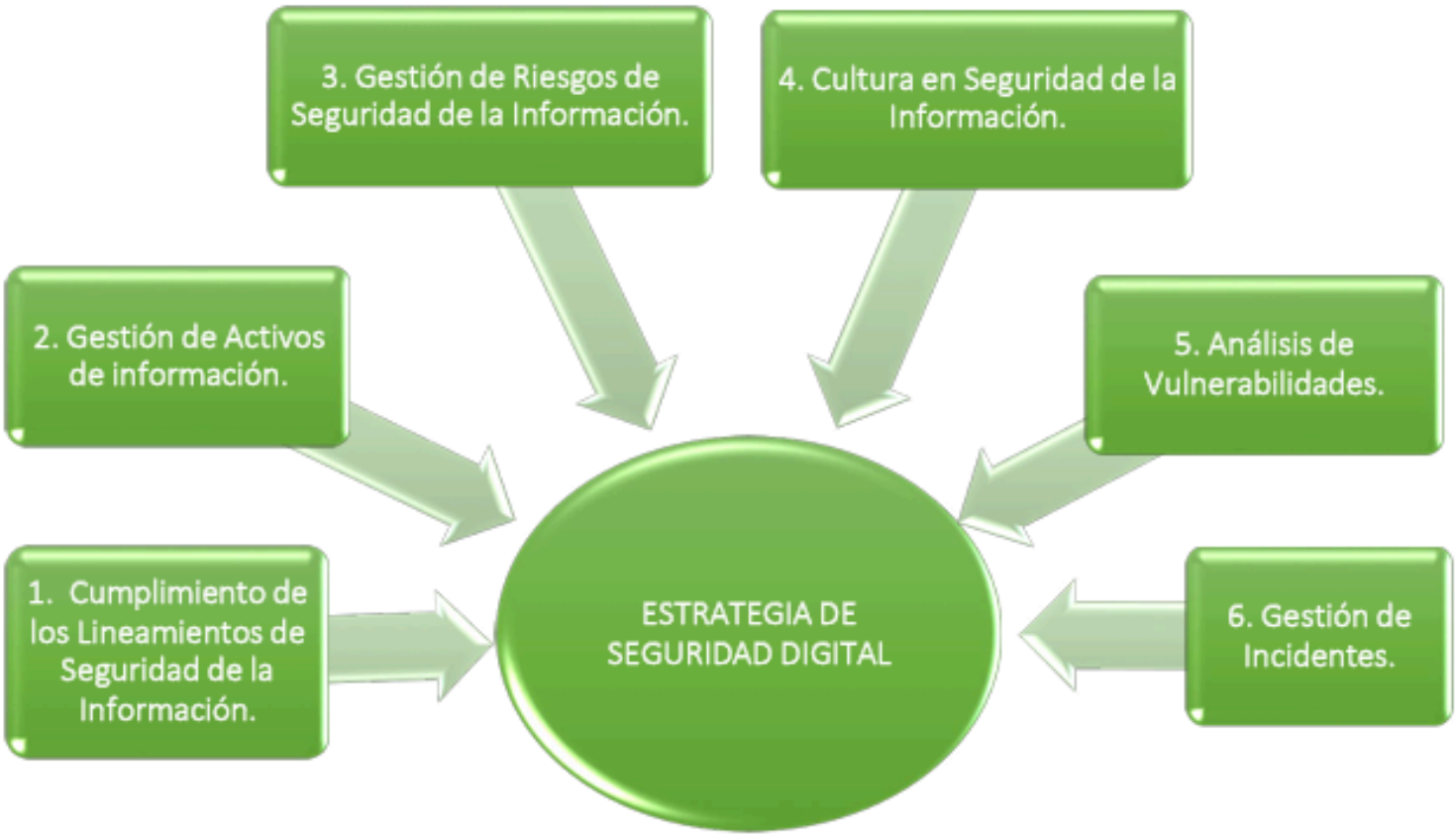
En la siguiente grafica radial se observa la situación actual en cada uno de los dominios de NTCISO/IEC 27001



# Estrategía de Seguridad digital

Indeportes Antioquia adoptara estrategias de Seguridad Digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la Gestión de la Seguridad de la Información Digital de acuerdo con las directrices de la resolución No.500 del 2021 de MinTIC, de conformidad con la Resolución 2023001322 que define “LAS POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y USO DE RECURSOS INFORMÁTICOS EN INDEPORTES ANTIOQUIA”, la cual contiene las estrategias, guias y políticas a utilizar por parte de la entidad para salvagardar la seguridad de la información.

La estrategia de Seguridad Digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.




INDEPORTES ANTIOQUIA

GOBERNACIÓN DE ANTIOQUIA

# Estrategía de Seguridad digital

| ESTRATEGIA | PROYECTO | 2025 | 2026 | 2027 |
|---|---|---|---|---|
| Cumplimiento de los lineamientos de Seguridad de la Información. | Implementar de controles Seguridad Información. | X | X | X |
| Gestión de activos información | Socialización y consolidación de los activos de información definitivos a cada proceso. | X | | |
| Gestión de Riesgos de Seguridad de la Información | Identificar, evaluar y realizar seguimiento de los riesgos de Seguridad de Información. | X | X | X |
| Cultura en Seguridad de la Información | Ejecutar y continur estrategias de sensibilización y capacitación sobre seguridad de la información al personal y actores involucrados | X | X | X |
| Análisis de vulnerabilidades. | Ejecutar análisis de (test y re-test) de vulnerabilidades técnicas a Plataforma Tecnológica | | X | X |
| Gestión de Incidentes. | Definir y ejecutar el procedimiento para la atención y gestión de incientes de seguridad de la información | | X | X |

# Estrategía de Seguridad digital

indeportes Antioquia, al finalizar cada vigencia realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si estos cumplieron o si se requiere ajustar tiempos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la Entidad. y a la asignación de los recursos necesarios para la ejecución del mismo