Oficina de Tecnología

Plan de Tratamiento de Riesgos de Seguridad en la Información

Versión 1.0
Enero 31 de 2022

Introducción

A través de la resolución 500 de 2021, se establecen lo 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 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 prácticas y 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 2022 con la implementación de actividades y controles establecidos en el plan de tratamiento de riesgos de seguridad de información que durante el 2021 no se culminaron.

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 de los 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 de seguridad 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.

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.

2. Política de Seguridad y Privacidad de la Información

1 https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

2 https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

A través de la resolución 000683 del 17 de diciembre de 2020 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 representa la seguridad de la información y considerándola como un factor fundamental para la gestión y operación del suministro de bienes y prestación de servicios, la infraestructura y el apoyo logístico y administrativo requeridos para el adecuado funcionamiento de los servicios penitenciarios y carcelarios a cargo del INPEC, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de los riesgos, cumplimiento de los objetivos de seguridad de la información, de los requisitos legales y organizacionales, de las 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

A continuación se presentan las actividades del plan de tratamiento de riesgos:

3.1 Gestión de Tecnologías de la Información

Control Norma ISO27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de disponibilidad y confidencialidad de información alojada en activos tipo software o servicios.(Interno y/o externos)					
A.9.2.1 Registro y cancelación del registro de usuarios	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento Gestión de Acceso a Usuarios.	Oficina de Tecnología - Grupo internode Seguridad	Resultado de verificación de procedimientos	2 reportesanuales	15/12/2022
Riesgo: Indisponibilidad de la plataforma tecnológica					
A.12.1.2 Control de cambios	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de control de cambios	Oficina de Tecnología	Reporte de seguimiento a procedimiento s	2 reportesanuales	15/12/2022
A.12.1.3 Gestión de la Capacidad	Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de gestión de la capacitación	Oficina de Tecnología	Reporte de seguimiento a procedimiento s	2 reportesanuales	15/12/2022

A.12.6.1 Gestión de las vulnerabilidades técnicas	Ejecutar el plan de remediación de vulnerabilidades de la plataforma tecnológica.	Oficina de Tecnología - Administradoresde plataforma tecnológica	Cuadro Control de gestión de vulnerabilidades diligenciado	Número de actividades ejecutadas del plan de remediación / Número de actividades programadas enel plan de remediación	20/11/2022

3.2 Gestión de Recursos Físicos y Suministros

Control Norma ISO27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de activos de información por ausencia de controles de acceso físico					
A.11.1.5 Trabajo en áreas Seguras	Actualizar la documentación de las zonas seguras de la Entidad definiendo los controles de acceso físico requeridos, así como las medidas de protección contra desastres naturales, ataques maliciosos o accidentes.	Coordinadora de Grupo de Administración de Personal (Se requiere apoyo por parte de los Directivos y Jefe que cuentan con zonas seguras)	Documento de zonas seguras actualizado	Documento aprobado, publicado ysocializado	30/11/2022
A.11.1.5 Trabajo en áreas Seguras	Designar a un responsable para el monitoreo permanente del Circuito Cerrado de Televisión de la Entidad. Realizar monitoreo en tiempo real del CCTV.	Director Administrativo y Financiero	Documento de delegación	Personal delegado para la supervisión.	31/3/2022

3.3 Gestión de Talento Humano

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de confidencialidad de las historias laborales de los funcionarios.					
A.8.2.3 Manejo de activos	Unificar matrices digitales de controlde documentos que deben reposar en historia laboral.	Coordinación Grupo Administración de Personal	Matriz digital de control	Matriz digital de control implementada	31/12/2022

3.4 Gestión de Infraestructura

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Fuga de información institucional por el uso de equipos portátiles personales					
A.6.2.1 Política para Dispositivos Móviles	Socializar el lineamiento para el usode portátiles y verificar que se está dando estricto cumplimiento al mismo, de acuerdo a las necesidades de la Dirección de Infraestructura.	Director de Infraestructura	Correo institucional conla solicitud	Solicitudes enviadas	15/12/2022
Riesgo: Pérdida de continuidad en la operación del proceso					
A.8.2.3. Manejo de activos	Actualizar lineamientos para la verificación del cargue de información de las gestiones adelantadas por el personal de la Dirección de Infraestructura en la carpeta compartida, a través de un método de operación establecido por la Entidad.	Director de Infraestructura	Método de operación actualizado	Documento actualizado	15/12/2022
Riesgo: Pérdida de confidencialidad de los planos de los ERONES					
A.8.2.3. Manejo de activos	Actualizar la directriz para el manejo de planos institucionales incluyendo lineamientos para elacceso de personal externo de la Entidad, y documentarse en un método de operación.	Director de Infraestructura	Método de operación actualizado	Documento actualizado	15/12/2022

3.5 Gestión Jurídica

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de confidencialidad de información clasificada y reservada					
A.8.2.1 Clasificación de la Información	Actualizar el A2-FO-03 Índice de Información Clasificada y Reservada con la información suministrada por las dependencias, realizar su correspondiente aprobación y publicación en el portal web de la Entidad.	Dependencias con el apoyo dela Oficina Asesora Jurídica	A2-FO-03 Índice de Información Clasificada y Reservada	1 Documento aprobado y publicado	15/12/2022

3.6 Gestión de Suministro de Bienes y Prestación de Servicios

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de confidencialidad, integridad y disponibilidad de la información					
A.13.2.1 Políticas y procedimientos de transferencia de información	Formalizar el lineamiento para la transferencia y consulta de información del listado censal a través de un método de operación definido por la Entidad.	Dirección Logística	Método de operación que contiene el lineamiento	1 documento aprobado y socializado	31/3/2022
	Realizar seguimiento al cumplimiento del lineamiento establecido.	Dirección Logística	Reporte de seguimiento (Acta de reunión)	3 reportes	31/12/2022

3.7 Gestión Contractual

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de disponibilidad de las compras realizadas a través de la plataforma de Tienda Virtual					

A.9.2.1 Registro y cancelación del registro de usuarios	Actualizar el procedimiento M3-PR-12 Adquisiciones Tienda Virtual del Estado Colombiano estableciendo controles para centralizar la información de las compras realizadas por Tienda Virtual.	Directora deGestión Contractual	Procedimiento actualizado, aprobado y publicado	Documento publicado	15/12/2022

3.8 Gestión de Atención a Establecimientos de Reclusión

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de disponibilidad y confidencialidad de la información de la SUBAER					
A.7.2.2 Toma de conciencia, educación y formación en seguridad de información	Realizar seguimiento al cumplimiento y asistencia a las actividades de sensibilización	Subdirección de Establecimientos de Reclusión	Registro de seguimiento	1 registro	31/3/2022
A.11.2.4 Mantenimiento de los equipos	Definir método de operación y formato para el reporte del estado de los equipos asignados a los funcionarios de la SUBAER	Subdirección de Establecimientos de Reclusión	Método de operación - Formato	1 método de operación - 1 formato	31/12/2022
	Solicitar el requerimiento para la actualización, mantenimiento o reparación de los equipos portátiles o clientes livianos asignados a los funcionarios de la SUBAER	Subdirección de Establecimientos de Reclusión	Memorando	1 memorando	31/12/2022

4. Seguimiento

El seguimiento al plan de tratamiento de riesgos de seguridad de información se realizará cada trimestre. de manera trimestral según lo establecido en la Política de Administración de Riesgos de la Entidad, es decir a través del formato G1-S3-FO-08 Herramienta de Administración de Riesgos, hoja "Seguimiento¨.