Oficina de Tecnología

Plan de Tratamiento de Riesgos de Seguridad en la Información

Versión 2.0
Abril 30 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]
- **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.

[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/

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

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 por cada proceso institucional con el cual se identificaron riesgos de seguridad digital:

Gestión de las tecnologías de la información

Control Norma ISO 27001	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.9.4.3 Sistema de Gestión de Contraseñas	* Actualizar la guía de gestión de contraseñas de la Entidad incluyendo el control de verificación semestral el reporte remitido por los administradores de servicios o sistemas de información para verificar la gestión realizada frente al cambio de las contraseñas. * Establecer lineamiento indicando que para la adquisición de nuevo software se debe dar cumplimiento a la guía de gestión de contraseñas de la Entidad y el procedimiento que contemple la adquisición de software en la Entidad. * Establecer el listado de los diferentes administradores de las plataformas o sistemas de información de la Entidad. * Realizar sensibilización entre todas las dependencias a cargo de la administración de servicios o aplicaciones con el fin de fortalecer las contraseñas.	* Oficina de Tecnología - Grupo interno de Seguridad	* Guía de gestión de contraseñas * Actas de sensibilización	*Guía actualizada, publicada y socializada	30/6/2020

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 y personal en general de la Entidad.	*Oficina de Tecnología - Grupo interno de Seguridad	*Procedimiento de registro y cancelación de cuentas de usuario	Procedimiento actualizado, aprobado y socializado.	31/7/2020
A.18.1.2 Derechos de propiedad intelectual	* Actualizar el procedimiento de instalación de software, incluyendo una herramienta de gestión de inventario de licenciamiento 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. * Socializar el procedimiento con el personal involucrado en su ejecución y demás personal de la Entidad.	Oficina de Tecnología - Grupo de Servicios de TI	*Procedimiento de instalación de software	Procedimiento actualizado, aprobado y socializado.	31/7/2020
Riesgo: Indisponibilidad de la plataforma tecnológica					
A.12.1.2 Control de cambios	-Actualizar procedimiento de control de cambios incluyendo respectivos controles para las modificaciones requeridas en la plataforma tecnológica -Socializar el procedimiento con el personal involucrado en su ejecución.	*Oficina de Tecnología - Grupo de Servicios de TI - Grupo de seguridad	Procedimiento de control de cambios	*Procedimiento actualizado, aprobado y socializado.	31/7/2020
A.11.2.2 Servicios de suministro	Establecer el plan de mantenimiento del aire acondicionado y el componente eléctrico de la Entidad incluyendo actividades, fechas, responsables y descripción de afectaciones sobre la plataforma tecnológica en el caso que se lleguen a presentar.	*Coordinadora Grupo Administrativo	*Plan de mantenimiento del centro de cómputo	*Plan definido, aprobado y socializado	31/7/2020
A.12.6.1 Gestión de las vulnerabilidades técnicas	Definir lineamiento incluyendo la gestión oportuna de vulnerabilidades, la actualización del cuadro de gestión de vulnerabilidades y el seguimiento semestral.	Jefe Oficina de Tecnología	Documento con lineamiento	Lineamiento socializado	30/4/2020
A.12.1.1 Procedimientos de operación documentados	Establecer hoja de ruta de actualización de los documentos de operación de la OTEC, realizar seguimiento a las actualizaciones realizadas y posteriormente socializar la documentación debidamente aprobada.	Jefe Oficina de Tecnología	*Hoja de ruta de actualización de procedimientos * Procedimientos actualizados	Número de procedimientos actualizados y socializados / Total de procedimientos programados en la hoja de ruta	31/7/2020
A.17.1.1 Planificación de la continuidad	Elaborar y socializar el plan de continuidad de negocio incluyendo los controles de seguridad requeridos. Esta labor se realizará con todas las dependencias de la	Jefe Oficina de Tecnología - Grupo Seguridad	Plan de continuidad de negocio	Plan aprobado, publicado y socializado	30/11/2020

de la seguridad de la información	Entidad				
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 estableciendo tiempos de seguimiento	Jefe Oficina de Tecnología - Administrador de backup	Plan de pruebas de restauración de backup	Plan de pruebas aprobado	30/4/2020
A.6.2.1 Política para Dispositivos Móviles	Establecer lineamientos para la autorización del uso de información institucional en los equipos portátiles (personales y propios de la USPEC) en la Entidad, incluyendo controles de seguridad de información. Las dependencias que requieran el uso de portátiles propios de la Entidad o externos deberán tener en cuenta estos lineamientos.	Jefe de Oficina de Tecnología - Coordinadora de Grupo Administrativo	Documento con lineamiento	Lineamiento socializado	30/11/2020
A.7.2.2 Toma de conciencia, educación y formación en seguridad de información	Definir y ejecutar plan de sensibilización y capacitación en seguridad de información incluyendo lineamientos definidos por OTEC para la protección de la información. Trimestralmente se realizará seguimiento a este plan con el fin de evaluar la ejecución de las actividades planeadas.	Jefe Oficina de Tecnología - Grupo seguridad Coordinadora de Grupo Talento Humano	Plan de sensibilización y capacitación en seguridad de información	Plan de sensibilización aprobado, publicado y ejecutado	15/12/2020

Gestión Administrativa y Financiera

Subproceso Gestión Documental

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de integridad de la información registrada en el software de correspondencia - INFODOC					
A.9.2.1 Registro y cancelación del registro de usuarios	Realizar a actualización de usuarios del software de correspondencia - INFODOC según el reporte suministrado por la Oficina de Tecnología respecto a usuarios habilitados en el directorio activo.	Coordinadora Grupo de Gestión Documental	Gestión de usuarios software de correspondencia - INFODOC	Número de usuarios deshabilitados / Total de usuarios que requieren deshabilitarse	31/11/2020

A.9.2.1 Registro y cancelación del registro de usuarios	Documentar y socializar lineamientos y controles para el reporte oportuno de todas las novedades de personal a las dependencias que gestionan usuarios.	Coordinadora Grupo Administración de Personal - Directora de Gestión Contractual	Documento que incluye lineamientos y controles	Documento aprobado y publicado	31/07/2020

Subproceso Gestión de Recursos Físicos y Suministros

Control Norma ISO 27001	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	Documentar 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	Documento aprobado, publicado y socializado	30/11/2020
A.11.1.5 Trabajo en áreas Seguras	Designar y capacitar 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 y acta de capacitación	Personal delegado para la supervisión.	30/11/2020

Gestión de Talento Humano

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Pérdida de confidencialidad de información por novedades del personal.					
A.9.2.1 Registro y cancelación del registro de usuarios	Documentar y socializar lineamientos y controles para el reporte oportuno de todas las novedades de personal a las dependencias que gestionan usuarios.	Coordinación Grupo Administración de Personal	Documento que incluye lineamientos y controles	Documento aprobado y publicado	31/07/2020
Riesgo: Pérdida de confidencialidad de las historias laborales de los funcionarios.					

A.11.1.5 Trabajo en áreas Seguras	Designar y capacitar 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 y acta de capacitación	Personal delegado para la supervisión.	30/11/2020
A.8.2.3 Manejo de activos	Definir, socializar y diligenciar matriz digital de control para llevar a cabo el registro de los documentos que se requiere anexar a las historias laborales	Coordinación Grupo Administración de Personal	Matriz digital de control	Documento elaborado y diligenciado	31/07/2020

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	Establecer lineamientos para la autorización del uso de información institucional en los equipos portátiles (personales y propios de la USPEC) en la Entidad, incluyendo controles de seguridad de información. Las dependencias que requieran el uso de portátiles propios de la Entidad o externos deberán tener en cuenta estos lineamientos.	Jefe Oficina de Tecnología - Director Administrativo y Financiero	Documento que contenga el lineamiento	Documento aprobado, publicado y socializado	30/11/2020
Riesgo: Pérdida de continuidad en la operación del proceso					
A.8.2.3. Manejo de activos	Establecer directriz para la revisión del contenido de las carpetas de los contratos , incluyendo la notificación que se se deberá remitir por correo electrónico a los supervisores y al Director de Infraestructura y los controles de seguridad de información.	Director de Infraestructura	Documento que contenga la directriz	Documento aprobado, publicado y socializado	30/11/2020
Riesgo: Pérdida de confidencialidad de los planos de los ERONES					
A.8.2.3. Manejo de activos	Establecer directriz para la consulta de planos físicos y consulta y modificación de planos digitales, incluyendo tiempos de consulta y controles de seguridad de información.	Director de Infraestructura	Documento que contenga la directriz	Documento aprobado, publicado y socializado	30/11/2020

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 A3MA02 - Manual de clasificación de activos incluyendo los lineamientos de clasificación para llevar a cabo la construcción del índice de información clasificado y reservado y adicionalmente Responsabilizar al jefe de cada dependencia de la Disponibilidad, Integridad y Confidencialidad de la información (Pública, Clasificada y Reservada) que se encuentre bajo su custodia, por lo cual no se podrá suministrar la información sin su previo consentimiento. *Construir el índice de información clasificado y reservado de la Entidad con el apoyo de las dependencias.	Oficina Asesora Jurídica, Oficina de Tecnología, Grupo de Gestión Documental (Actualización de manual) Oficina Asesora Jurídica con el apoyo de todas las dependencias (Construcción de índice de información clasificado y reservado)	A3MA02 - Manual de clasificación de información Índice de información clasificada y *reservada	Documentos aprobados y publicados Documentos aprobados y publicados	Actualización de manual. 31/07/2020 Índice de información clasificado y reservado 31/10/2020
A.8.2.3 Manejo de Activos	Etiquetar la información de cada dependencia aplicando los lineamientos previamente socializados	Todas las dependencias	Documentos etiquetados	Número de carpetas etiquetadas por dependencia / Total de carpetas por dependencia	31/03/2021

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:

Diana Paola Cardenas Huertas
Profesional Universitario

Mayra Alexandra Agudelo Carvajal
Profesional Especializado