Oficina de Tecnología

Plan de Tratamiento de Riesgos de Seguridad en la Información

Versión 1.0

Enero 15 de 2020

Tabla de contenido

Introducción

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 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. Así mismo se han definido otros lineamientos para mejorar los estándares de seguridad de información

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, la USPEC definió la "Política de Administración de Riesgos" incluyendo lineamientos establecidos por el DAFP a través de la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*". Esta guía definió los requisitos para la administración de riesgos de gestión, corrupción y seguridad digital a través de la identificación, análisis, valoración, tratamiento y seguimiento de aquellas acciones que permitirán mitigar los riesgos.

El presente plan se ejecutará durante el 2020 y reúne las actividades definidas en cada uno de los procesos institucionales en los cuales se identificaron riesgos de seguridad digital, así mismo se establecen responsables, indicadores, fechas de inicio y finalización de cada actividad y porcentajes de avance por cada trimestre.

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]

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

- **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 de las acciones definidas.

2. Alcance

Teniendo en cuenta la actualización del mapa de riesgos de seguridad digital realizada a finales del 2019, se establecieron acciones para aquellos riesgos catalogados como Altos y Extremos según lo contemplado en la Política de Administración de Riesgos de la Entidad, en tal sentido el presente plan comprende únicamente los siguientes procesos: Gestión Contractual, Gestión de la Infraestructura, Gestión de Suministro de Bienes y Prestación de Servicios, Gestión Administrativa y Financiera, Gestión Jurídica, Gestión de Talento Humano y Gestión de Tecnologías e la información.

3. Política de Seguridad y Privacidad de la Información

A través de la resolución 000705 del 10 de octubre de 2019 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 responsabilidades de todo el personal de la Entidad para el cumplimiento de la política.

4. Comité de Seguridad de la Información en la entidad

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

Actualmente la gestión requerida en este comité la asume el Comité Institucional de Gestión y Desempeño, creado a través de la Resolución 152 de 28 de febrero de 2018. Así mismo a través de la resolución 000705 del 2019 se establecen como responsabilidades para el Sistema de Gestión de Seguridad de Información las siguientes:

a. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la Entidad.
b. Revisar los diagnósticos del estado de la seguridad de la información
c. Acompañar e impulsar el desarrollo de proyectos de seguridad.
d. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
e. Realizar revisiones periódicas del SGSI (por lo menos cada 12 meses) y según los resultados de esta revisión definir las acciones pertinentes.
f. Promover la difusión y sensibilización de la seguridad de la información dentro de la Entidad.
g. Las demás funciones inherentes a la naturaleza del Comité.

5. Contexto de riesgos de seguridad digital

El Departamento Administrativo de la Función Pública - DAFP actualizó en octubre de 2018 la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*", unificando una metodología para administrar de manera efectiva los riesgos de corrupción, gestión y seguridad digital en las Entidades públicas. Adicionalmente esta guía estableció la evaluación de los controles definidos para mitigar los riesgos con el fin de determinar su efectividad de manera objetiva y definió un esquema de líneas de defensa, estableciendo roles y responsabilidades del personal involucrado en la gestión de riesgos. Para complementar esta guía en materia de seguridad digital se cuenta igualmente con el *"Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas".*

Tomando como referencia la documentación mencionada, la USPEC actualizó la Política de Administración de Riesgos estableciendo como objetivo Establecer los lineamientos para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de gestión, de corrupción y de seguridad digital, con el fin de prevenir de forma anticipada su ocurrencia y minimizar el impacto que pueda afectar el logro de los objetivos Institucionales

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

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

6.1 Gestión de las tecnologías de la información

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha inicio	Fecha fin	Trim. I	Trim. II	Trim. III	Trim. IV
							P	P	P	P
Riesgo: Pérdida de disponibilidad y confidencialidad de información alojada en activos tipo software o servicios.										
A.9.4.3 Sistema de Gestión de Contraseñas	* Actualizar la guía de gestión de contraseñas de la Entidad. * Realizar sensibilización entre todas las dependencias a cargo de la administración de servicios o aplicaciones con el fin de	Administradores de plataformas	* Guía de gestión de contraseñas * Cumplimiento plan de sensibilización	Porcentaje de cumplimiento del plan de sensibilización	01/02/2020	31/12/2020	*40%*	*20%*	*20%*	*20%*

	fortalecer las contraseñas. * Realizar seguimiento con los administradores de servicios o sistemas de información para verificar el cambio de las contraseñas.		* Actas de seguimiento							
A.9.2.1 Registro y cancelación del registro de usuarios	* Actualizar el procedimiento de registro y cancelación de cuentas de usuarios. * Realizar sensibilización entre todas las dependencias a cargo de la administración de servicios o aplicaciones. * Verificación de accesos de funcionarios y contratistas	Administradores de plataformas	*Procedimiento de registro y cancelación de cuentas * A3-FO-15 Gestión de Devolución de Activos de Información * A3-FO-01 Gestión y Entrega de Cuentas y/o de Equipos	Binario	01/02/2020	31/12/2020	40%	20%	20%	20%
A.18.1.2 Derechos de propiedad intelectual	* Diseñar una herramienta que permita llevar el control de las licencias con que cuenta la Entidad. Mensualmente se realizará control del estado de las licencias con el fin de determinar si se requiere realizar gestión para la actualización.	Coordinador de Grupo de Comunicaciones – Oficina de Tecnología	Informe de automatización y control de licenciamiento disponible en la USPEC	Binario	01/02/2020	31/12/2020	0%	50%	0%	50%
Riesgo: Indisponibilidad de la plataforma tecnológica										
A.9.2.3 Gestión de derechos de acceso privilegiado	* Realizar verificación de accesos a plataformas * Realizar actividades de sensibilización	Oficina de Tecnología	* Cumplimiento plan de sensibilización * Informe de verificación	Porcentaje de cumplimiento del plan de sensibilización	01/02/2020	31/12/2020	25%	25%	25%	25%
A.12.1.1 Procedimientos de operación documentados	*Realizar la actualización de procedimientos de operación. * Realizar seguimiento a la actualización de la documentación según hoja de ruta establecida por la OTEC	Jefe Oficina de Tecnología	*Hoja de ruta de actualización de procedimientos * Procedimientos actualizados	Número de procedimientos actualizados / Total de procedimientos programados en la hoja de ruta	01/02/2020	31/12/2020	50%	50%	0%	0%
Riesgo: Pérdida, daño o fuga de información digital de la Entidad.										
A.12.3.1 Respaldo de la Información	*Definir plan de pruebas de restauración de backup * Realizar seguimiento a la ejecución del plan	Oficina de Tecnología	* Plan de pruebas de restauración de backup * Informe de seguimiento	Número de pruebas ejecutadas / Total de pruebas programadas	01/02/2020	31/12/2020	0%	50%	0%	50%
A.7.2.2 Toma de conciencia, educación y formación en seguridad	* Realizar actividades de sensibilización sobre los lineamientos definidos por OTEC para la protección de la información. * Realizar seguimiento al personal de la Entidad con el fin de validar el almacenamiento de	Jefe Oficina de Tecnología	* Cumplimiento plan de sensibilización	Porcentaje de cumplimiento del plan de sensibilización	01/02/2020	31/12/2020	25%	25%	25%	25%

de informaci ón	información en las rutas establecidas.									

Como actividad adicional se incluye la siguiente:

Actividad	Responsable	Soporte	Indicador	Fecha inicio	Fecha fin	Trim. I	Trim. II	Trim. III	Trim. IV
						P	P	P	P
Nivelación del plan de tratamiento de riesgos de seguridad de información según actualización de riesgos de seguridad digital 2019	Dependencias involucradas	Plan de tratamiento de riesgos de seguridad de información actualizado	Binario	01/02/2020	30/03/2020	*100%*	*0%*	*0%*	*0%*

7. Seguimiento

El seguimiento al plan de tratamiento de riesgo se realizará de manera transversal 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”.

Revisó: Oscar Javier Suárez Ramos
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado