# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Proceso:** Gestión de TICS

2022

| Versión | Fecha Versión | Observación |
|---|---|---|
| **1** | **2021-01-20** | **Versión año 2021** |
| **2** | **2022- 01- 207** | **Actualización 2022** |

Tabla 1. Control de cambios

# TABLA DE CONTENIDO

# 1. OBJETIVO

Este plan tiene como objetivo implementar y proteger los activos de información de El Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas - IPSE, con base en los criterios de confidencialidad, integridad y disponibilidad.

- Administrar los riesgos de seguridad de la información para mantenerlos en

niveles aceptables.

- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital".

# 2. ALCANCE DEL PLAN

La implementación, gestión y operación del Sistema de Gestión de Seguridad de la Información – SGSI y la creación de las políticas de seguridad bajo el lineamiento del documento CONPES 3995, se realiza en todos los procesos de El Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas - IPSE, de acuerdo con el ciclo de mejora continua PHVA; esto incluye, las actividades de formalización de los procesos, procedimientos y documentación correspondiente al SGSI a través de su integración con el Sistema de Gestión Integrado – SGI

De ahí la importancia que, el IPSE, considera establecer un marco, en el cual, se asegure que la preservación de la confidencialidad, integridad y disponibilidad de la información que maneja, como producto del desarrollo su actividad, es protegida de manera adecuada, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración.

El presente documento contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por MINTIC, el cual orienta a las entidades a la preservación de la confidencialidad, integridad, disponibilidad de la información y permite fijar los criterios para proteger la privacidad de la información, los datos, así como de los procesos y las personas vinculadas con dicha información.

Para la elaboración de este documento, se toma como referencia además de los lineamientos de MINTIC en el MSPI y sus correspondientes guías de apoyo, la norma ISO 27001:2013, CONPES 3995 y el anexo A.

Las políticas de seguridad de la información incluidas en este documento constituyen una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y se convierten en la base para la implementación de los controles, procedimientos definidos por las normas anteriormente mencionadas.

Es responsabilidad de todas las partes interesadas del IPSE velar por que no se realicen actividades que contradigan la esencia de este documento con el fin de preservar la confidencialidad, integridad y disponibilidad de la información que aquí se maneja.

# 3. RESUMEN EJECUTIVO

La implementación de las adecuadas medidas de protección de la información estratégica de negocio y la preservación de la confidencialidad son requisitos esenciales para garantizar la confianza de las partes interesadas, factor indispensable para lograr los objetivos institucionales administrando y protegiendo la información del sector energético en el país.

La adopción de un sistema de gestión de seguridad de la información basado en el cumplimiento del Modelo de Seguridad y Privacidad de la Información, la norma ISO 27001:2013 y la guía de gestión de riesgos del DAFP, es una decisión de carácter estratégico que permite no solo el cumplimiento de los requisitos de ley sino la optimización de los recursos humanos, tecnológicos y administrativos necesarios para reducir los riesgos que afectan la información física generada o administrada por el Instituto y la presente en el entorno tecnológico actual.

El presente documento se elabora dando cumplimiento al Decreto 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, entre los que menciona el plan de tratamiento de riesgos de seguridad de la información.

Considerando la importancia de cumplir los requisitos normativos en materia de protección de información y mitigar los impactos de sanciones derivadas de su incumplimiento, se incluye una serie de actividades que responden al ciclo Planear-Hacer-Verificar-Actuar (PHVA) para el sistema de gestión de seguridad de la información en miras a la certificación en la norma internacional ISO 27001:2013 y dando cumplimiento con lo establecido por MINTIC.


El plan de seguridad y privacidad de la información contempla todos los requisitos necesarios para garantizar a la entidad el fortalecimiento de su gestión institucional mediante la mejora de la confianza de todas las partes interesadas en la adecuada protección de la información.

# 4. DEFINICIONES

**Aceptación de riesgo**: Decisión de asumir un riesgo.

**Activo**: Cualquier cosa que tiene valor para la organización.

**Adaptabilidad**: Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.

**Amenazas**: [1]Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

**Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable.

**Auditoria**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría.

**Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

**Capacity Planning**: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

**Centros de cableado**: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir

[1] ISO/IEC 27000

requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

**Centro de cómputo**: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

**Criptografía**: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

**Cifrado**: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información. Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

**Ciberseguridad**[2]: Capacidad del Estado para minimizar el nivel de riesgo aceptable al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

**Comité de Seguridad de la Información**: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

**Confiabilidad de la Información**: Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

**Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptado. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Custodio del activo de información**: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

**Dato personal**: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

**Dato público**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre

[2] CONPES 3701

otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

**Datos sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

**Declaración de aplicabilidad**: [3]Listado que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la entidad, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

**Declaración de aplicabilidad**: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.

**Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.

**Evaluación del riesgo**: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

**Evento de seguridad de la información**: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

**Gestión de incidentes de seguridad de la Información**: [4]Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

**Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

**Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

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

**Guía DAFP**: Guía para la administración y gestión del riesgo del Departamento Administrativo de la Función Pública.

**MSPI**: Modelo de Seguridad y Privacidad de la información, comprende las acciones transversales a los demás procesos, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

[3] ISO/IEC 27000

[4] ISO/IEC 27000

**Plan de continuidad del negocio**: [5]Plan orientado a permitir la continuación de las principales funciones misionales o críticas del negocio en el caso de un evento imprevisto que las ponga en peligro.

**Plan de tratamiento de riesgos**: [6]Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

**Partes interesadas**: Persona u organización que puede afectar, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. Para la entidad son: los servidores públicos, contratistas, proveedores, ciudadanos y agencias relacionadas con el IPSE.

**Política**: Es el marco referencial o lineamiento general emitido por la Alta Dirección, que orienta para las actuaciones, conductas o funciones de los colaboradores y dependencias.

Procedimiento: Es la forma especificada para llevar a cabo una actividad o un proceso.

**Proceso**: Es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas en resultados.

**Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

**Recursos informáticos**: Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.

**Seguridad de la Información**[7]: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

**Sistema de Gestión de Seguridad de la Información SGSI**[8]: 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.

**SIG**: Sistema Integrado de Gestión

**Tecnología de la Información**: Se refiere al hardware y software operado por la organización o por un tercero que procese información en su nombre, para llevar a cabo una función propia del IPSE

**Trazabilidad**[9]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

**Tratamiento del riesgo**: Proceso de selección e implementación de acciones de mejorar que permita gestionar el riesgo.

---

[5] ISO/IEC 27000
6 ISO/IEC 27000
7 ISO/IEC 27000
8 ISO/IEC 27000
9 ISO/IEC 27000

**Valoración del riesgo**: Proceso de análisis y evaluación del riesgo.

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.[10]

# 5 ACTIVIDADES DEL PLAN PARA DESARROLLAR

En un mundo interconectado, la información y los procesos relacionados, los sistemas, las redes y el personal involucrado en su operación, el manejo y la protección de los activos que, como cualquier otro activo importante del instituto, son valiosos para la entidad, y en consecuencia ameritan o requieren protección contra diversos peligros.

Por lo que la implementación del sistema de gestión de seguridad de la información permite definir e identificar los mecanismos necesarios para proteger la información de la entidad, definir las responsabilidades internas y a través de una constante evaluación que permita realizar mejora, generar confianza en el trabajo realizado de cara al ciudadano y a los requerimientos legales o de entes de control.

## 5.1 AJUSTES E IMPLEMENTACIÓN A LA DOCUMENTACIÓN DE LOS PROCEDIMIENTOS

Dentro del trabajo de integración del Sistema de Gestión de Seguridad de la Información con los procesos del IPSE, se presentan a continuación los temas a documentar o actualizar, de acuerdo con las respectivas responsabilidades de cada proceso y área existente en el instituto.

Se realizará la revisión documental teniendo en cuenta los requerimientos de la norma ISO 27001: 2013 para las siguientes áreas:

**Secretaria y/o Dirección**

- Impulsar y garantiza la implementación del SGSI de acuerdo con lo estipulado en el Anexo A.7.2.1.
- Formar Auditores Internos en NTC ISO 27001:2013

**Gestión de Tecnologías de la Información y las comunicaciones**

- Auditorías de los Sistemas de Información, Sistemas Operativos. de acuerdo con lo estipulado en el Anexo A.12.7.
- Procesos de Desarrollo y Soporte Seguro de acuerdo con lo estipulado en el dominio A.14.
- Separación de los ambientes de desarrollo, pruebas y operación de acuerdo con lo estipulado en el Anexo A.12.1.4.
- Control de Software Operacional de acuerdo con lo estipulado en el Anexo A.12.5.1.
- Gestión de la vulnerabilidad técnica de acuerdo con lo estipulado en el Anexo A.12.6.
- Adquisición, desarrollo y mantenimiento de sistemas de acuerdo con lo estipulado en el Dominio A.14.

[10] ISO/IEC 27000

- Gestión de Capacidad de acuerdo con lo estipulado en el Anexo A.12.1.3.
- Configuraciones seguras para dispositivos móviles de acuerdo con lo estipulado en el Anexo A.6.2.1.
- Accesos seguros a la información en teletrabajo de acuerdo con lo estipulado en el Anexo A.6.2.2.
- Gestión de Medios Removibles de acuerdo con lo estipulado en el Anexo A.8.3.1
- Control de acceso, apoyados por los responsables o coordinadores de cada área, contractual y talento humano de acuerdo con lo estipulado en el Dominio A.9.
- Criptografía, apoyados por los responsables o coordinadores de cada área, de acuerdo con lo estipulado en el Dominio A.10.
- Seguridad en equipos de cómputo de acuerdo con lo estipulado en el Anexo A.11.2.
- Gestión de Capacidad de acuerdo con lo estipulado en el Anexo A.12.1.3.
- Protección contra código malicioso de acuerdo con lo estipulado en el Anexo A.12.2.
- Copias de respaldo, apoyados por los responsables o coordinadores de cada área, de acuerdo con lo estipulado en el Anexo A.12.3.
- Registro y Seguimiento de actividades por usuario logs de acuerdo con lo estipulado en el Anexo A.12.4.
- Seguridad de las comunicaciones de acuerdo con lo estipulado en el Anexo A.13.

**Coordinación Gestión de Talento Humano**

- Protección de la Información en teletrabajo de acuerdo con lo estipulado en el Anexo A.6.2.2.
- Seguridad en recursos humanos de acuerdo con lo estipulado en el Dominio A.7.

**Planeación**

- Seguridad de la Información en la planeación de proyectos de acuerdo con lo estipulado en el Anexo A. 6.1.5.
- Proceso de Gestión de Cambios de acuerdo con lo estipulado en el Anexo A.12.1.2.
- Implementación de la seguridad en continuidad del negocio de acuerdo con lo estipulado en el Anexo A.17.1.2.
- Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio de acuerdo con lo estipulado en el Anexo A.17.
- Apoyo en el inventario de Activos de Información de acuerdo con lo estipulado en el Anexo A.8.

**Grupo Contractual**

- Seguridad en recursos humanos esto incluye contratistas, de acuerdo con lo estipulado en el Dominio A.7.
- Acuerdos de confidencialidad al contratista de acuerdo con lo estipulado en el Anexo A.13.2.4.
- Acuerdos sobre transferencia de información de acuerdo con lo estipulado en el Anexo A.13.2.2.
- Relaciones con los Proveedores de acuerdo con lo estipulado en el Anexo A.15.

**Gestión Administrativa**

- Entrega y devolución de Activos de Información de acuerdo con lo estipulado en el Anexo A.8.1.4.
- Áreas Seguras de acuerdo con lo estipulado en el Anexo A.11.1.
- Relaciones con los Proveedores de acuerdo con lo estipulado en el Dominio A.15.

- Adquisición, desarrollo y mantenimiento de sistemas de acuerdo con lo estipulado en el Dominio A.14.
- Gestión de Capacidad de acuerdo con lo estipulado en el Anexo A.12.1.3.

**Gestión Documental**

- Etiquetado de la Información de acuerdo con lo estipulado en el Anexo A.8.2.2.
- Transferencia de medios físicos de acuerdo con lo estipulado en el Anexo A.8.3.3.
- Apoyo en el inventario de Activos de Información de acuerdo con lo estipulado en el Anexo A.8.

**Jurídica**

- Acuerdos de confidencialidad al contratista de acuerdo con lo estipulado en el Anexo A.13.2.4.
- Acuerdos sobre transferencia de información de acuerdo con lo estipulado en el Anexo A.13.2.2.
- Cumplimiento de acuerdo con lo estipulado en el Anexo A.18.

**Control Interno**

- Revisión Independiente de la seguridad de la Información (Contratar un externo para auditorías internas) de acuerdo con lo estipulado en el Anexo A.18.2.1.
- Formar Auditores Internos en NTC ISO 27001:2013

**Control Interno Disciplinario**

- Proceso disciplinario si se incumple algún lineamiento o Política de Seguridad de la Información de acuerdo con lo estipulado en el Anexo A.7.2.3.

**Procesos y áreas misionales**

- Cumplimiento de las políticas y directrices de protección de la información de acuerdo con lo estipulado en el Dominio A.5
- Informar a Talento Humano sobre terminación o cambios de responsabilidades de los funcionarios de acuerdo con lo estipulado en el Anexo A.7.3.1
- Identificación clasificación y valoración de activos de información de acuerdo con lo estipulado en el Dominio A.8
- Control de acceso, apoyando a soporte tecnológico, talento humano y contractual de acuerdo con lo estipulado en el Dominio A.9.
- Copias de respaldo, apoyando a soporte tecnológico, de acuerdo con lo estipulado en el Anexo A.12.3.
- Reportar eventos o incidentes de seguridad de la información, de acuerdo con lo estipulado en el Anexo A.16.1.2.
- Identificar la información que contiene datos personales, de acuerdo con lo estipulado en el Anexo A.18.1.4.

## 5.2REVISIÓN TÉCNICA INDEPENDIENTE

Contratar un experto para poder realizar un ejercicio de hacking ético, análisis de vulnerabilidades, diseño de red segura e ingeniería social que permita identificar oportunidades de mejora en:

- Puertos, servicios y direcciones IP relacionadas con la infraestructura que soporta los servicios tecnológicos expuestos en el ciberespacio del IPSE.

- Vulnerabilidades a nivel de red y sistema operativo de los servidores publicados en internet de propiedad del IPSE.

- Vulnerabilidades web sobre las aplicaciones importantes de propiedad de IPSE.

- Vulnerabilidades de red y sistema operativo para el 10% de las direcciones IP internas que incluye servidores, dispositivos de red y una muestra de equipos de escritorio (Máquinas Virtuales VDI) y portátiles.

- La topología actual de la red interna de IPSE y rediseño de la misma, enfocado en la alineación con las mejores prácticas internacionales en arquitectura de red segura.

- Verificación de cultura de la seguridad en los usuarios realizando una prueba de ingeniería social para al menos el 10% de los usuarios del IPSE, que se escogerá de un conjunto de opciones posibles de acuerdo la prueba más conveniente para la organización.

## 5.3 REVISIÓN INDEPENDIENTE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de evitar el incumplimiento de las obligaciones frente al MINTIC, DAFP, y de acuerdo con las evaluaciones del FURAG, MIPG, así como las obligaciones legales o de reglamentación relacionadas con seguridad de la información, se realizará una auditoría interna.

# 6 CONDICIONES GENERALES PARA LA EJECUCIÓN DEL PRESENTE PLAN

## 6.1 MEDIOS Y HERRAMIENTAS PROFESIONALES

Para llevar a cabo el siguiente plan para monitoreo y ejecución de las diferentes tareas se pondrán a disposición de las siguientes herramientas

- Actualización de licenciamiento de firewall tales como son filtrado web, prevención de intrusos, antivirus, filtrado de correos
- Fortianalyzer el cual tiene como objetivo interconectar diferentes tipos de soluciones, para tener una visión completa de la red y así automatizar la respuesta a incidentes
- GLPI Plataforma de mesa de ayuda con la cual administra los servicios solicitados, incidentes, problemas y cambios en la infraestructura con el estándar y las mejores practicas
- VPN para la conexión remota de forma segura al acceso de la infraestructura del IPSE

Se utilizarán las herramientas profesionales requeridas para llevar a cabo las asignaciones, como por ejemplo computadora y programas de software (software de Office 365, cliente de correo electrónico, navegador web) teléfono celular y elementos de oficina.

**FIN DEL DOCUMENTO**