



000705

RESOLUCIÓN NÚMERO DEL 10 OCT 2019

"Por la cual se adopta una nueva política de seguridad y privacidad de información y se deroga la resolución 001046 del 27 de Noviembre de 2018"

**EL DIRECTOR GENERAL DE LA UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS**

En uso de las facultades legales y en especial la conferida en el artículo 12 del Decreto 4150 de 2011 y

**CONSIDERANDO**

Que el artículo 12 del Decreto 4150 de 2011 faculta al Director General para expedir actos administrativos necesarios para la ejecución y cumplimiento de la Política General de la Unidad de Servicios Penitenciarios y Carcelarios – USPEC.

Que el capítulo 1, sección 2, artículo 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 CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital en la República de Colombia.

Que a través de la Resolución 001046 del 2018 se modifica la política de seguridad de información y es necesario derogarla teniendo en cuenta los ajustes realizados a la plataforma estratégica de la USPEC, en tal sentido se cambia su nombre por Política General de Seguridad y Privacidad de Información y se modifican los objetivos de seguridad, los roles y responsabilidades de seguridad de información.

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 denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes" "...12. Seguridad 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 Seguridad de la Información, los objetivos y los roles y responsabilidades de Seguridad de la Información de conformidad con la norma NTC-ISO-IEC 27001:2013 a través del presente acto administrativo.

Que en virtud de lo anterior;

**RESUELVE:**

**ARTÍCULO 1. Objeto:** La presente resolución tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información en la Unidad de Servicios Penitenciarios y Carcelarios – USPEC, así como definir los roles y responsabilidades frente a la implementación del Sistema de Gestión de Seguridad de Información.

**ARTÍCULO 2. Política General de Seguridad y Privacidad de la Información.** Por la cual se adopta la Política General de Seguridad y Privacidad de la Información que se incorpora con la presente resolución y quedará así:

*"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*



**MINJUSTICIA**



000705

10 OCT 2019

RESOLUCIÓN NÚMERO DEL

*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".*

**ARTÍCULO 3. Objetivos de Seguridad de la Información.** Para la implementación de la presente política se establecen los siguientes objetivos generales:

- ✓ Gestionar los riesgos de seguridad digital, con el fin de implementar controles que permitan proteger los activos de información que soportan la estrategia y operación de la Entidad.
- ✓ Capacitar y sensibilizar al personal de la USPEC en temas relacionados con seguridad de la información.
- ✓ Gestionar los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas.
- ✓ Implementar acciones preventivas, correctivas y de mejora generadas como resultado de las auditorías internas, externas con el fin de apoyar la mejora continua del sistema de gestión de seguridad de información.

**PARAGRAFO PRIMERO.** El Oficial de Seguridad de Información o quien haga sus veces debe establecer el plan para el logro de los objetivos de seguridad de información y realizar seguimiento al mismo de manera semestral.

**ARTÍCULO 4. Alcance de la Política.** La Política de Seguridad y Privacidad de la Información aplica a todos los procesos institucionales incluidos los estratégicos, misionales, de apoyo, evaluación y control, así como a todos los funcionarios, contratistas, proveedores y todos los terceros que en ejercicio de sus funciones y las propias de la Entidad tengan acceso o gestionen la información institucional, así como los Entes de Control u otras Entidades que accedan a la misma. La implementación del SGSI en la USPEC se realizará acorde a los lineamientos contenidos en el Modelo de Seguridad y Privacidad de la Información y los requisitos de la Norma ISO 27001 en su versión vigente.

**ARTÍCULO 5. Representante de la Dirección General.** El representante de la Dirección General para el SGSI es el Oficial de Seguridad de Información de la USPEC o en su ausencia el Jefe de la Oficina de Tecnología.

**ARTÍCULO 6. Roles y Responsabilidades del SGSI.** A continuación se describen tanto los roles como las responsabilidades que se deben asumir al interior de la USPEC para la gestión del Sistema de Gestión de Seguridad de Información.

- 1. 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 encuentran las siguientes responsabilidades:
  - a. Asegurar que se definan y asignen los roles y responsabilidades de seguridad de la información.
  - b. Asegurar que se definan la política general, objetivos, políticas específicas de seguridad de información y que estos sean compatibles con la planeación estratégica de la Entidad.
  - c. Asegurar que los recursos necesarios para el mantenimiento del SGSI estén disponibles.
  - d. Revisar el Sistema de Gestión de Seguridad de la Información de la Entidad semestralmente, para asegurarse de su conveniencia, adecuación y eficacia continua. Esta revisión se realizará conforme a la información remitida por el Oficial de Seguridad de Información o quien haga sus veces.
  - e. Dirigir y apoyar a los Funcionarios y/o Contratistas para contribuir a la eficacia, mejora continua y logro de los resultados previstos dentro del SGSI.
  - f. Apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo dentro del SGSI aplicado a sus áreas de responsabilidad.
- 2. Comité Institucional de Gestión y Desempeño:** La conformación de este Comité se encuentra establecida en la Resolución 152 de 28 de febrero de 2018, quienes para el SGSI deberán cumplir con las siguientes responsabilidades:
  - 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





RESOLUCIÓN NÚMERO 200000705 DEL

10 OCT 2019

- 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.

**PARÁGRAFO SEGUNDO.** El Oficial de Seguridad de Información deberá hacer parte de este comité con voz y voto.

### 3. Oficial de Seguridad de Información:

- a. Liderar el mantenimiento del SGSI velando por el cumplimiento de las políticas de seguridad establecidas en la Entidad, los objetivos y planes del SGSI de forma que se encuentren alineados con los requerimientos de normas y leyes vigentes.
- b. Realizar actualizaciones de las metodologías y políticas de Seguridad de la Información.
- c. Socializar con funcionarios y contratistas de la Entidad los lineamientos del SGSI.
- d. Acompañar a los procesos en la actualización de activos de información, riesgos de seguridad digital y la definición de los planes de tratamiento.
- e. Realizar seguimiento a la ejecución de todos los planes que forman parte del SGSI.
- f. Definir métodos que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
- g. Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad de la Información.
- h. Asegurar la adecuada gestión de los incidentes de seguridad de la información en la USPEC.
- i. Definir las mediciones requeridas para verificar el desempeño del SGSI.
- j. Mantener actualizada la declaración de aplicabilidad definiendo la justificación de las inclusiones de los controles implementados o justificación de aquellos que se pueden considerar como exclusión en el SGSI. Esta actualización se llevará a cabo de forma anual, posterior a la actualización del mapa de riesgos de seguridad digital con el fin de incluir los controles implementados en el tratamiento de riesgos.
- k. Coordinar las actividades y reuniones del equipo operativo de seguridad de información.
- l. Informar semestralmente a la Alta Dirección sobre el desempeño del sistema de gestión de seguridad de información a través del informe de revisión por la Dirección.
- m. Revisar que el sistema se encuentre conforme con los requisitos de la Norma ISO 27001:2013 y el MSPI y mantener actualizada la herramienta de diagnóstico del MSPI.

**Nota:** En ausencia del Rol de Oficial de Seguridad de Información en la Entidad, el Jefe de la Oficina de Tecnología asumirá estas responsabilidades.

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

- a. Asignar los integrantes para la conformación del Equipo Operativo SGSI del(los) proceso(s) a cargo.
- b. Difundir las políticas, procedimientos y demás documentos relacionados con el SGSI en su respectivo proceso.
- c. Mantener actualizado el inventario de activos de información de su proceso de acuerdo a la metodología establecida por la entidad y velar por la ejecución de los controles requeridos para asegurar la confidencialidad, integridad y disponibilidad de los mismos.
- d. Liderar la gestión para llevar a cabo la actualización de riesgos de seguridad digital al interior de su proceso según la metodología establecida por la entidad.
- e. Definir el plan de tratamiento de riesgos de seguridad digital, aprobarlo y velar por su cumplimiento.
- f. Gestionar los recursos necesarios para la mitigación de riesgos de seguridad digital a través de la implementación de controles definidos en los planes de tratamiento de riesgos.
- g. Asegurar la disponibilidad de los Funcionarios y Contratistas de su proceso para la asistencia a actividades de formación y sensibilización que permitan el fortalecimiento de la cultura en Seguridad de la Información.
- h. Gestionar la definición y ejecución de planes de mejoramiento requeridos para apoyar la mejora continua del SGSI.
- i. Aprobar los planes, procedimientos y demás documentación necesaria para el mantenimiento del SGSI acorde a su proceso.
- j. Las demás responsabilidades asignadas en los procedimientos, instructivos, guías y demás documentación del SGSI.





000705  
RESOLUCIÓN NÚMERO DEL 10 OCT 2019

**5. Equipo Operativo de Seguridad de Información:**

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

- Apoyar la actualización del inventario de activos de su proceso teniendo en cuenta la metodología definida por la entidad.
- Apoyar la actualización de riesgos de seguridad digital y la formulación de su respectivo plan de tratamiento de riesgos.
- Apoyar a los responsables de la implementación del plan de tratamiento de riesgos de su proceso en la ejecución de controles según lo requerido.
- Realizar seguimiento al interior de su proceso al plan de tratamiento de riesgos definido para mitigar los riesgos de seguridad digital y los demás planes relacionados con el cumplimiento de lineamientos de seguridad de información.
- Participar en la actividades de formación y sensibilización organizadas por el Sistema de Gestión de Seguridad de Información.
- Apoyar la definición de los planes de mejoramiento requeridos para evidenciar la mejora continua del SGSI.
- Difundir al interior de su proceso las políticas, procedimientos y demás documentos que hacen parte del SGSI.

El Equipo Operativo de Seguridad de la Información se reunirá de acuerdo a las necesidades del Sistema de Gestión de Seguridad de Información y por solicitud del Responsable del SGSI.

**6. Funcionarios y Contratistas:**

- Apoyar el mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información, de acuerdo con las políticas, metodologías, procesos, procedimientos y los demás lineamientos establecidos para tal fin.
- Aceptar y dar cumplimiento a las políticas de seguridad de la información.
- Ejecutar los controles que al interior de su proceso y la Entidad se requieran para la adecuada protección de los activos que se encuentran bajo su gestión.
- Reportar eventos y/o incidentes de seguridad de la información de acuerdo al procedimiento establecido por la Entidad.
- Clasificar, etiquetar y manejar la información de acuerdo con los procedimientos y políticas establecidas por la Entidad.
- Participar activamente en las actividades de sensibilización, formación y toma de conciencia desarrolladas por la Entidad.

**ARTÍCULO 7. Actualización del alcance, política, objetivos, roles y responsabilidades de seguridad de la información.** La Política de Seguridad y Provacidad de la Información se revisará anualmente, o antes si se presentan situaciones que puedan llegar a afectar la seguridad de la información en la Entidad. Esta gestión está a cargo del Oficial de Seguridad de Información o quien haga sus veces y será aprobada por la el Director General de la USPEC.

**ARTÍCULO 8.** La presente Resolución rige a partir de la fecha de su expedición.

**ARTÍCULO 9.** Derogar la Resolución 001046 del 27 de Noviembre de 2018 "por la cual se adopta una nueva Política de Seguridad de Información" en lo referente a la Política General del Sistema de Gestión de Seguridad de la Información.

**PUBLÍQUESE Y CÚMPLASE**

Dada en Bogotá, D.C. a los

10 OCT 2019

**RICARDO VARELA DE LA ROSA**

Director General de la Unidad de Servicios Penitenciarios y Carcelarios

Elaboró: Mayra Alexandra Agudelo Carvajal / Profesional Especializado  
Revisó: Oscar Javier Suárez Ramos / Jefe Oficina de Tecnología  
Control de Legalidad: Julibeth De Leon Cueto / Jefe Oficina Asesora Jurídica  
Ruta: \\.....\sgsi\SGSI\_2019\Política\Política seguridad informacion.docx  
Ubicación archivo físico: Carpeta SGSI



**MINJUSTICIA**

Calle 97 A No. 9 A - 34 Bogotá, Colombia  
Teléfono: (57) (1) 4864130  
www.uspec.gov.co