PLAN DE TRATAMIENTO Y SEGURIDAD DE LA INFORMACIÓN

VIGENCIA 2024

CONTENIDO

1. INTRODUCIÓN

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es muy importante que el Instituto cuente con un plan de gestión de riesgos para garantizar la continuidad de las gestión estratégica de acuerdo a su misión y visión, por tal motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información en el Instituto, antes de iniciar con este plan de gestión se ha revisado la situación actual de la entidad y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de los activos de información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentra la información mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

La Seguridad de la Información en las Entidades tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de la Entidad.

2. OBJETIVOS

➢ GENERAL

Presentar el plan de tratamiento de riesgos de seguridad y privacidad de la información del INSTITUTO DEPARTAMENTAL DE DEPORTES DEL CAUCA – INDEPORTES 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 que la soportan al interior de la Entidad. Atendiendo las orientaciones dadas por el Ministerio de las Tecnologías información y de las comunicaciones MINTIC en su Guía de Gestión de riesgos Seguridad y Privacidad de la Información.

➢ ESPECIFICO

- Determinar el alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información.

- Definir los principales activos a proteger en INDEPORTES CAUCA.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo en INDEPORTES CAUCA.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo en INDEPORTES CAUCA.
- Desarrollar y aplicar mejoras a las políticas vigentes de gobierno digital.
- Definir estándares de protección y monitoreo a cada tipo de riesgo y de información.

3. NORMATIVIDAD

- Decreto 1008 del 14 de junio de 2018, Política de Gobierno Digital.
- Decreto 1078 de 2015 Articulo 2.2.17.7.1, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1499 de 2017 Artículo 2.2.22.2.1., Políticas de institucional.
- Decreto 2693 de 2012.
- Decreto 1499 de 2017 se crea el nuevo Modelo Integrado de Planeación y Gestión.
- Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones -TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

4. ALCANCE

El Plan de tratamiento de riesgos tiene alcance para los procesos INSTITUTO DEPARTAMENTAL DE DEPORTES DEL CAUCA – INDEPORTES CAUCA, de acuerdo a las metodologías establecidas por el MINTIC, la identificación y definición de los riesgos de seguridad de la información para los activos de información de INDEPORTES CAUCA. Esto permitirá, la evaluación, valoración y la mitigación de los riesgos de los activos de información a su cargo en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información SGSI.

5. RESPONSABILIDADES

Los responsables para garantizar la adecuada aplicación y ejecución del documento son:

- Jefe planeación/ Líder del Proceso de Sistemas de Información y Comunicación
- Gerente
- Líderes de Procesos.

6. TÉRMINOS Y DEFINICIONES

- **Riesgo:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto servicio generado de un proceso o el cumplimiento de los objetivos institucionales.
- **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 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.

7. DESARROLLO

El Instituto en su aplicación del Plan de Tratamiento de Riesgos de Seguridad de la Información implementara las políticas de Gobierno Digital, según la normatividad vigente.

7.1. Política de Gobierno Digital

El Instituto Departamental de Deportes y Recreación INDEPORTES CAUCA, fortalecerá y promoverá el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital contribuyendo a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso te de la tecnología (principalmente tecnologías emergentes

y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes, que garantice los servicios digitales más eficientes, con transparencia y participación, a través de las tecnologías de la información y las comunicaciones (TIC´S), mejorando los servicios y procesos, para el cumplimiento de las expectativas de los diferentes grupos de interés. Por tal motivo es importante que desde la dimensión de Direccionamiento Estratégico y de Planeación se tenga en cuenta la tecnología para apoyar la ejecución de los procesos, manejo y seguridad de la información, los servicios de soporte tecnológico y en general el uso de medios electrónicos para una gestión efectiva en la entidad.

La Política de Gobierno digital, se ajusta a la normatividad que rige para las entidades estatales y se encuentra orientado por los principios rectores de la función pública.

7.2. Política de Seguridad Digital.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social INDEPORTES CAUCA, con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, adoptará la política que en su conjunto tendrá como fin contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

La Política de Seguridad digital, se ajusta a la normatividad que rige para las entidades estatales y se encuentra orientado por los principios rectores de la función pública.

7.3. Acciones de Mejoras Implementadas d las Políticas del Instituto

Sin una herramienta de autodiagnóstico precisa, se crea un plan de acciones de mejora con el fin de proteger y preservar los recursos electrónicos, informáticos y equipos de cómputo el cual incluye:

- Crear una circular de uso adecuado y aceptable en el que se informa a los funcionarios del instituto, de lo que pueden y no pueden hacer en los equipos de la entidad.
- Concientización a los funcionarios proactivamente a través de comunicaciones periódicas y las actualizaciones en las políticas.

Así mismo y teniendo en cuenta la importancia que representa el uso adecuado de los activos informáticos de INDEPORTES CAUCA, se indican a continuación normas pertinentes con el objetivo de que cada funcionario se comprometa a dar un uso adecuado a los mismos, siendo consciente del riesgo en que incurre la entidad al incumplirlas.

7.4. Metodología de la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en adelante (MSPI) en el Instituto, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones — MinTIC, a través de los decretos emitidos.

7.5. Actividades a Realizar en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

- Realizar diagnóstico, levantamiento de información sobre aspectos de vulnerabilidad.
- Elaborar el alcance del plan del tratamiento de riesgos de seguridad y privacidad de la información.
- Realizar la identificación de los riesgos con los líderes del proceso.
- Plantear plan de tratamiento de riesgos aprobado por los líderes INDEPORTES CAUCA.
- Realizar actividades de sensibilización, inducción, reinducción al personal frente a las mejoras propuestas a las políticas de INDEPORTES CAUCA.

8. SEGUIMIENTO Y EVALUACIÓN

- Al finalizar cada etapa se realizará una reunión con los responsables, para presentar el informe del avance del plan y de esta manera evaluar todos los pasos se han ido realizado para lograr la aprobación y publicación del plan definitivo.
- Seguimiento a los riesgos de Seguridad de la Información identificados en el mapa de riesgos del proceso

9. ANEXOS

El siguiente anexo del cronograma de actividades al Plan se diseña con el propósito de cumplir la fase para determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de INDEPORTES CAUCA, los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del modelo MSPI estrategia de MINTIC.

CRONOGRAMA DE EJECUCION PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA FORMACION. 2024

	Actividades	F	M	A	M	J N	J l	A	S	O	N	D
1	Actividades de sensibilización con el personal frente a las acciones de mejora a las políticas de INDEPORTES CAUCA.											
2	Elaboración diagnóstico											
3	Analisis del diagnóstico inicial											
4	Elaboración alcance plan de tto de riesgos											
5	Realizar identificación de los riesgos con líderes											
6	Seguridad del recurso humano											
7	Valoración del riesgo y riesgo residual											
8	Mapa de calor de los riesgos identificados											
9	Socializar el plan a los líderes para su aprobación											
FASE DE IMPLEMENTACION												
FASE DE EVALUACION Y DESEMPEÑO												
FASE DE MEJORA CONTINUA												

10. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
V1	2024/29/01	Elaboración del Plan de Tratamiento de Riesgos de Seguridad de la Información

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