Objetivo

Establecer los roles y responsabilidades dentro del Sistema de Gestión de la Seguridad de la Información

para el Instituto Nacional Penitenciario y Carcelario.

Glosario

- **Acción Correctiva**: acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir.
- **Acción Preventiva**: acción para eliminar la causa de una no conformidad potencial u otra situación potencialmente no deseable.
- **Alta dirección**: persona o grupo de personas que dirige y controla una organización al más alto nivel.
- **Confidencialidad**: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **COLCERT**: Grupo de Respuestas a Emergencias Cibernéticas de Colombia.
- **Corrección**: acción emprendida para eliminar una no conformidad.
- **CSIRT-PONAL**: Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional.
- **Criptografía**: técnica utilizada para salvaguardar los datos a través de la utilización de cifras o códigos para impedir que terceros no autorizados puedan acceder a información valiosa o alterarla para su propio beneficio o en perjuicio de otros.
- **Dato personal**: se refiere a cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados. Superintendencia de Industria y Comercio.
- **Disponibilidad**: propiedad de que la información se accesible y utilizable por solicitud de una entidad autorizada.

- **Eficiencia**: relación entre el resultado alcanzado y los recursos utilizados.

- **Eficacia**: grado en el cual se realizan las actividades planificadas y se logran los resultados planificados.

- **Evento de Seguridad de la Información**: de acuerdo a la ISO/IEC 27035:2012, presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación a la política de seguridad de la información o la falla de las salvaguardias, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **ERON**: sigla usada para denominar a los Establecimientos de Reclusión del Orden Nacional.

- **IEC** : International Electrotechnical Commission, es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.

- **Incidente de Seguridad de la Información**: de acuerdo a la ISO/IEC 27035:2012, evento o series de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información**: de acuerdo a la Unión Internacional de Telecomunicaciones es la inteligencia o conocimiento capaz de ser representado en formas adecuadas para comunicación, almacenamiento o procesamiento.

- **Integridad**: propiedad de salvaguardar la exactitud y estado completo de los activos.

- **ISO**: sigla de la expresión inglesa International Organization for Standardization, 'Organización Internacional de Estandarización', sistema de normalización internacional para productos de áreas diversas.

- **ISOlucion**: herramienta integral que facilita la planeación, implantación, automatización, administración y mantenimiento de la información asociada al Sistema de Gestión Integrado.

- **No conformidad**: incumplimiento de un requisito.

- **OFISI**: Oficina de Sistemas de Información.

- **Responsabilidad**: de acuerdo a la Guía No 4 Roles y Responsabilidades MINTIC es la cualidad de la persona responsable. "para cubrir ese puesto buscan a una persona con responsabilidad".

- **Rol**: de acuerdo a la Guía No 4 Roles y Responsabilidades MINTIC es el papel, función que alguien o algo desempeña.

- **Seguridad lógica**: conjunto de procesos destinados a garantizar la seguridad en el uso de los sistemas y los programas destinados a gestionar los datos y procesos en una organización.

- **Servidor público**: persona natural vinculada a la planta de personal de una organización y quien presta sus servicios según funciones asignadas. Para el caso del INPEC perteneciente al Personal Administrativo o al Cuerpo de Custodia y Vigilancia.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

Marco Legal

• Ver Normograma del Instituto Nacional Penitenciario y Carcelario

1. Organización de la Seguridad de la Información

La Ley 489 de 1998 tiene por objeto regular el ejercicio de la función administrativa, determinar la estructura y definir las reglas básicas de la organización y funcionamiento de la administración pública, por lo anterior y teniendo cuenta el capítulo **7.2 Recursos** de la Norma ISO/IEC 27001:2013 *"La organización deberá identificar y proporcionar todos los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información"*, por lo anterior los dueños de proceso junto con la Dirección General del INPEC deben establecer y organizar el equipo o comité de trabajo responsable de la implementación del Sistema de Gestión de Seguridad de la Información SGSI, teniendo en cuanta cada uno de los roles y responsabilidades que a continuación se describen.

El modelo a desarrollar para asignar los roles y responsabilidades será centralizado y distribuido de igual manera para que sea aplicado de modo homogéneo en cada una de las dependencias del Instituto.

1.1. Dirección General

La norma ISO/IEC 27001:2013 en su capítulo **5.1. Liderazgo y Compromiso** dice que la Alta Dirección tiene la obligación de demostrar su liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad, como también en su capítulo **9.3 Revisión por la Dirección** dice que debe revisar el SGSI a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacias continuas. Por lo anterior cumplirá las siguientes responsabilidades:

1. Asegurar que la política de seguridad de la información como los objetivos de seguridad sean establecidos.

2. Asegurar que los requisitos del Sistema de Gestión de Seguridad de la Información estén integrados en los procesos de la Entidad.

3. Garantizar la disponibilidad de los recursos necesarios para el Sistema de Gestión de Seguridad de la Información para lograr los resultados esperados.

4. Comunicar la importancia del Sistema de Gestión de la Seguridad de la información conforme a sus requisitos.

5. Asignar y comunicar las responsabilidades para llevar a cabo las tareas específicas de seguridad de la información designando a las personas adecuadas dentro de la Entidad.

6. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

7. Validar la implementación y operación del SGSI de su dependencia.

8. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

9. Apoyar al Responsable de seguridad de la información en la implementación del SGSI en la Entidad.

10. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

11. Asistir a las sensibilizaciones y capacitaciones del SGSI.

12. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.2. Responsable de Seguridad de la Información para la entidad

[1]En aquellas entidades que así lo justifiquen, por ejemplo, con insuficiencia de recursos técnicos o experticia, se recomienda la definición de un responsable de seguridad que responda simultáneamente para un conjunto de entidades que acuerden agruparse.

Y de acuerdo al capítulo **7.2 Competencia** de la ISO/IEC 27001:2013 requiere que una organización defina las competencias necesarias para la gestión de la seguridad de la información teniendo en cuenta el conocimiento, habilidades, experiencia y actitud frente a temas de Seguridad de la Información.

Como líder del Sistema de Gestión de Seguridad de la Información el responsable de seguridad de la información de la Entidad tiene las siguientes responsabilidades:

1. Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

2. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

3. Gestionar la definición y actualización, documentación y divulgación de políticas y procedimientos de seguridad de la información.

4. Orientar a líderes de procesos o dependencias de la entidad en el inventario, análisis y evaluación de riesgos de seguridad de la información sobre los activos de información de la entidad.

5. Orientar a los líderes de procesos o dependencias de la entidad en la definición e implantación de los controles de seguridad de la información.

6. Verificar y emitir recomendaciones en el cumplimiento normativo, políticas, controles y procedimientos de seguridad de la información a los líderes de procesos o

dependencias de la entidad.

7. Planear, ejecutar y orientar en los planes de sensibilización y concienciación en seguridad de la información al interior del Instituto con el apoyo de los líderes de procesos o dependencias.

8. Liderar la programación de reuniones de seguimiento de los avances del SGSI.

9. Reportar incidentes de seguridad de la información en coordinación con la OFISI a las autoridades pertinentes ante cualquier evento o incidente de seguridad de la información que afecte los activos de información de la Institución.

10. Identificar comunidades y grupos de interés relacionados con Seguridad de la Información que le permitan mantenerse actualizado y en contacto con expertos en los temas de seguridad.

11. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

12. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales

1.3. Oficina Asesora de Planeación

La documentación, creación y control de los registros de un Sistema de Gestión de Seguridad de la Información son aspectos relevantes en la norma ISO/IEC 27001:2013, Capitulo **7.5 Información documentada**; y teniendo en cuenta que la Resolución 02673 del 31 de mayo de 2016 adopta el software ISOlucion en el Instituto como herramienta integral que facilita, la planeación, implantación, automatización, administración y mantenimiento de la información asociada al Sistema de Gestión Integrado como fuente de información en el Instituto y que la Oficina Asesora de Planeación es el líder en la implementación y estandarización de la herramienta, tiene como responsabilidad:

1. Revisar los documentos del Sistema de Gestión Integrado generados en relación a la seguridad de la información antes de su emisión.
2. Revisar y requerir a los dueños de los procesos la actualización de los documentos asociados al Sistema de Gestión de Seguridad de la Información.
3. Mantener disponibles en la plataforma ISOlucion los documentos asociados a la seguridad de la información.
4. Mantener la distribución de los documentos del SGSI controlados y protegidos adecuadamente contra pérdida de confidencialidad o integridad.
5. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.
6. Validar la implementación y operación del SGSI de su dependencia.
7. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.
8. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.
9. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.
10. Asistir a las sensibilizaciones y capacitaciones del SGSI.
11. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.4. Oficina Asesora Jurídica

La Norma ISO/IEC 27001:2013 en su Anexo A dominio **A.18 Cumplimiento**, auxilia a las organizaciones en el cumplimiento de los requisitos legales o a los reglamentos contractuales

de seguridad de la información, los cuales, tienen la finalidad de eludir la vulneración de la legislación o el incumplimiento de toda obligación legal de las entidades de cualquier requisito de seguridad. Por lo anterior cumplirá las siguientes responsabilidades:

1. Asesorar al INPEC para que cumpla las normas legales y regulatorias locales en referencia a la Seguridad de la Información que afecten al Instituto.

2. Asesorar en la modificación de los contratos de trabajo de personal y de reglamento internos de trabajo para que incluyan responsabilidades de Seguridad de la Información.

3. Apoyar para que la Política de Seguridad de la Información, la Política de Tratamiento y Protección de Datos Personales del Instituto y demás políticas que se llegaren a crear junto con el Sistema de Gestión de Seguridad de la Información estén dentro del marco legal y regulatorio donde opere el INPEC, contando con el sustento legal que formalice y haga viable su aplicación.

4. Orientar y apoyar a la Oficina de Sistemas de Información y Oficina de Control Interno Disciplinario en la aplicabilidad de Ley 1273 del 2009 de delitos informáticos en Colombia dependiendo de la gravedad de violación a la Seguridad de la Información en el Instituto.

5. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

6. Validar la implementación y operación del SGSI de su dependencia.

7. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

8. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

9. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

10. Asistir a las sensibilizaciones y capacitaciones del SGSI.

11. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.5. Oficina Asesora de Comunicaciones

La Norma ISO/IEC 27001:20013 en la cláusula **7.4 Comunicación**, determina la necesidad de comunicaciones externas e internas en relación a la Seguridad de la Información. El INPEC debe comunicar claramente sobre la importancia de la Seguridad de la Información con mensajes objetivos y cortos en su forma y contenido para producir el comportamiento esperado por parte de los funcionarios, contratistas, judicantes y proveedores. Por lo anterior la Oficina Asesora de Comunicaciones cumplirá las siguientes responsabilidades:

1. Apoyar y asesorar al responsable de seguridad de la información de la Entidad en el diseño y edición de vídeos, fondos de pantallas, personaje, eslogan, folletos, afiches y todos aquellos artes visuales y auditivos en relación con la sensibilización en Seguridad de la Información.

2. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

3. Validar la implementación y operación del SGSI de su dependencia.

4. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

5. Apoyar al responsable de seguridad de la información en la implementación del SGSI en la Entidad.

6. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

7. Asistir a las sensibilizaciones y capacitaciones del SGSI.

8. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.6. Oficina de Sistemas de Información

De manera particular se resalta la participación activa de la Oficina de Sistemas de Información, durante y continuamente como parte fundamental en la implementación del Sistema de Gestión de Seguridad de la Información SGSI. Es responsable de la seguridad lógica del INPEC administrando herramientas tecnológicas que son gestionadas desde el Nivel Central, así mismo efectúa las tareas de desarrollo y mantenimiento de Sistemas de Información, siguiendo una metodología de ciclo de vida de la información, la cual debe contemplar medidas de seguridad. De esta forma tiene las siguientes responsabilidades siguiendo las recomendaciones de la **Guía**

No. 4 Roles y Responsabilidades de MINTIC y los requisitos de la Norma ISO/IEC 27001:2013 en su Anexo A y dominios **A.9 Control de acceso, A.10 Criptografía, A.12 Seguridad de las Operaciones, A.13 Seguridad en las comunicaciones, A.14 Adquisición, desarrollo y mantenimiento de sistemas y A.16 Gestión de Incidentes de seguridad de la información**:

1. Establecer los requerimientos mínimos de seguridad que deben cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la Entidad.

2. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado Colombiano.

3. Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución.

4. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

5. Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.

6. Trabajar con la Dirección General y los dueños de los procesos dentro de la entidad en el desarrollo de los planes de recuperación de desastres tecnológicos y los planes de continuidad del negocio

7. Mantener la confidencialidad, integridad y disponibilidad de la información y de los servicios de procesamiento de información a través de copias de respaldo de la información y del software debidamente ejecutadas y documentas.

8. Administrar las bases de datos alojadas en los centros de cómputo de la entidad, aplicando controles de seguridad de la información.

9. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad en los sistemas de información.

10. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.

11. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados.

12. Registrar, analizar y responder de manera controlada las solicitudes de cambios de las dependencias que realizan sobre los sistemas de información, asegurando su correcta aplicación según los acuerdos y prioridades, evitando interrupciones en la prestación de dichos servicios.

13. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

14. Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI.

15. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

16. Validar la implementación y operación del SGSI de su dependencia.

17. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

18. Apoyar al Responsable de seguridad de la información en la implementación del SGSI en la Entidad.

19. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia y coordinar el mismo con las dependencias del instituto, bajo los parámetros que fije el responsable de seguridad de la información.

20. Liderar y asistir a las sensibilizaciones y capacitaciones del SGSI.

21. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.7. Oficina de Control Interno

La Norma ISO/IEC 27001:2013 en su capítulo 9. **Evaluación del desempeño**, el Modelo de Seguridad y Privacidad de la Información y la Guía de Auditoria No. 15 de MINTIC, requieren la realización de auditarías internas a intervalos planificados para verificación de la implementación de un Sistema de Gestión de Seguridad de la Información para una mejora continua; por lo anterior la Oficina de Control Interno tiene bajo su responsabilidad:

1. Planificar, establecer, implantar y mantener uno o varios programas de auditaría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Los programas de auditoria deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditarías. Literal a) al literal g), clausula **9.2. Auditaría Interna** ISO/IEC 27001:2013.

2. Verificar la implantación y administración del Sistema de Gestión de Seguridad de la Información cumple con los requisitos de la norma.

3. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

4. Validar la implementación y operación del SGSI de su dependencia.

5. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

6. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

7. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

8. Asistir a las sensibilizaciones y capacitaciones del SGSI.

9. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.8. Oficina de Control Interno Disciplinario

Según la Norma ISO/IEC 27001:2013 en su Anexo A control **A.7.2.3 Proceso disciplinario**, dentro de los requisitos las organizaciones deben contar con un proceso disciplinario formal, comunicado para emprender acciones en contra de empleados que hayan cometido una violación a la seguridad de información. Teniendo en cuenta lo anterior la Oficina de Control Único Disciplinario tiene como responsabilidad:

1. Establecer el proceso disciplinario o incluir en el proceso disciplinario existente en la Entidad, el tratamiento de las faltas de cumplimiento a las políticas de seguridad, controles o los incidentes de seguridad que lo ameriten.

2. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

3. Validar la implementación y operación del SGSI de su dependencia.

4. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

5. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

6. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

7. Asistir a las sensibilizaciones y capacitaciones del SGSI.

8. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.9. Grupo de Policía Judicial

Teniendo en cuanta los lineamientos de la Guía No. 13 Evidencia Digital de MINTIC, cuando un evento es reportado y catalogado como un incidente de seguridad de la información, es necesario delimitar el ingreso a la zona donde se produjo el incidente para evitar cualquier tipo de alteración o contaminación a la evidencia que pueda recolectarse para la posterior investigación, dado que estos procedimientos deben ejecutarse a la mayor brevedad posible, debe proceder el personal del Grupo de Policía Judicial quienes están en capacidad de aislar la escena; con el apoyo de la OFISI y el Responsable de Seguridad de la Información; seguidamente comunicar a alguna autoridad competente en el tema como el CSIRT-PONAL o el COLCERT entre otros, ya que son Equipos de Respuestas ante Incidentes de Seguridad Informática, expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información y son puntos de apoyo para realizar investigaciones de este tipo.

Si el incidente de seguridad de la información se materializa en una Dirección Regional o ERON, el funcionario del servicio de Policía Judicial junto con el responsable del área de sistemas, realizan la actividad anterior y comunican a la OFISI para que a su vez este último informe del hecho a las autoridades competentes.

1. Restringir el acceso a la zona del incidente, para evitar algún tipo de alteración en la posible evidencia a recolectar.

2. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

3. Validar la implementación y operación del SGSI de su dependencia.

4. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

5. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

6. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

7. Asistir a las sensibilizaciones y capacitaciones del SGSI.

8. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.10. Dirección Escuela de Formación

La sensibilización o concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI, por ello la Norma ISO/IEC 27001:2013 en su cláusula **7.3 Toma de conciencia** todo el personal del Instituto debe conocer y aplicar políticas y controles de seguridad de la información ya que como usuarios finales son los que gestionan, procesan, almacenan y transfieren información utilizando medios físicos, digitales (sistemas de información) y verbales. Cumplirá las siguientes responsabilidades:

La Dirección Escuela de Formación facilita los mecanismos necesarios para la sensibilización y/o concienciación en seguridad de la información en el Instituto.

1. Definir, desarrollar e implementar cursos de sensibilización y/o concienciación de la cultura de seguridad de la información, para los funcionarios y contratistas con apoyo de la Oficina de Sistemas de Información y el responsable de la seguridad de la información.

2. Verificar la efectividad de la sensibilización y/o concienciación de la cultura de seguridad de la información reportando los resultados a la Oficina de Sistemas de Información y al responsable de seguridad de la información, sugiriendo acciones correctivas cuando hubiere lugar.

3. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

4. Validar la implementación y operación del SGSI de su dependencia.

5. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

6. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

7. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

8. Asistir a las sensibilizaciones y capacitaciones del SGSI.

9. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.11. Grupo de Gestión Documental

Clasificar la información según el Anexo A en el dominio **A.8 Gestión de Activos**, objetivo de control **A.8.2 Clasificación de la información** de la Norma ISO/IEC 27001:2013 es una de las partes de mayor relevancia y de los primeros aspectos a gestionar en el ámbito de la seguridad de la información y teniendo en cuenta la Guía No. 6 de Referencia sobre Gestión Documental de MINTIC, cuyo objetivo es presentar una relación de la Normatividad Técnica Colombiana – NTC de consulta, de acuerdo con los lineamientos establecidos por el Archivo General de la Nación, el Grupo de Gestión Documental tiene la responsabilidad de:

1. Proteger la integridad, disponibilidad y clasificación de los documentos generados y/o remitidos físicos como electrónicos en el Instituto para garantizar resultados óptimos en el almacenamiento y manejo confidencial de la información.

2. Definir las directrices del inventario, clasificación y etiquetado de la información, como de las medidas de tratamiento o de manejo que deben darse a la información en función del nivel de clasificación al que pertenecen. Para el manejo y almacenamiento de la información acorde a la clasificación establecida anteriormente, es necesario tener en cuenta lo siguiente:

    - Restringir el acceso solo al personal debidamente autorizado.

    - Mantener un registro formal de los receptores autorizados de datos o información.

    - Conservar los medios de almacenamiento en un ambiente seguro.

3. Asegurar que la política de gestión de documentos y archivos de la institución ha identificado los riesgos en relación a la gestión de documentos y las estrategias o medios para tratarlos o mitigarlos.

4. Establecer controles de seguridad para la transferencia de información documental física.

5. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

6. Validar la implementación y operación del SGSI de su dependencia.

7. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

8. Apoyar al Responsable de seguridad de la información en la implementación del SGSI en la Entidad.

9. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

10. Asistir a las sensibilizaciones y capacitaciones del SGSI.

11. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.12. Grupo Logístico

Mantiene la seguridad de la información de la Entidad protegida de accesos inadecuados y otras amenazas a las que se pueda enfrentar. Responsable de la seguridad física de la sede central, regionales y dependencias administrativas. Anexo A, dominio **11. Seguridad Física y del Entorno** de la Norma ISO/IEC 27001:2013. La función fundamental de la seguridad física es la de servir de protección a los activos de información frente a las amenazas físicas como el acceso no autorizado, los perjuicios provocados por la acción humana, o las inclemencias meteorológicas. Cumplirá las siguientes responsabilidades:

1. Mantener y controlar un programa de seguridad física que incluya la protección de áreas seguras contra amenazas externas con controles de acceso e implantar medidas contra

   inundaciones e incendios. La protección tiene que ser proporcional a los riesgos identificados.

2. Clasificar, junto con Responsable de la Seguridad de la Información y la Oficina de Sistemas de Información, las áreas de procesamiento de la información de acuerdo con la criticidad de la información.

3. Garantizar el acceso restringido de terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible.

4. Exigir a todo el personal de la Entidad el porte del carné Institucional de forma visible.

5. Solicitar a las personas ajenas a la Institución que no lleven consigo la identificación o sticker visible generado en la recepción ni acompañadas por un funcionario de la Entidad, el propósito de su visita e identificación.

6. Controlar la protección de los directorios telefónicos internos por parte del público externo a la Institución.

7. Vigilar que las áreas seguras estén cerradas, el trabajo y las actividades realizadas en ellas solo estará en conocimiento del personal autorizado.

8. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

9. Validar la implementación y operación del SGSI de su dependencia.

10. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

11. Apoyar al Responsable de seguridad de la información en la implementación del SGSI en la Entidad.

12. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

13. Asistir a las sensibilizaciones y capacitaciones del SGSI.

14. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.13. Subdirección de Talento Humano

La Norma ISO/IEC 27001:2013 en su Anexo A, dominio **A.7 Seguridad de los recursos humanos** hace referencia a la seguridad ligada a los recursos humanos como el componente más crítico al momento de garantizar las tres propiedades de la seguridad de la información: integridad, confidencialidad y disponibilidad, por lo tanto es responsabilidad de la Subdirección de Talento Humano gestionar prácticas que ayuden a mitigar el impacto de los riesgos que por este factor se pudieran materializar antes del empleo, durante el empleo y tras finalizar el empleo por lo anterior cumplirá las siguientes responsabilidades:

1. Verificar antecedentes de los candidatos a un empleo de acuerdo con leyes y normas establecidas por la entidad y el gobierno.

2. Establecer los términos y condiciones de empleo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la Entidad.

3. Definir, desarrollar e implementar en la inducción y reinducción sensibilización y/o concienciación en cultura de seguridad de la información, para los servidores públicos.

4. Informar al personal desde su ingreso y de forma continua, cualquiera que sea la situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y asuntos de confidencialidad en el Instituto.

5. Aplicar la protección y tratamiento de datos personales consignados en las hojas de vida de los funcionarios administrativos y de cuerpo y custodia de acuerdo a la Ley 1581 de 2012.

6. Desarrollar procedimientos para garantizar que los retiros definitivos o temporales de funcionarios y contratistas sea debidamente controlados garantizando la devolución de todo el equipamiento e informado a la Oficina de Sistemas de Información la eliminación de las credenciales de acceso a los sistemas de información.

7. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

8. Validar la implementación y operación del SGSI de su dependencia.

9. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad de la información en su dependencia.

10. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

11. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

12. Asistir a las sensibilizaciones y capacitaciones del SGSI.

13. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

1.14. Demás dependencias de la sede central, Direcciones Regionales y Establecimientos de Reclusión

Las demás dependencias de la Institución, son responsables de ejecutar, aplicar y cumplir el Sistema de Gestión de Seguridad de la Información así:

1. Cumplir con las disposiciones de la Política de Seguridad de la Información, Guía de Normas y Buenas Prácticas de Seguridad de la Información y todos aquellos documentos asociados al Sistema de Gestión de Seguridad de la Información.

2. Acatar y gestionar los procedimientos o guías de inventario y clasificación de activos de información de su dependencia.

3. Acatar y gestionar la Metodología de Gestión y Evaluación del riesgo de Seguridad de la Información de su dependencia y los requisitos reglamentarios.

4. Validar la implementación y operación del SGSI de su dependencia.

5. Ejecutar las acciones de mejora derivadas de los procedimientos de seguimiento y revisión del SGSI en su dependencia.

6. Realizar la medición de la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad en su dependencia.

7. Ejecutar las recomendaciones derivadas de las auditarías internas del SGSI realizadas

8. Plantear acciones preventivas o correctivas, comunicar al Responsable de Seguridad de la Información sobre su efectividad y ejecutar las recomendaciones correspondientes.

9. Apoyar al Responsable de Seguridad de la Información en la implementación del SGSI.

10. Realizar el inventario de activos de información y gestión de riesgos de seguridad de la información de su dependencia, en coordinación con la OFISI y bajo los parámetros que fije el responsable de seguridad de la información.

11. Asistir a las sensibilizaciones y capacitaciones del SGSI.

12. Aplicar los principios de confidencialidad, integridad y disponibilidad de la información que procesen, almacenen o transmitan dentro y fuera de la entidad como también dentro del entorno personal y de las redes sociales.

---

[1] Guía No. 4 Roles y Responsabilidades. Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y Comunicaciones MINTIC.

Anexos

- Guía No. 4 Roles y Responsabilidades. Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y Comunicaciones MINTIC
- Guia No. 6 Guía de Referencia sobre Gestión Documental. Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y Comunicaciones MINTIC.
- Guía No. 13 Evidencia Digital. Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y Comunicaciones MINTIC.

- Guía No. 15 - Auditoria. Seguridad y Privacidad de la Información. Ministerio de Tecnologías de
la Información y Comunicaciones
MINTIC.

Lista de Versiones			
Versión	**Fecha de Emisión**	**Motivo de la Modificación**	**Modificaciones**
1	18/Nov/2019	creación del documento	N/A

Elaboró	Revisó	Aprobó
Nombre: María Cristina Reyes Castillo **Cargo:** Técnico Operativo **Fecha:** 26/Nov/2019	**Nombre:** Eduardo Iván Guzmán Guzmán **Cargo:** Distinguido **Fecha:** 22/Nov/2019 **Nombre:** Juan Manuel Riaño Vargas **Cargo:** Jefe Oficina Asesora de Planeación **Fecha:** 22/Nov/2019	**Nombre:** Adriana Cetina Hernández **Cargo:** Jefe Oficina Sistemas de Información **Fecha:** 26/Nov/2019