RESOLUCIÓN NÚMERO 000008 **DEL** 9/1/2025 16:54:30

"Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la Entidad y la política de privacidad y seguridad de la información y se deroga la Resolución 000181 del 17 de abril de 2022"

LA DIRECTORA GENERAL (E) DE LA UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS

En uso de las facultades legales y en especial la conferida en el numeral 15 del artículo 12 del Decreto 4150 del 3 de noviembre de 2011, y la Resolución No.00022 del 3 de enero de 2025, expedida por el Ministerio de Justicia y del Derecho, y

CONSIDERANDO

Que, el artículo 12 del Decreto 4150 de 2011 faculta al Director General para implementar, mantener y mejorar el Sistema de Gestión Institucional de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC.

Que, el Decreto 1377 de 2013, reglamenta la Ley 1581 de 2012, que trata sobre la protección de datos personales en Colombia y regula la protección de la información contenida en sistemas y equipos informáticos.

Que, el Decreto 1499 de 2017, por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, adopta la actualización del Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su título 2, capítulo 1, artículo 2.2.22.3.2 como "(...) un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio". Así mismo en su capítulo 2, artículo 2.2.22.2.1 se define "Las Políticas de Gestión y Desempeño Institucional. Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominan políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes (…) 12. Seguridad Digital".

Que, el capítulo I sección 2 artículo 2.2.9.1.1.3. del Decreto 1008 de 2018 incluye la seguridad de la Información entre los principios de la Política de Gobierno Digital, igualmente el artículo 2.2.9.1.2.1 define la seguridad de la información como habilitador transversal de la Política de Gobierno Digital que junto con los demás habilitadores permiten el desarrollo de los componentes y logros incluidos en dicha política.

Que, el parágrafo del artículo 16 del Decreto 2016 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

Que, la Ley 527 de 1999 define la firma digital como "Un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación "

Que, la ley 1581 de 2012 establece los requisitos para el tratamiento de los datos personales, garantizando la protección de la privacidad de los individuos y el cumplimiento de los derechos de habeas data.

Que, el CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia y busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica del país.

Que el CONPES 3995 del 2020 establece la Política Nacional de Confianza y Seguridad Digital, a través de los cuales se pretende establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que, a través de la Resolución 1519 de 2020 por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Que, a través de la Resolución 500 de 2021, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, "se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital". Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el

Procedimiento para la gestión de los incidentes de seguridad digital, así mismo, establece las directrices y estándares para la estrategia de seguridad digital. a los sujetos obligados señalados en el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015.

El artículo 5 de la misma resolución establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, formatos, manuales y lineamientos para la

gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de Información que se integra al plan de acción en los términos del artículo 2.2.22.3.14 del capítulo 3 del Titulo 2 de la parte 2 del Libro 2 del Decreto 1083 del 2015, Único reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como adaptar el Modelo de Seguridad y Privacidad de Información – MSPI, señalado en el Anexo 1 de la misma resolución, como habilitador de la Política de Gobierno Digital.

Que, en la implementación del Sistema de Gestión de Seguridad de La Información (en adelante SGSI), es preciso establecer el alcance, la Política de Privacidad y Seguridad de la Información, los objetivos y los roles y responsabilidades de Seguridad de la Información, de conformidad con la norma NTC-ISO-IEC 27001:2022 a través del presente acto administrativo.

Que, a través del **NIST Cybersecurity Framework**, Marco de referencia desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos, se proporciona un enfoque basado en el riesgo para mejorar la ciberseguridad, buenas prácticas y brinda alternativas para mejorar la capacidad de recuperación de ciberataques en una organización.

Que, la Política de Protección de Datos Personales AC-PO-001, establece los criterios para la adecuada protección de la información personal recolectada por USPEC, a través del almacenamiento, uso y circulación de los datos, tratamiento y respuesta a PQRSD presentadas a la Entidad y el manejo de la información que reposa en el diligenciamiento de las encuestas de satisfacción y percepción de los grupos de valor

Que, a través de la Resolución 000181 de 2022 se actualizó la **política de privacidad y seguridad de la información** de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, siendo necesario actualizar las generalidades de la política, los roles y responsabilidades, la revisión, vigencia y derogatoria de la misma.

Que, en sesión del Comité Institucional de Gestión y Desempeño de la USPEC, celebrada el 10 de diciembre de 2024, se socializó a los miembros de este comité, la actualización efectuada al documento de la Política de Privacidad y Seguridad de la Información de la Entidad, y en la misma sesión, se dio aprobación por parte del comité a esta política.

Que en virtud de lo anterior;

RESOLUCIÓN NÚMERO 000008 **DEL** 9/1/2025 16:54:30

"Por la cual se actualizan los lineamientos del Sistema de Gestión de Seguridad de Información de la Entidad y la política de privacidad y seguridad de la información y se deroga la Resolución 000181 del 17 de abril de 2022"

RESUELVE:

CAPÍTULO I
GENERALIDADES DE LA POLÍTICA

ARTÍCULO 1. **Objeto**: La presente resolución tiene como objeto actualizar los lineamientos del Sistema de Gestión de Seguridad de información - SGSI y la Política Privacidad y Seguridad de la Información, en la USPEC, con el fin de mantener los requisitos para garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información de la Entidad a través de un SGSI robusto.

ARTÍCULO 2. Manual de Seguridad de la Información - TI-MA-03. Este Manual se adopta a través de la presente política y establece todos los parámetros técnicos y proporciona instrucciones específicas para implementar y mantener los controles de seguridad.

ARTÍCULO 3. Política General de Privacidad y Seguridad de la Información. Por la cual se actualiza la Política de Privacidad y de Seguridad de la Información que se incorpora con la presente resolución y quedará así:

"La USPEC, reconociendo la importancia estratégica de su información, ha adoptado el MSPI, y ha integrado este modelo al SGSI de la entidad, teniendo como objetivo principal preservar la confidencialidad, integridad y disponibilidad de los activos de información para el cumplimiento de la misión institucional, por lo tanto la USPEC se compromete a gestionar los riesgos, implementar controles de seguridad, cumplir con la normativa vigente y asignar los recursos necesarios para gestionar la mejora continua de dicho sistema de gestión".

ARTÍCULO 4. Objetivos de Seguridad de la Información. Como parte del proceso de implementación de la política se establecen los siguientes objetivos:

- Gestionar los riesgos de seguridad de la información a través de la identificación, evaluación y tratamiento de los riesgos que puedan afectar la seguridad de los activos de información, implementando controles de seguridad adecuados y proporcionales al nivel de riesgo.

- Promover una cultura de seguridad de la información a través de programas de capacitación y sensibilización dirigidos a todo el personal, con el objetivo de fomentar prácticas seguras en el manejo de la información.

- Gestionar incidentes de seguridad mediante la detección, respuesta, investigación y aprendizaje de los incidentes de seguridad, con el fin de minimizar sus impactos y prevenir futuras ocurrencias.

- Implementar un proceso de mejora continua basado en la evaluación del desempeño, el análisis de los resultados de auditorías (internas y externas) y la aplicación de acciones correctivas y preventivas.

- Monitorear y controlar el desempeño del Sistema de Gestión de la Seguridad de la Información alineados a las buenas prácticas, los marcos de referencia, la norma ISO 27000 y el MSPI.

ARTÍCULO 5. Alcance de la política. La presente Política de Privacidad Seguridad de la Información se aplica a todos los procesos institucionales, sistemas, aplicaciones, datos y activos de información de la USPEC, independientemente de su formato, medio o ubicación (incluyendo la nube).

Esta política abarca a todo el personal vinculado a la USPEC, contratistas, proveedores y cualquier otra persona o entes de control que tenga acceso a la información de la Entidad, ya sea de manera interna o externa. Asimismo, se aplica a toda la información que la USPEC crea, procesa, almacena o transmite, incluyendo datos personales, información confidencial, propiedad intelectual y cualquier otro tipo de información relevante para las operaciones de la entidad.

La implementación del SGSI se realizará de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información y los requisitos de la norma ISO 27001 en su versión vigente."

ARTÍCULO 6. **Compromiso de la Alta Dirección.** La Alta Dirección de la USPEC asume el compromiso de establecer, liderar, implementar, mantener y mejorar continuamente el SGSI. Para ello, garantizará la asignación de los recursos necesarios (humanos y tecnológicos), realizará revisiones semestrales del sistema y tomará las decisiones estratégicas en materia de seguridad de la información.

CAPÍTULO II
ROLES Y RESPONSABILIDADES DE SEGURIDAD DE INFORMACIÓN

ARTÍCULO 7. La implementación exitosa del SGSI requiere la participación activa de todos los miembros de la USPEC y el cumplimiento de todos los lineamientos establecidos a través del SGSI, adicionalmente se detallan los roles y responsabilidades específicas de cada actor involucrado:

A. Dirección General

Responsable por el direccionamiento estratégico e impulso del Sistema de Gestión de Seguridad de Información. Establece su compromiso, mediante la asignación de recursos, responsabilidades y revisiones internas. Como parte de la gestión de la Dirección General para seguridad de la información se establecerán los lineamientos para:

1. Asignar los roles y responsabilidades
2. Revisar y aprobar la política general, objetivos de seguridad.
3. Asignar los recursos necesarios para implementar y mantener el SGSI.
4. Revisar el Sistema de Gestión de Seguridad de la Información de la Entidad semestralmente.
5. Apoyar a los funcionarios y contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del SGSI.
6. Liderar la gestión del SGSI en la Entidad.

B. Responsables de proceso

Director, Jefe de Oficina o Líder encargado de proceso, quienes deberán asumir y ejecutar las siguientes responsabilidades:

1. Asignar los integrantes para la conformación del Equipo Operativo SGSI del proceso a cargo.
2. Difundir las políticas, procedimientos y demás documentos relacionados con el SGSI en su respectivo proceso.
3. Mantener actualizado el inventario de activos de información de su proceso.
4. Aplicar los controles de seguridad requeridos para la protección de los activos.
5. Liderar la gestión del proceso de gestión de riesgos de seguridad de la información de su proceso.
6. Definir, aprobar y ejecutar el plan de tratamiento de riesgos de seguridad de la información.
7. Asegurar la disponibilidad de recursos, para implementar los controles de seguridad definidos.
8. Promover la capacitación en seguridad de la información para todos los involucrados.
9. Liderar la mejora continua a través de la gestión de planes de mejora.
10. Aprobar la documentación relacionada con el SGSI.
11. Validar la entrega de los activos de información del personal que se encuentra a su cargo.
12. Cumplir con las demás responsabilidades establecidas en los procedimientos del SGSI.

C. Oficial de Seguridad de la Información

Responsable de garantizar la implementación y el mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI)

1. Implementar, mantener y mejorar de forma continua el SGSI, asegurando su alineación con las normas y regulaciones vigentes.
2. Coordinar la gestión de riesgos de seguridad de la información, actualizando continuamente el mapa de riesgos y los planes de tratamiento.
3. Promover la cultura de seguridad de la información a través de programas de capacitación y sensibilización.

4. Establecer y ejecutar los procedimientos para la detección, respuesta y recuperación ante incidentes de seguridad.
5. Coordinar y participar en auditorías internas y externas, asegurando el cumplimiento de la norma ISO 27001 y otras regulaciones aplicables.
6. Gestionar métricas y realizar un seguimiento continuo del desempeño del SGSI, generando reportes a la alta dirección.
7. Realizar seguimiento a la ejecución de todos los planes que forman parte del SGSI.

D. Comité Institucional de Gestión y Desempeño

La conformación de este Comité se encuentra establecida en la Resolución 613 del 03 de diciembre de 2020, por la cual se adopta el Modelo Integrado de Planeación y Gestión Institucional – MIPG en la USPEC. Se adoptarán las funciones relacionadas con la implementación del MIPG relacionadas con el SGSI.

E. Oficina Asesora Jurídica

1. Asesorar en materia legal y representar a la entidad en procesos judiciales relacionados con la política de privacidad y seguridad de la información y garantizar el cumplimiento normativo en materia de protección de datos
2. Realizar investigaciones internas en carácter disciplinario, caso de incidentes de seguridad de información relacionados con el personal vinculado a la Entidad, esto será previo al informe remitido por la dependencia que reporte el incidente.

F. Dirección de Gestión Contractual

1. Asegurar que los contratos con proveedores incluyan cláusulas, acuerdos de confidencialidad y no divulgación de la información y derechos de autor.

G. Grupo Administración de Personal

1. Gestionar la capacitación del personal en temas de seguridad de la información.
2. Implementar los controles requeridos en el proceso de vinculación y desvinculación del personal de planta de la Entidad.
3. Asegurar que el personal de planta cuenta con acuerdos de confidencialidad, no divulgación de la información y derechos de autor.
4. Comunicar oportunamente a la Oficina de Tecnología - OTEC cualquier modificación en el estado laboral o en las funciones del personal de planta, con el fin de realizar los ajustes necesarios en sus credenciales de acceso a sistemas y aplicaciones.

H. Oficina de Control Interno

1. Gestionar auditorías internas para verificar el cumplimiento del SGSI.

2. Verificar la efectividad de los controles de seguridad implementados a través de la ejecución de los planes de tratamiento de riesgos de seguridad.
3. Informar al Comité Institucional de Gestión y Desempeño sobre los resultados de las auditorías, incluyendo las no conformidades y las medidas correctivas para su mitigación.
4. Realizar seguimiento a los planes de mejoramiento de seguridad de información y determinar la efectividad de las acciones tomadas.

I. Oficina de Tecnología

1. Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información sobre los activos del proceso Gestión de Tecnologías de Información.
2. Monitorear los sistemas y redes en busca de actividades sospechosas o amenazas.

J. Equipo Operativo de Seguridad de Información

Este equipo está integrado por delegados de cada proceso institucional y dentro de sus responsabilidades se encuentran las siguientes:

1. Apoyar la identificación, clasificación y valoración de los activos de información, así como la gestión de los riesgos asociados.
2. Monitorear la implementación y eficacia de los planes de tratamiento de riesgos y otros controles de seguridad.
3. Participar en actividades de formación y sensibilización, y difundir las políticas de seguridad dentro de sus respectivos procesos.
4. Contribuir a la identificación de oportunidades de mejora y a la definición de planes de acción para fortalecer el SGSI.
5. Participar en las reuniones del equipo y colaborar con el Oficial de Seguridad de la Información.
6. El Equipo Operativo de Seguridad de la Información se reunirá de acuerdo con las necesidades del Sistema de Gestión de Seguridad de Información y por solicitud del Oficial de Seguridad de Información.

K. Funcionarios y Contratistas

1. Cumplir con los lineamientos establecidos en el SGSI.
2. Proteger los activos bajo su custodia, aplicando los controles de seguridad establecidos.
3. Reportar cualquier incidente o evento de seguridad de manera oportuna.
4. Manejar la información de forma segura, según las normas de clasificación y etiquetado establecidas.
5. Participar activamente en las actividades de capacitación y sensibilización en seguridad de la información.
6. Realizar la entrega de activos de información en el momento en que se desvinculen de la Entidad, de acuerdo a los lineamientos establecidos en el SGSI.

7. Contribuir a la mejora continua del SGSI.

L. Visitantes y Proveedores

1. Cumplir las políticas de seguridad de la información establecidas en la Entidad.
2. Utilizar únicamente la red de invitados para acceder a internet.
3. Utilizar la información institucional de acuerdo a los permisos conferidos por la Entidad.
4. Cumplir con los controles de seguridad establecidos a través del SGSI de la Entidad.
5. En caso requerido por la Entidad, se deben establecer acuerdos de confidencialidad de información.

CAPÍTULO III
REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO 8. Actualización del alcance, política, objetivos, roles y responsabilidades de seguridad de la información. La Política de Privacidad y Seguridad de la Información será revisada anualmente o de manera anticipada si se presentan situaciones que puedan impactar la seguridad de la información en la Entidad.

El responsable de realizar la actualización es el Oficial de Seguridad de la Información o quien ocupe dicho rol; cualquier modificación deberá ser aprobada por el Comité Institucional de Gestión y Desempeño y el Director General de la USPEC.

ARTÍCULO 9. Seguimiento, medición, análisis y evaluación del SGSI. La USPEC realizará revisiones semestrales para evaluar la conveniencia, adecuación y eficacia de la implementación del MSPI, conforme a los lineamientos de la Norma ISO 27001:2022 y mediante el informe de revisión por la dirección, generado por el Oficial de Seguridad de Información. Esta información será analizada por el Comité Institucional de Gestión y Desempeño, quien definirá los compromisos necesarios para la mejora continua del SGSI.

ARTÍCULO 10. Incumplimiento de las políticas y lineamientos de seguridad de información. El incumplimiento de las políticas de esta resolución, o la violación de procedimientos y lineamientos de seguridad de la información, leyes, decretos y demás normativas aplicables, constituirá un incidente de seguridad y será gestionado según los lineamientos de SGSI.

Para funcionarios, se notificará al jefe inmediato y, si corresponde, se iniciará un proceso disciplinario siguiendo el procedimiento **Procesos Disciplinarios JU-PR-0O2 a cargo de la Oficina Asesora Jurídica.**

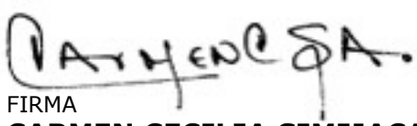
En el caso de contratistas, se notificará al interventor o supervisor del contrato y se enviará copia a la Dirección de Gestión Contractual para que realice las

investigaciones correspondientes. En el caso de terceros, se remitirá una solicitud de explicación al representante legal de la firma contratista, y en caso de manipulación indebida, se procederá a acciones penales; además, se notificará al interventor o supervisor del contrato.

ARTÍCULO 11. La presente Resolución entrará en vigencia a partir de la fecha de su expedición, y deroga la Resolución 000181 del 27 de abril de 2022, así como cualquier otra disposición que le sea contraria.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a los 9/1/2025 16:54:30



FIRMA
CARMEN CECILIA SIMIJACA AGUDELO
Directora General (E)
Unidad de Servicios Penitenciarios y Carcelarios

Elaboró: Daniel Ricardo Muñoz Alvarado Oficial de Seguridad de Información – Mayra Alexandra Agudelo Carvajal Profesional Especializado
Revisó: Imelda Muñoz Mancipe / Jefe Oficina de Tecnología
Control de Legalidad: Carmen Rosa Castañeda Quitian - Coordinadora Grupo de Acciones de Tutelas, Conceptos, Control de Legalidad y Derechos de Petición.
Revisó: Fabián Alberto Beltrán Mejía – Asesor Dirección General
Ruta: \\192.168.70.20\sigi\8 Formatos Vigentes\G1_PROCESO DE PLANEACIÓN ESTRATÉGICA Y GESTIÓN ORGANIZACIONAL\S1_DIRECCIONAMIENTO ESTRATÉGICO INSTITUCIONAL\G1-S1-FO-01_Resolución_2025.
Ubicación archivo físico: Carpeta SGSI

PROYECTO	MAYRA ALEXANDRA AGUDELO CARVAJAL PROFESIONAL ESPECIALIZADO 18 GRADO 18	12/27/2024 11:09:01 AM	
REVISO	IMELDA MUÑOZ MANCIPE JEFE DE OFICINA DE TECNOLOGÍA	12/27/2024 12:34:13 PM	
REVISO	CARMEN ROSA CASTAÑEDA QUITIAN COORDINADOR (A)	1/8/2025 19:13:36 PM	
REVISO	FABIAN ALBERTO BELTRAN MEJIA ASESOR APOYO A LA GESTION	1/9/2025 10:58:55 AM	
FIRMO	CARMEN CECILIA SIMIJACA AGUDELO JEFE OFICINA DE PLANEACION Y DESARROLLO	1/9/2025 4:54:24 PM