# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**Proceso:** Gestión de TICS

2024

## CONTENIDO



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

# 1. GENERALIDADES DEL PLAN INSTITUCIONAL

## 1.1. Introducción

En consecuencia a lo establecido en el decreto 1008 del 14 de junio de 2018; por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas - IPSE, procede a definir normativas y buenas prácticas para el tratamiento de la información dentro de la entidad.

Mediante este plan se indicarán las medidas que se implementará que pretende garantizar la seguridad y privacidad de la información que maneja la institución.

## 1.2. Alcance

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.



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

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.

## 1.3. Objetivos

### 1.3.1. Objetivo general

Implementar un marco normativo de buenas prácticas en el buen uso de la información dando cumplimiento a lo planteado en el decreto 1008 del 14 de junio de 2018 (Gobierno Digital)

## 1.4. Objetivos específicos

1. Diagnosticar la situación actual del Sistema de Gestión de Seguridad y Privacidad de la Información al interior de la entidad (Herramienta de autodiagnóstico MSPI), así como detectar posibles riesgos.
2. Establecer alcance, roles, responsabilidades, políticas, procedimientos y demás elementos que permitan construir un marco normativo al interior de la institución.
3. Determinar el estado de los activos de información, identificación, valoración y tratamiento de riesgos dentro de la Entidad.
4. Diseñar e implementar controles para mitigar, minimizar o transferir los riesgos de Seguridad y Protección de la información en cada una de las áreas.
5. Evaluar el desempeño de las herramientas, políticas y controles implementados en el Sistema de Gestión de Seguridad y Privacidad de la Información.

# 2. CONTEXTO ESTRATÉGICO

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.



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

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.


*Ilustración 1: Flujo de un Sistema de Gestión*

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.

## 3. MARCO CONCEPTUAL

**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.



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

**Amenazas:** 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.

**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 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.

**Ciberseguridad**: Es la práctica de proteger los sistemas de información y activos digitales

**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:** Garantiza que la fuente de la información generada sea adecuada para



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

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 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.

**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.

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



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

**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.

**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.

**Plan de continuidad del negocio:** 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:** 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



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

(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.

**Riesgo:** Efecto de la incertidumbre, es una posibilidad de desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.

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

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

**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.

El anterior marco conceptual se construyó tomando en cuenta las definiciones suministradas en la ISO/IEC 27000 (Seguridad de la Información) y del CONPES 3701 (Lineamientos de Política para Ciberseguridad y Ciberdefensa)



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

## 4. MARCO NORMATIVO

- **En materia de Seguridad Informática:**

ISO 27001:2013, Política de Seguridad Digital – MIPG, Modelo de Seguridad MSPI – MINTIC, CONPES 3701 - Lineamientos de Política para Ciberseguridad y Ciberdefensa.

## 5. DESCRIPCIÓN DEL PLAN

Un plan de privacidad y seguridad de la información es un conjunto de medidas y procedimientos diseñados para proteger la privacidad y seguridad de la información confidencial de una organización. El plan debe incluir medidas para prevenir, detectar y responder a incidentes de privacidad y seguridad de la información, así como cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

Para la gestión de este plan se tienen en cuenta actividades que impacten en los siguientes aspectos del MSPI:

- **Identificación y evaluación de riesgos:** Un análisis de los riesgos potenciales para la privacidad y seguridad de la información, incluyendo los riesgos internos y externos.
- **Políticas y procedimientos**: Un conjunto de políticas y procedimientos para garantizar que la información se maneja de manera segura y cumpliendo con las regulaciones aplicables
- **Medidas de seguridad física y digital:** Medidas de seguridad para proteger la información física y digital, tales como protección de la infraestructura, firewalls, encriptación, autenticación de usuarios, etc.
- **Educación y concientización:** Capacitaciones a los empleados sobre la privacidad y seguridad de la información, incluyendo temas como el manejo seguro de contraseñas, el uso seguro de dispositivos móviles, y cómo identificar y responder a incidentes de seguridad.
- **Monitoreo y auditorías:** Monitoreo y auditorías regulares para detectar y responder a incidentes de privacidad y seguridad de la información.
- **Plan de respuesta a incidentes:** Un plan detallado para responder a incidentes de privacidad y seguridad de la información, incluyendo un plan de comunicación con los interesados afectados.

## 6. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN

Para el seguimiento y evaluación de este Plan, se deberá entregar trimestralmente



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia

informes con evidencias en las fechas programadas por la Oficina de Planeación.



**Sede Principal:** Calle 99 No. 9 A - 54 Torre 3. Piso 14
PBX: (60 1) 639 7888
**IPSE Centro Nacional de Monitoreo**: (60 1) 6101130
ipse@ipse.gov.co
Bogotá D.C. – Colombia