## Oficina de Tecnología

# Plan de Tratamiento de Riesgos de Seguridad en la Información

***Versión 1.0***
***Diciembre 23 de 2020***

# Tabla de contenido

**Introducción** 2

**Glosario** 3

1. 5
   1.1 5
   1.2 5
2. 5
3. 5
4. **¡Error! Marcador no definido.**
5. 6
6. 6
   6.1 6
7. 11

# 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 y en cumplimiento con la actual “Política de Administración de Riesgos” de la USPEC, se llevó a cabo un análisis del avance del plan de tratamiento de riesgos de seguridad de información para la vigencia 2020, así como de la ejecución de los controles diseñados, como producto de esta revisión se realizó la actualización del mapa de riesgos de seguridad de información y su respectivo PTR para el 2021.

## 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.

## 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

[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 responsabilidades de 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.

## 4. 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 en el 2019 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.

## 5. Formulación del Plan de Tratamiento de Riesgos de Seguridad digital

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

### 5.1 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 | Realizar auditoria de sistemas de información o aplicaciones de la Entidad incluyendo la verificación de lineamientos incluidos en la A3-GU-01 Guía Manejo de Contraseñas Seguras. | Oficina de Tecnología - Grupo interno de Seguridad | Informe de auditoría | 1 informe | 15/12/2021 |
| A.9.2.1 Registro y cancelación del registro de usuarios | Sensibilizar a los administradores de plataformas de la Oficina de Tecnología el procedimiento de Gestión de Acceso a Usuarios con el fin de ejecutarlo adecuadamente. | Oficina de Tecnología - Grupo interno de Seguridad | Acta de socialización | 1 acta | 30/3/2021 |
| | Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento Gestión de Acceso a Usuarios. | Oficina de Tecnología - Grupo interno de Seguridad | Resultado de verificación de procedimientos | 2 reportes anuales | 15/12/2021 |
| **Riesgo: Indisponibilidad de la plataforma tecnológica** | | | | | |
| A.12.1.2 Control de cambios | Sensibilizar al personal a cargo de la ejecución del procedimiento de control de cambios con el fin de generar la evidencia correspondiente en cada solicitud de cambio. | Oficina de Tecnología - Grupo interno de Seguridad | Actas de socialización | 1 acta | 16/4/2021 |
| | Realizar seguimiento semestral al diligenciamiento de los registros establecidos en el procedimiento de control de cambios | Oficina de Tecnología | Reporte de seguimiento a procedimientos | 2 reportes anuales | 15/12/2021 |
| 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 procedimientos | 2 reportes anuales | 15/12/2021 |
| A.12.6.1 Gestión de las vulnerabilidades técnicas | Ejecutar el plan de remediación de vulnerabilidades de la plataforma tecnológica. | Oficina de Tecnología - Administradores de plataforma tecnológica | Cuadro Control de gestión de vulnerabilidades diligenciado | Número de actividades ejecutadas del plan de remediación / Número de actividades programadas en el plan de remediación | 20/11/2021 |
| | Realizar seguimiento al plan de remediación de vulnerabilidades de la plataforma tecnológica. | Oficina de Tecnología - Grupo interno de Seguridad | Seguimiento al Cuadro Control de gestión de vulnerabilidades | 2 seguimientos | 15/12/2021 |
| A.17.1.1 Planificación de la continuidad de la seguridad de la información | Realizar y documentar las pruebas del plan de continuidad de TI, teniendo en cuenta el resultado de las pruebas se deberán realizar ajustes al plan. | Jefe Oficina de Tecnología | Resultado de pruebas de continuidad de TI | 1 documento | 30/11/2021 |
| **Riesgo: Pérdida, daño o fuga de información digital de la Entidad.** | | | | | |
| A.7.2.2 Toma de conciencia, educación y formación en | Ejecutar plan de sensibilización y capacitación en seguridad de información | Jefe Oficina de Tecnología - Grupo interno de seguridad | Seguimiento al plan | 4 seguimientos | 15/12/2020 |

| | | | | | |
|---|---|---|---|---|---|
| seguridad de información | | Coordinadora de Grupo Talento Humano | | | |

## 5.2 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 | Diligenciar los registros para la adecuada gestión de usuarios de la plataforma INFODOC, según los lineamientos establecidos por la OTEC | Coordinadora Grupo Gestión Documental | Formato diligenciado | (Número de registros en el formato durante el trimestre / Número total de solicitudes en el trimestre)*0.25 | 15/12/2021 |

### 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 | 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 y socializado | 30/11/2021 |
| 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. | 31/3/2021 |

## 5.3 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 | Definir lineamiento de acuerdo a los métodos de operación establecidos por la Entidad, para la entrega de documentos que deben reposar en la historia laboral de cada funcionario. | Coordinación Grupo Administración de Personal | Método de operación | Documento elaborado y diligenciado | 30/9/2021 |
| | Unificar matrices digitales de control de documentos que deben reposar en historia laboral. | Coordinación Grupo Administracion de Personal | Matriz digital de control | Matriz digital de control implementada | 31/12/2021 |

## 5.4 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 uso de 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 con la solicitud | Solicitudes enviadas | 15/12/2021 |
| **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 | 15/12/2021 |
| **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 el acceso de personal externo de la Entidad, y documentarse en un método de operación. | Director de Infraestructura | Método de operación actualizado | Documento actualizado | 15/12/2021 |

## 5.5 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 de la Oficina Asesora Jurídica | A2-FO-03 Índice de Información Clasificada y Reservada | 1 Documento aprobado y publicado | 15/12/2021 |
| A.8.2.3 Manejo de Activos | Socializar con las diferentes dependencias los lineamientos establecidos en el A3-MA-02 Manual de Clasificación de Activos | Grupo de Gestión Documental - Oficina Jurídica - Oficina de Tecnología | Acta de socialización | Documento socializado | 31/03/2021 |

## 5.6 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 | 31/3/2021 |
| | Realizar seguimiento al cumplimiento del lineamiento establecido. | Dirección Logística | Reporte de seguimiento (Acta de reunión) | 3 reportes | 31/12/2021 |

## 5.7 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 de Gestión Contractual | Procedimiento actualizado, aprobado y publicado | Documento publicado | 15/12/2021 |
| | Diligenciar el formato A3-FO-49 Trazabilidad de Cuentas de Usuario de acuerdo a las necesidades de la Entidad | Administrador de plataforma Tienda Virtual | Formato diligenciado | Formato diligenciado y actualizado | 15/12/2021 |

## 6. 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”.