UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

VERSIÓN 3.0

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

TABLA DE CONTENIDO

Introducción

A través de la resolución 500 de 2021, se establecen los estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad de información como habilitador de la política de gobierno digital. Así mismo a través del decreto 1008 del 14 de junio de 2018 se establecieron los lineamientos generales de la política de Gobierno Digital, así mismo se establecen dos componentes o líneas de acción de esta política: TIC para el estado y TIC para la sociedad y tres habilitadores transversales que permitirán el cumplimiento de los logros establecidos en el decreto mencionado, estos habilitadores son Arquitectura de TI, Servicios ciudadanos digitales y Seguridad y privacidad.

A través del Modelo de Seguridad y Privacidad de Información se realizó una recopilación de mejores prácticasy requisitos que permiten en conjunto establecer un ciclo PHVA (Planear, Hacer, Verificar y Actuar) para contribuir en la implementación del Sistema de Gestión de Seguridad de Información en las Entidades públicas.

Un riesgo de seguridad digital se conoce como un conjunto de amenazas y vulnerabilidades derivadas del entorno digital y que pueden comprometer la confidencialidad, integridad y su disponibilidad de los activos de información, afectando el logro de los objetivos institucionales, por tanto es importante realizar una identificación oportuna de posibles riesgos, así como el establecimiento de controles que permitan su mitigación. En tal sentido y en cumplimiento de la “Política de Administración de Riesgos” de la USPEC,se continúa para la vigencia 2024 con la implementación de actividades y controles establecidos en el plan de tratamiento de riesgos de seguridad de información de acuerdo a la información recopilada con el proceso Gestión de Tecnologías de la Información.

Glosario

- **Amenazas.** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **MSPI.** Modelo de Seguridad y Privacidad de Información, definido por MINTIC que define un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.1
- **Norma ISO 27001:** Norma internacional que permite el aseguramiento, la confidencialidad e integridad delos datos y de la información, así como de los sistemas que la procesan. 2
- **Riesgo.** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)
- **SGSI.** Sistema de Gestión de Seguridad de Información. 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 deseguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Vulnerabilidad.** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

1. Objetivos

1.1 Objetivo General

Establecer las actividades requeridas para la mitigación de riesgos de seguridad digital a través del plan de tratamiento de riesgos con el fin de implementar controles que permitan proteger los activos de información de la Entidad, contra posibles amenazas que afecten la integridad, la disponibilidad y la confidencialidad de la información institucional.

1.2 Objetivos Específicos

- Actualizar el plan de tratamiento de riesgos de acuerdo al mapa de riesgos de seguridad digital.
- Realizar seguimiento trimestral al plan de tratamiento de riesgos con el fin de identificar el avance delas acciones definidas y la implementación de controles

2. Política de Seguridad y Privacidad de Información

A través de la resolución 000181 del 2022, 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 información, los roles y responsabilidadesde todo el personal de la Entidad para el cumplimiento de la política, las políticas adicionales de seguridad de información y las directrices en caso de incumplimiento de la política.

3. Formulación del Plan de Tratamiento de Riesgos de Seguridad digital

El mapa de riesgos de seguridad se actualizó tomando como referencia los activos de información del proceso Gestión de Tecnologías de la Información, en total se identificaron 4 riesgos y un total de 7 controles. Tomando esta información como referencia se definió el plan de tratamiento de riesgos de seguridad definiendo un total de 11 actividades enfocadas en las siguientes temáticas:

- ✓ Gestión del plan de mantenimiento de la plataforma tecnológica
- ✓ Gestión de control de cambios
- ✓ Gestión de vulnerabilidades de la plataforma tecnológica
- ✓ Gestión de la capacidad de la plataforma tecnológica
- ✓ Actualización de lineamientos de operación de TI
- ✓ Gestión de documentos electrónicos

De acuerdo a las buenas prácticas establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones en cuanto a la publicación de los planes de tratamiento de riesgos de seguridad de información se recomienda" *No deberá brindarse ningún tipo de detalle sobre los riesgos específicos, amenazas o vulnerabilidades analizados durante el proceso de gestión de riesgos, ya que esta información es clasificada o reservada de acuerdo con la ley 1712 de 2014".*

Por lo anterior, el mapa de riesgos de seguridad y el plan de tratamiento de riesgos se mantiene como información reservada de la USPEC.

4. 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.

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
1.0	17/01/2024	Todos	Se crea el plan de tratamiento de riesgos de seguridad, con el alcance del proceso Gestión de Tecnología de la Información
2.0	23/01/2023	Todos	Se actualiza el plan de tratamiento de riesgos de seguridad.
2.1	14/06/2023	Todos	Se actualiza el plan de tratamiento de riesgos de seguridad, teniendo en cuenta los ajustes de los procesos gestión de suministro de bienes y prestación de servicios, gestión financiera
3.0	15/01/2024	Todos	Se actualiza el plan de tratamiento de riesgos de seguridad,

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: 	Firma: 	Firma: 
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Imelda Muñoz Mancipe	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Jefe Oficina de Tecnología	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
		Comité Institucional de Gestión y Desempeño Acta N. 25-01-24 del 25 de enero de 2024