UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C., ENERO 2025

VERSIÓN 01

USPEC

INTRODUCCIÓN

En cumplimiento de la Resolución 500 de 2021 y del Decreto 1008 de 2018, que establecen los lineamientos para la seguridad digital y la política de Gobierno Digital en Colombia, respectivamente, nuestra entidad ha adoptado el Modelo de Seguridad y Privacidad de Información como marco de referencia para garantizar la protección de nuestros activos digitales. Este modelo, alineado con las mejores prácticas internacionales, promueve un enfoque proactivo en la gestión de riesgos de seguridad de la información, basado en el ciclo PHVA.

La identificación, evaluación y tratamiento de riesgos son fundamentales para asegurar la confidencialidad, integridad y disponibilidad de la información institucional, y así contribuir al logro de los objetivos estratégicos de la entidad. En este sentido, el presente plan de tratamiento de riesgos se enfoca en actualizar y fortalecer las medidas de seguridad implementadas para los procesos de Gestión de las Tecnologías de la Información.

A través de un riguroso análisis de riesgos, se han identificado las principales amenazas y vulnerabilidades que podrían afectar a este proceso crítico. Para cada riesgo identificado, se han definido controles específicos y se ha establecido un plan de acción con el objetivo de mitigar su impacto.

Este plan se encuentra alineado con la Política de Administración de Riesgos de la USPEC y busca garantizar que la entidad cuente con un sistema de gestión de seguridad de la información robusto y eficaz, capaz de enfrentar los desafíos del entorno digital actual.

1. OBJETIVO

Establecer el plan de tratamiento de riesgos que forma parte del Sistema de Gestión de Seguridad de la Información (SGSI), a través del monitoreo, análisis, identificación, controles y evaluación, que permitan mitigar la materialización de los riesgos de seguridad de la información, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad, y fomentar una cultura de seguridad en toda la organización.

1.1 OBJETIVOS ESPECÍFICOS

- ✓ Gestionar los riesgos de seguridad y privacidad de la información asociada a los procesos de la Entidad.
- ✓ Realizar seguimiento y control a la implementación del plan de tratamiento de riesgos.
- ✓ Establecer el plan de tratamiento de riesgos.

2. ALCANCE

El Plan de tratamiento de riesgos de seguridad de la información se inicia con la identificación y el tratamiento de los riesgos de seguridad de la información, siguiendo las directrices de la alta dirección y la normatividad vigente. Este plan se aplica a todas las dependencias, contratistas y terceros que prestan sus servicios o tienen alguna relación con la USPEC

3. DOCUMENTOS DE REFERENCIA

El Plan de Tratamiento de Riesgos de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su actualización y funcionamiento:

NORMATIVIDAD	
REFERENCIA	**DESCRIPCIÓN**
Decreto 612 de 2018	Fija directrices para la integración de planes al Plan de Acción.
Decreto 767 de 2022	Establece los lineamientos generales de la Política de Gobierno Digital.
Resolución 1519 de 2020	Define estándares para publicar información y requisitos de acceso a la información pública.
Resolución 500 de 2021	Establece lineamientos para la estrategia de seguridad digital.
Norma ISO 27001:2022	Norma internacional para la gestión de seguridad de la información.

NORMATIVIDAD	
REFERENCIA	**DESCRIPCIÓN**
Manual de Gobierno Digital	Establece lineamientos para los componentes de la política y habilitadores transversales.
Modelo de Seguridad y Privacidad de la Información	Define el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Guía para la administración de riesgos y el diseño de controles de las entidades públicas	Guía del DAFP para la administración de riesgos y diseño de controles.

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A través de la resolución 000008 del 2025, se aprobó la actualización de la Política de Seguridad y Privacidad de Información a través de la cual se establece que:
"La UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS, a través de la implementación del Modelo de Seguridad y privacidad de Información – MSPI, enmarcado en el Sistema de Gestión de Seguridad de Información y consciente de la importancia que representan los activos de información para el cumplimiento de su misión institucional, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de los riesgos, la implementación estrategias y controles, el cumplimiento de los objetivos de seguridad de la información, los requisitos legales, organizacionales y obligaciones contractuales, y de la asignación de los recursos necesarios para mejorar continuamente el Sistema de Gestión de Seguridad de la Información".
Adicionalmente, se establecen los objetivos de seguridad de la información, los roles y responsabilidades de todo el personal de la entidad para el cumplimiento de la política, así como las políticas adicionales de seguridad de la información y las directrices en caso de incumplimiento de la política.

5. ATRIBUTOS DE SEGURIDAD DE LA INFORMACIÓN

- ✓ **Confidencialidad:** Propiedad que se encarga de proteger la información frente a accesos no autorizados y evitar su divulgación a personas o sistemas no autorizados. Su aplicación es implementar mecanismos de tipo control de acceso, autenticación segura y cifrado para información clasificada o reservada.
- ✓ **Integridad:** Propiedad que se encarga de la exactitud y consistencia de la información durante su procesamiento, almacenamiento y transmisión. Y busca prevenir modificaciones no autorizadas o la corrupción de datos mediante controles tecnológicos y procesos de auditoría.
- ✓ **Disponibilidad:** Propiedad que se encarga de asegurar que los datos y sistemas estén accesibles para los usuarios autorizados cuando se requieran. Y su finalidad es mitigar interrupciones en los servicios tecnológicos mediante planes de contingencia, redundancia de infraestructura y monitoreo continuo.

6. METODOLOGÍA DE IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

A través de la política de administración de riesgos de la Entidad - GE-PO-001, se establecen los lineamientos para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, y seguimiento de los riesgos de gestión, de corrupción y de seguridad de la información entendidos como el efecto que se causa sobre los objetivos estratégicos de la Entidad, debido a eventos potenciales y que pueden llevar a la entidad a la posibilidad de incurrir en pérdidas o afectaciones a nivel económico o reputacional por deficiencias, fallas o inadecuaciones, en el recurso humano, procesos, tecnología, infraestructura o por la ocurrencia de acontecimientos externos.

7. ACTUALIZACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

La actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información se elaboró con base en un análisis exhaustivo de la información proporcionada por los diferentes procesos institucionales, considerando las amenazas, vulnerabilidades y probabilidades de ocurrencia identificadas.
Este análisis, que incluye información sensible sobre las estrategias de mitigación, y que se registra en la Matriz de Riesgos de Seguridad de la Información, no se publica en este documento con el fin de proteger la seguridad de la información institucional. El acceso al análisis completo está restringido al personal autorizado y se maneja con la debida confidencialidad.

8. SEGUIMIENTO

El seguimiento al plan de tratamiento de riesgos de seguridad de información se realizará cada trimestre, según lo establecido en la Política de Administración de Riesgos de la Entidad, empleando el formato establecido por la Oficina Asesora de Planeación y Desarrollo, a través de la hoja "Mapa de Riesgos", columnas de seguimiento por trimestre. Lo solicitará el Oficial de Seguridad de Información a cada uno de los líderes de proceso y posteriormente se llevará a cabo una evaluación por parte del Oficial frente al cumplimiento del plan de tratamiento de riesgos.

9. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección a través del Comité Institucional de Gestión y Desempeño y de los dueños de los riesgos, con el objetivo de ser actualizado, aprobado y aplicado conforme a lo que aquí se define. Lo anterior según lo establecido en el Modelo de Seguridad y Privacidad de Información Versión 4.0, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

9. INDICAODRES

INDICADORES		
Formula del indicador	**Periodicidad**	**Tipo de indicador**
(Σ del porcentaje de avance en la implementación del PTR por cada riesgo/ Número de riesgos)	Trimestral	Eficacia

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
1	17/01/2022	Todos	Se crea el plan de tratamiento de Riesgos de seguridad de información..
2	23/01/2023	Todos	Se actualiza el plan de tratamiento de Riesgos de seguridad de información
3	15/01/2024	Todos	Se actualiza el plan de tratamiento de Riesgos de información
4	27/01/2025	Todos	Se actualiza el plan de tratamiento de Riesgos de seguridad de información para la vigencia 2025 y se aprueba a través del Comité Institucional de Gestión y Desempeño, según acta N° 13 del 30 de enero 2025

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Daniel Ricardo Muñoz	Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Imelda Muñoz Mancipe
Cargo: Oficial de Seguridad de Información	Cargo: Profesional Especializado	Cargo: Jefe Oficina de Tecnología
Dependencia: Dirección General	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología