Oficina de Tecnología

Plan de Tratamiento de Riesgos de Seguridad en la Información

Versión 2.1
Junio 14 de 2023

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 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 2023 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 cada uno de los procesos institucionales. A través de la presente versión, se actualizan las actividades de tratamiento para los procesos Gestión Financiera, Gestión Jurídica y Gestión de Recursos Físicos y Suministros.

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, 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 de las acciones definidas y la implementación de controles

2. Política de Seguridad y Privacidad de la 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. Actualización 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: Posibilidad de pérdida de disponibilidad por fallas en el suministro del fluido eléctrico debido a la falta de mantenimiento de los componentes de la infraestructura tecnológica					
A.11.2.4 Mantenimiento de los equipos	Actualizar el plan de mantenimiento de la plataforma tecnológica	Jefe Oficina de Tecnología	Plan de mantenimiento actualizado y socializado	1 plan actualizado y socializado	15-01-2023 al 30-03-2023
	Realizar seguimiento semestral al plan de mantenimiento de la plataforma tecnológica	Administradores de plataforma tecnológica	Seguimiento al plan de mantenimiento con la gestión del trimestre	3 seguimientos	01-04-2023 al 31-12-2023
Riesgo: Posibilidad de pérdida de disponibilidad por cambios sin autorización en los servicios que componen la plataforma tecnológica debido a la falta de gestión por parte de la supervisión de apoyo a los proveedores de TI					
A.12.1.2 Gestión de cambios	Definir a través de un documento de apoyo de la OTEC, los lineamientos para llevar a cabo la gestión de proveedores de TI (Este documento será parte de la operación de TI por lo tanto no se formalizará dentro de la documentación de MIPGESTION)	Jefe Oficina de Tecnología	Documento de apoyo aprobado y socializado	1 documento de apoyo aprobado por la Jefe de OTEC y socializado	01-02-2023 al 31-03-2023
	Realizar seguimiento al diligenciamiento del formato TI-PR-013 control de cambios	Encargado de SGSI	Soportes formato control de cambios	2 revisiones de los soportes del formato de control de cambios	15-01-2023 al 31-12-2023
Riesgo: Posibilidad de pérdida de disponibilidad por interrupción en la operación de los servicios de TI debido a que no se realiza una adecuada gestión de la capacidad y las vulnerabilidades de la plataforma tecnológica					

A.12.1.3 Gestión de la capacidad	Realizar seguimiento trimestral al estado de la plataforma de TI de acuerdo a los umbrales de gestión de la capacidad	Administradores de plataforma tecnológica	Informe de gestión de la capacidad con el análisis del trimestre	4 informes de gestión de la capacidad	15-01-2023 al 31-12-2023
A.12.6 Gestión de la vulnerabilidad técnica	Definir a través de un método de operación los lineamientos de gestión de vulnerabilidades de la plataforma tecnológica	Administradores de plataforma tecnológica Encargado de Seguridad de Información	Método de operación aprobado, publicado y socializado	1 método de operación aprobado, publicado y socializado	01-02-2023 al 31-03-2023
	Realizar seguimiento al plan de remediación de vulnerabilidades	Coordinador del Grupo de Comunicaciones	Seguimiento del plan de remediación de vulnerabilidades con la gestión realizada durante el trimestre	2 seguimientos del plan de remediación de vulnerabilidades	01-07-2023 al 31-12-2023
A.12.1 Procedimientos operacionales y responsabilidades	Definir el cronograma de actualización de documentos de operación de la plataforma tecnológica	Administradores de plataforma tecnológica Encargado de Seguridad de Información	Cronograma definido	1 cronograma	01-02-2023 al 31-03-2023
	Realizar seguimiento trimestral a la ejecución del cronograma de actualización de documentos de operación de la plataforma tecnológica	Encargado de Seguridad de Información	Cronograma con seguimiento de la gestión realizada durante el trimestre	3 seguimientos	01-04-2023 al 15-12-2023
Riesgo: Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por fuga de información debido a la falta de gestión sobre los documentos electrónicos					
A.8.2.3 Manejo de activos	Definir cronograma de implementación de controles para evitar fuga de información	Jefe Oficina de Tecnología	Cronograma definido	1 cronograma definido	01-02-2023 al 31-03-2023
	Realizar seguimiento a cronograma	Jefe Oficina de Tecnología	Cronograma con seguimiento de la gestión realizada durante el trimestre	3 seguimientos	01-04-2023 al 15-12-2023

3.2 Gestión de Recursos Físicos y Suministros

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por acceso físico no autorizado o pérdida de activos de información debido a que no se cuenta con lineamientos para la gestión de seguridad física de las zonas seguras					
A.11.1.2 Controles de acceso físicos	Documentar las necesidades de los controles de acceso o mejora, requeridos para las zonas seguras por sus responsables para garantizar la seguridad de los mismos.	Coordinadora Grupo Administrativo (Responsables de zonas seguras)	Solicitud a los responsables de zonas seguras Requisitos de las zonas seguras entregadas por el responsable de proceso Documento análisis de los controles de las zonas seguras	1 documento	15-06-2023 al 15-12-2023
	Realizar seguimiento a las actividades de mantenimiento de los controles ubicados en las zonas seguras	Coordinadora Grupo Administrativo	Soportes de actividades de mantenimiento realizadas durante el trimestre	4 reportes de actividades mantenimiento	15-02-2023 al 15-12-2023
	Documentar dentro de un método de operación los lineamientos para el adecuado uso y protección de las zonas seguras	Coordinadora Grupo Administrativo	Borrador del método de operación Método de operación aprobado, publicado y socializado	Método de operación publicado y socializado	15-04-2023 al 15-12-2023
Riesgo: Posibilidad de pérdida de confidencialidad, integridad y disponibilidad por acceso no autorizado a la información debido a que no se cuenta con controles definidos sobre el uso interno y externo de equipos portátiles					
A.11.2 Equipos	Documentar a través de un método de operación los lineamientos para el uso de los equipos portátiles en la Entidad, incluyendo los propios y los personales y el formato de gestión de préstamos y entrega de los mismos.	Coordinadora Grupo Administrativo	Borrador del método de operación Método de operación aprobado, publicado y socializado	1 Método de operación publicado y socializado	15-04-2023 al 15-12-2023
	Realizar seguimiento al préstamo y entrega de equipos portátiles	Coordinadora Grupo Administrativo	Soportes de gestión de equipos portátiles realizadas durante el trimestre	Matriz de seguimiento	15-01-2023 al 31-12-2023

3.3 Gestión de Talento Humano

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de confidencialidad por acceso no autorizado a la información debido a que no se aplican lineamientos de autorización de datos personales de la información recepcionada a través de actividades de bienestar.					
A.8.2.3 Manejo de activos	Realizar seguimiento a la revisión de los formularios que recolectan datos personales producto de las actividades de bienestar	Coordinador Grupo Talento Humano	Consolidado de correos de seguimiento	2 reportes con el registros de seguimiento	15-01-2023 al 15-12-2023
Riesgo: Posibilidad de pérdida de confidencialidad por acceso no autorizado a las historias laborales de los funcionarios de la Entidad debido al control inadecuado del acceso físico a la zona segura donde se aloja la información					
A.11.1.2 Controles de acceso físicos	Realizar seguimiento al funcionamiento de los controles de la zona segura donde se encuentran almacenadas las hojas de vida	Encargado de hojas de vida	Reporte informando la revisión realizada durante el trimestre	4 reportes	01-02-2023 al 31-12-2023
Riesgo: Posibilidad de pérdida de confidencialidad por uso indebido de los sistemas de información debido al reporte inoportuno de las novedades de personal					
A.9.2.6 Retiro o ajuste de los derechos de acceso	Reportar las novedades de personal a las dependencias encargadas de los recursos de TI	Coordinador Grupo Administración de Personal	Consolidado de reportes enviadas durante el trimestre	4 reportes	01-02-2023 al 31-12-2023

3.4 Gestión de Infraestructura

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de Pérdida de confidencialidad por acceso no autorizado a los planos de los ERONES debido a la ausencia de lineamientos internos para la transferencia de la información					
A.13.2.1 Política y procedimientos de transferencia de información	Elaborar el método de operación que contiene los lineamientos para llevar a cabo la transferencia de información confidencial	Jefe Oficina de Tecnología - Dirección de Infraestructura (Apoyo)	Borrador del método de operación Método de operación publicado, socializado	1 método de operación actualizado	01-02-2023 al 30-04-2023

	Registrar la trazabilidad de las transferencias realizadas durante el trimestre	Encargado de los planos	Formato de trazabilidad diligenciado con las transferencias realizadas durante el trimestre	Registro de trazabilidad diligenciad	01-05-2023 al 31-12-2023
Riesgo: Posibilidad de Pérdida de disponibilidad por cambios no autorizados de la información alojada en las carpetas compartidas debido al manejo inadecuado de los recursos tecnológicos					
A.7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación	Realizar seguimiento a los asistentes de la Dirección de Infraestructura a las actividades de sensibilización	Jefe Oficina de Tecnología	Memorando con el reporte de asistentes a las actividades de sensibilización	Registro de seguimient o	01-05-2023 al 31-12-2023
A.8.1.4 Devolución de los activos	Verificar la entrega de información por parte del personal que se desvincula de la Entidad	Supervisor de contrato (DINFRA)	Paz y salvo diligenciado por cada personal que culmina su vínculo laboral con la entidad	Paz y salvo diligenciado firmado por el supervisor de contrato	01-02-2023 al 31-12-2023

3.5 Gestión Atención al Ciudadano

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de confidencialidad e integridad por daño causado por un tercero debido a que no se aplican lineamientos para el uso y tratamiento de información personal en las gestiones propias de la entidad					
A.8.2.3 Manejo de activos	Solicitar la modificación del software INFODOC - Módulo PQRSD, con el fin de modificar la autorización de datos personales por parte de la ciudadanía	Coordinadora del Grupo de Atención al Ciudadano	Memorando radicado en INFODOC	1 Memorando	02-01-2023 al 31-03-2023
	Actualizar política de datos personales - AC-PO-001, incluyendo lineamientos para la captura de datos personales de las dependencias que recepcionan este tipo de información	Coordinadora del Grupo de Atención al Ciudadano	Borrador de actualización de política Documento de política aprobado, publicado y socializado	1 Política aprobada, publicada y socializada	01-02-2023 al 30-06-2023
	Realizar capacitación frente al manejo de datos personales de la Entidad	Coordinadora del Grupo de Atención al Ciudadano	Listado de asistencia con el personal capacitado	1 Listado de asistencia	01-10-2023 al 31-12-2023

3.6 Gestión Contractual

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de disponibilidad por fallo en los reportes de las compras realizadas a través de tienda virtual debido a la ausencia de lineamientos para la gestión de la información					
A.8.2.3 Manejo de activos	Actualizar el método de operación que permite consolidar el registro de las compras realizadas por la Entidad a través de la plataforma de tienda virtual	Director de Gestión Contractual	Método de operación radicado en la OAPLA para revisión Método de operación publicado y socializado	1 método de operación actualizado	01-02-2023 al 15-12-2023
	Registrar en la matriz de contratación las órdenes de compra realizadas por los ordenadores de gasto de la Entidad	Analista de sistemas	Reporte mensual de la matriz de contratación	Reporte matriz de contratación	01-02-2023 al 15-12-2023

3.7 Gestión Documental

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de Pérdida de integridad por uso no autorizado de software debido a la baja implementación de lineamientos para eliminar los derechos de acceso a la terminación del empleo.					
A.9.2.1 Registro y cancelación de cuentas de usuario	Realizar seguimiento al diligenciamiento del formato TI-FO-049 trazabilidad de cuentas de usuario	Coordinadora del Grupo Gestión Documental	Formato de trazabilidad de Cuentas de usuario diligenciado con el registro de usuarios del semestre	2 reportes	15-01-2023 al 31-12-2023

3.8 Gestión Financiera

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de confidencialidad e integridad por acceso no autorizado a la información debido al inadecuada gestión y protección de los de los dispositivos criptográficos (tokens)					
A.9.2.1 Registro y cancelación del registro de usuarios	Capacitar al personal de la Subdirección Financiera que se encuentra a cargo de la gestión de la plataforma SIIF Nación, en cuanto a los lineamientos del Sistema de Gestión de Seguridad de Información y las directrices definidas por Ministerio de Hacienda para el correcto de uso del sistema y la información de la USPEC alojada en el mismo.	Oficina de Tecnología - Subdirección Financiera	Acta de capacitación	1 acta de capacitación	17-09-2023 al 30-09-2023
	Diligenciar el formato TI-FO-049 trazabilidad de cuentas de usuario registrando las acciones realizadas en la plataforma SIIF Nación	Administrador SIIF Nación Entidad	Formato trazabilidad de cuentas de usuario con la gestión realizada durante el trimestre	2 reportes formato trazabilidad de cuentas de usuario diligenciados	01-04-2023 al 31-12-2023
	Definir a través de un método de operación los lineamientos para la gestión de usuarios y perfiles de la plataforma SIIF Nación.	Oficina de Tecnología - Subdirección Financiera - Oficina Asesora de Planeación y Desarrollo	Borrador de procedimiento remitido a la Oficina de Planeación Procedimiento aprobado, publicado y socializado	Método de operación aprobado, publicado y socializado	15-05-2023 al 15-09-2023

3.9 Gestión Jurídica

Control Norma ISO 27001	Actividad	Responsable	Soporte	Indicador	Fecha
Riesgo: Posibilidad de pérdida de confidencialidad por acceso no autorizado a los activos debido a la inadecuada clasificación de información clasificada y reservada de la entidad					
A.8.2.3 Manejo de activos	Actualizar y aprobar el índice de información clasificada y reservada de la entidad de acuerdo a las necesidades presentadas por las dependencias	Jefe Oficina Asesora Jurídica	Acta de comité de gestión y desempeño y resolución con la aprobación del Índice de información clasificada y reservada	Índice de información clasificada y reservada aprobado	15-01-2023 al 31-03-2023
	Realizar la entrega del índice de información clasificada y reservada - IICR a cada dependencia a través de correo institucional, informando las directrices de seguridad a tener en cuenta	Jefe Oficina Asesora Jurídica	Correos electrónicos	Correos enviados a cada dependencia que cuenta con IICR	06-06-2023 al 30-06-2023

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.

5. Aprobación

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección a través del Comité Institucional de Gestión y Desempeño y de los dueños de los riesgos, con el objetivo de ser actualizado, aprobado y aplicado conforme a lo que aquí se define. Lo anterior según lo establecido en el Modelo de Seguridad y Privacidad de Información Versión 4.0, establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

ACTUALIZÓ	REVISÓ	APROBÓ
Nombre: Mayra Alexandra Agudelo Carvajal **Cargo**: Profesional Especializado **Dependencia**: Oficina de Tecnología	**Nombre**: Imelda Muñoz Mancipe **Cargo**: Jefe Oficina de Tecnología **Dependencia**: Oficina de Tecnología	Comité Institucional de Gestión y Desempeño Acta N. 4 del 14 de junio de 2023.