PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA

ENERO 31 DE 2024

CONTENIDO

1. INTRODUCIÓN

El Instituto Departamental de Deportes del Cauca; INDEPORTES CAUCA, considera el valor de proteger los activos de información institucional dado que, expuestos a perdida, daños y/o modificaciones por parte de terceros. Continuamente en la gestión de los procesos y procedimientos de acuerdo a la misión y visión de la Entidad se están procesando información valiosa que es generada desde cada una de las dependencias del Instituto que va desde información confidencial del personal de la Entidad, proveedores, usuarios, entrenadores, hasta datos de deportistas de alto rendimiento del Departamento que no debe ser divulgada a personal no autorizado, lo cual pondría en riesgo a la Entidad.

Por consiguiente, INDEPORTES CAUCA para esta vigencia asume la función de implementar el Sistema de Seguridad de la Información (SGSI), de acuerdo con la estructura organizacional y presupuestal, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno Digital.

2. OBJETIVOS

➢ GENERAL

Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Departamental de Deportes del Cauca, como marco de referencia para el establecimiento y regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad.

➢ ESPECIFICO

- Proteger los activos de información del **INDEPORTES CAUCA.**
- Identificar los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Sensibilizar a los funcionarios y contratistas del Instituto, acerca del SGSI, fomentando la cultura institucional en materia de seguridad de la información, cuyo objetivo primordial será la preservación de la Confidencialidad, Integridad y Disponibilidad de la información, así como la socialización y divulgación de buenas prácticas y recomendaciones de seguridad.
- Ejecutar las acciones para la implementación y apropiación del Sistema de Gestión de Seguridad de la Información, con el objetivo de salvaguardar la seguridad y privacidad de la información.

3. NORMATIVIDAD

- Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", dentro de los cuales se encuentran: Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información, Política de Gobierno Digital.
- 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 1341 de 2012, Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC.
- Ley 1581 de 2012, Protección de datos personales.
- Decreto 1377 de 2013 Reglamentación parcial de la Ley de datos personales.
- 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.

4. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a todos los procesos de INDEPORTES CAUCA, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información SGSI 2024.

5. RESPONSABILIDADES

La entidad debe definir mediante un acto administrativo (Resolución) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos del Instituto en cuanto a seguridad y privacidad de la información.[1]

6. TÉRMINOS Y DEFINICIONES

Se hace alusión a los términos empleados dentro del documento, que son necesarios para la comprensión del mismo. Estos términos son organizados alfabéticamente.

- **Riesgo de seguridad de la información**: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

información por el aprovechamiento de oportunidades y fortalezas que se presenten.

- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **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 del Estado, y de los servicios que prestan al ciudadano.
- **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). plan de seguridad y privacidad de la información.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Administración Municipal y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenaza:** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de riesgos de seguridad de la información**: proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **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).
- **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) plan de seguridad y privacidad de la información.
- Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **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).
- *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).
- **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).
- **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.
- **Propietarios de los activos de información:** son los responsables de cada uno de los activos de información (archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, las personas, etc. Esta persona se hará cargo de mantener la seguridad del activo.
- **Recursos tecnológicos**: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Sistema de información (SI):** es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general.

7. DESARROLLO

7.1. Estructura del Plan de Seguridad y Privacidad de da Información

INDEPORTES CAUCA; deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos

7.2. Fase diagnóstica

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

- Para esta fase se cuentas con las siguientes metas:
- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de INDEPORTES CAUCA.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en Ciber- seguridad.
- Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. Para ello, utilizaremos las siguientes herramientas publicadas en: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

7.3. Fase Planificación

7.3.1. Política de seguridad y privacidad de la Información:

Se proyectará la Política de Seguridad y Privacidad de la información que estará contenida en un documento de alto nivel que incluye la voluntad de la gerencia de INDEPORTES CAUCA; para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

- La política contendrá una declaración general por parte de la gerencia, donde se especifique sus objetivos, alcance, nivel de cumplimiento.
- La política será sometida a aprobación en el comité de gestión TIC y será divulgada al interior de INDEPORTESCAUCA.
- Se tomará de base la Guía 2 - Política General MSPI del Modelo de Seguridad y privacidad de la Información de Min Tic.
- https://www mintic.gov.co/gestionti/615/articles-5482 G2_Politica_General.pdf.
- La actualización de la política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la Seguridad de la Información.
- Se desarrollará un manual de políticas con objetivos, alcances y nivel de cumplimiento que garanticen un uso adecuado de los activos de información de INDEPORTES CAUCA, el manual de políticas debe contener de forma general, las políticas, los principios de seguridad y la normatividad vigente.

7.3.2. Procedimientos de Seguridad de da Información

Se formalizarán los procedimientos que permitan consolidar la seguridad y privacidad de la información en cada uno de los procesos definidos en INDEPORTES CAUCA; de acuerdo a la Guía 3 Procedimiento de Seguridad de la información.
https://www mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_seguridad.pdf.

7.3.3. Inventario de Activos

Realizar el Inventario de los activos de información por parte de cada proceso, siendo gestión tecnológica quien recopila la información generando un solo documento con todos los activos de la entidad, con el fin de definir la criticidad, sus propietarios, custodios y usuarios, para desarrollar estas actividades, tomaremos La Guía No 5 - Gestión De Activos, https://www minticgovco/gestionti/615/articles-5482 G5_Gestion_Clasificacion,pdf

7.3.4. Identificación, Valoración y Tratamiento de Riesgos

INDEPORTES CAUCA, deberá definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad esto mediante la Guia 7 – gestión de riesgos de MINTIC.
https://www.mintic.govfl)/gestionti/615/articles-5482 G7 Gestión Riesgos.pdf.
y la Guía No 8 - Controles de Seguridad https://www.mintic.gov.co/gestionti/615/articles-5482_(38 Controles Seguridad.pdf

7.3.5. Plan de Comunicaciones

INDEPORTES CAUCA; definirá un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad y privacidad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, contratistas, terceros) , para su elaboración se utilizará la Guía No 14 — plan de comunicación, sensibilización y capacitación. https://www.mintic.gov.co/gestionti/615/articles-5482 G14 Plan comunicación sensibilización pdf.

7.4. Fase de Implementación

Se deberá implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI. https://www.mintic.gov.co/gestionti/615/articles-5482 G8 Controles Seguridad.pdf

8. SEGUIMIENTO Y EVALUACIÓN

8.1. Indicadores de Gestión

Se deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de INDEPORTES.
- Servir como insumo al plan de control operacional, mediante La Guía No 9 - Indicadores de Gestión, brinda información relacionada para poder llevar a cabo la realización de esta actividad. https://www.mintic.gov.co/gestionti/615/articles-5482 (39 Indicadores Gestión Segundad pdf

8.2. Revisión y Seguimiento a la Implementación del MSPI

Este plan debe contener las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.
- La Guía No 16 Evaluación del Desempeño, brinda información relacionada para poder llevar a cabo la realización de esta actividad. https://www.mintic.gov.co/gestionti/615/articles-5482_G16_evaluaciondesempeno.pdf

8.3. Ejecución de auditorías

Se debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Se debe llevar a cabo auditorías y revisiones independientes a intervalos

planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz.
La Guía No 15 - Guía de Auditoría, brinda información relacionada para poder llevar a cabo la realización de esta actividad. https://www.mintic.gov.co/gestionti/615/articles-5482 G 15 Auditoria.pdf.

8.4. Fase de Mejora Continúa

En esta fase se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

9. ANEXOS

Como anexo a este plan se tomará el cronograma de actividades Para la vigencia 2024

CRONOGRAMA DE EJECUCION PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024												
	Actividad	**FEBRERO**	**MARZO**	**ABRIL**	**MAYO**	**JUNIO**	**JULIO**	**AGOSTO**	**SEPTIEMBRE**	**OCTUBRE**	**NOVIEMBRE**	**DICIEMBRE**
FASE DIAGNOSTICO	autodiagnostico de la situación actual											
	análisis del diagnóstico inicial											
FASE PLANEACION	realización política de seguridad y privacidad de la informacion											
	aprobación y socialización manual de políticas											
	procedimientos de seguridad de la información											
	seguridad del recurso humano											
	gestión de activos											
	control de acceso											
	seguridad física											
	seguridad de operaciones											
	seguridad de comunicaciones											
	gestión de incidentes de seguridad											
	roles y responsabilidades											
	inventario, clasificación y publicación de activos											
	identificación y tto de riesgos											
	realización plan de comunicaciones											
FASE DE IMPLEMENTACION												
FASE DE EVALUACION Y DESEMPEÑO												
FASE DE MEJORA CONTINUA												

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
V1	2024/01/31	Elaboración del Plan en el nuevo formato de Planes Institucionales

ELABORÓ	REVISÓ	APROBÓ
Mónica Margoth Mera Cerón Jefe Oficina de Planeación	Mónica Margoth Mera Cerón Jefe Oficina de Planeación.	Comité Institucional de Gestión y Desempeño 01 31 de enero de 2024