2024

Plan de Seguridad y Privacidad de la Información

VERSIÓN VERIFICADA
FECHA: 29/12/2023

Listado de Versiones

Tabla 1

Listado de Versiones

VER.	FECHA	RAZÓN DE LA ACTUALIZACIÓN
01	15/12/2021	Versión inicial.
02	13/01/2023	Actualización vigencia del Plan-Versión 2.
03	29/12/2023	Actualización vigencia del Plan-Versión 3.

Fuente: MINENERGÍA

Aprobaciones

Tabla 2

Aprobación

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Óscar Sánchez S.	Juan J. Cedeño L.			
Cargo:	Profesional Especializado-Grupo TICS	Cargo:	Coordinador Grupo TICS	Cargo:	
Dependencia:	Grupo TICS	Dependencia:	Grupo TICS	Dependencia	OPGI
Fecha:	29/12/2023	Fecha:	29/12/2023	Fecha:	

Fuente: *MINENERGÍA*

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

1. Introducción

La capacidad de acceder a la información a través de Internet desde múltiples dispositivos electrónicos, el incremento de los servicios digitales y el auge creciente de las nuevas tecnologías, son aspectos que le han dado un impulso a la digitalización de las empresas en los últimos años. No obstante, la incursión de la pandemia COVID-19 catapultó la proliferación de los servicios de información digitales, y son muchas las empresas que dieron ese paso. En Colombia, el sector público se vió obligado a brindar prácticamente todos los trámites y servicios a través de medios digitales y tratamientos remotos de la información.

Dado lo anterior, hoy se observan tendencias incrementales en cuanto a información compartida a través de medios digitales, recuperación de datos remotos, uso de ambientes colaborativos y de dispositivos electrónicos. Razón por la cual es necesario proveer entornos seguros orientados a estas nuevas modalidades de interacción entre la Ebtidad y sus colaboradores.

Así como se incrementa el consumo y disponibilidad de datos, de las misma manera se incrementa el valor de esta información y el riesgo de ser sujetos a ciber ataques, por la explotación de nuevas vulnerabilidades, en la infraestructura y sistemas de información de las organizaciones corporativas. En ese sentido, el año 2023, no fue ajeno a esta realidad. demostrando ser una prueba de rigor, donde muchas más medidas se tomaron, en procura de atender de una mejor forma, las recomendaciones hechas desde el Gobierno (Presidencia-MINTIC), los organismos internacionales y las nuevas versiones de las normas y estándares internacionales. Muy a pesar de ello, se evidenció una gran vulnerabilidad en uno de los proveedores multinacionales de servicios en la nube, afectando un número importante de entidades gubernamentales.

El Plan de Seguridad y Privacidad de la Información, es el resultado de analizar, realizar e implementar las lecciones aprendidas, con el objeto de poder darle cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), conforme van evolucionando las TICS. Esta adapatación y actualización ha permitido una mejora sustancial y continua a las políticas, procedimientos, protocolos, instructivos y guías, que, le han permitido al Ministerio, estar acorde en el cumplimiento de los requerimientos del Modelo de Seguridad y Privacidad de la información (MSPI).

Continuando con este propósito, como se observó en la vigencia 2023, el Grupo de Tecnologías de la Información y las Comunicaciones-TICS, del MINENERGÍA, estará siempre comprometido y en búsqueda constante de estrategias y alternativas que, permitan el aseguramiento y la preservación de los cuatro pilares de la seguridad de la información: confidencialidad, integridad, disponibilidad, y privacidad de la información institucional, como producto del desarrollo de su actividad, la cual será protegida en los entornos de persistencia y transmisión de la misma (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, e-mail, transmitida en conversaciones, entre otros.), de su origen (de la propia organización o de fuentes externas) 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 Ministerio de Tecnologias de la Información y Comunicaciones en adelante MINTIC, el cual orienta a las entidades a la preservación de la confidencialidad, integridad y disponibilidad de la información, ademas permite fijar los criterios para proteger la privacidad de la información y 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/IEC 27001:2022, ISO/IEC 22301:2019, e ISO/IEC 31000:2018.

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), el Sistema de Gestión y Continuidad del Negocio (SGCN), 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 y procedimientos definidos por las normas anteriormente mencionadas.

2. Justificación

Debido a la necesidad de cumplir con el ciclo PHVA, el cual busca la mejora continua del sistema de gestión, y apoyado en los diferentes controles de seguridad que deben ser implementados en busca de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, es importante establecer un plan de seguridad de la información que facilite la gestión y el seguimiento de las actividades anuales que son cruciales para el éxito del Modelo de Seguridad y Privacidad de la Información (MSPI).

3. Contextualización

Con el ánimo de asegurar la integridad, disponibilidad, confidencialidad y privacidad de la información de sus procesos, el MINENERGÍA, se encuentra en la fase del HACER y VERIFICAR del ciclo PHVA del Plan de Seguridad y Privacidad de la información (MSPI) a través de la **implementación de la herramienta de Gobierno Riesgo y Cumplimiento adquirida por la entidad, la cual se encuentra sin soporte en estos momentos**, y que puede permiter el cumplimiento a la exigencia del Gobierno Nacional en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), de la política de Gobierno Digital y la Política de Seguridad Digital, propendiendo de igual forma por los derechos como el habeas data, la imagen, la intimidad, el buen nombre y la privacidad.

4. Antecedentes

El MINENERGÍA ha venido contratando el diagnóstico y planeación del Modelo de Seguridad y Privacidad de la Información (MSPI,) dando asi cumplimiento a lo estipulado en la estrategia de Gobierno en línea y la Política de Gobierno Digital.

El dinamismo, la evolución y actualización en los modelos, guías y normas, le han permitido al Ministerio incorporar y mejorar el uso de nuevas prácticas en seguridad de la información

alineado todo el tiempo a la vigencia de las normas y estándares antes mencionados, apropipandolos e integrándolos a las necesidades y requerimientos actuales de la Entidad, tal cual ocurrió con la expedición de la nueva resolución de políticas de seguridad de la información, por parte de la Alta Dirección e identificada como: Resolución 40646 del 01.11.2023, por medio de la cual se establece el marco de las POLÍTICAS APLICABLES AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI DEL MINISTERIO DE MINAS Y ENERGÍA.

Lo anterior, en busca de poder contar con una directriz que, permitan sustentar y fortalecer la protección de los cuatro pilares de la seguridad de la información: Integridad, Disponibilidad, Confidencialidad y Privacidad de la Información.

5. Objetivos

A continuación, se presentan el objetivo general y los objetivos específicos:

5.1 Objetivo General

Establecer las directrices para la gestión y seguimiento de la seguridad de la información por medio de actividades de control y planes de acción que ayuden a mantener la confidencialidad, integridad, disponibilidad y privaciad de la información, así como la relación de los procedimientos asociados a las políticas establecidas que permitan asegurar la protección y persistencia de la SI.

5.2 Objetivos Específicos

a) Contribuir al incremento de la transparencia, frente a la gestión pública.
b) Dar lineamiento para la implementación de la gestión de la seguridad y privacidad de la información.
c) Establecer las actividades anuales a ejecutar en temas de Seguridad de la Información.
d) Concentrar los planes relacionados con Seguridad de la Información en un punto único de consulta y gestión.

6. Alcance

Los lineamientos del Modelo de seguridad y privacidad de la información (MSPI) y sus correspondientes guías de apoyo, serán aplicadas a los procesos estratégicos, misionales, de apoyo, de evaluación y control, así como especiales del MINENERGÍA, por tal motivo, deberán ser conocidas y cumplidas por todas las partes interesadas, que accedan a los sistemas de información, repositorios (locales, nube, e híbridos, entre otros) e instalaciones físicas.

7. Plan de Seguridad de la Información

A continuación, se presentan los numerales que hacen parte del Plan de Seguridad de la Información (PSI):

7.1 Plan Operacional de Seguridad de la Información

A continuación, se describen los componentes que hace parte del plan operativo de Seguridad de la Información:

7.1.1 Gestión de Activos de Información

A continuación, se describe como se debe realizar la gestión de activos de información:

Los activos deben revisarse y actualizarse anualmente, por lo que es necesario que las áreas propietarias y los responsables de los activos de información ejecuten esta actividad como mínimo una vez al año.

Las actividades por ejecutar para esta actualización se pueden consultar en la **Tabla *3***.

Tabla 3

Actualización de Activos de Información

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA ENTREGA
1	Distribución del inventario de activos de información por dependencia.	Grupo de Relacionamiento con el Ciudadano y Gestión de la Información.	Semana 2 Mes 2
2	Revisión y actualización del inventario de activos de información por dependencia.	Responsables de los activos de información (directivos).	Semana 4 Mes 2
3	Envío del inventario de activos de información actualizado.	Responsables de los activos de información (directivos).	Semana 1 Mes 3
4	Revisión y unificación de los activos de información.	Grupo de Relacionamiento con el Ciudadano y Gestión de la Información.	Semana 1 Mes 3
5	Publicación en el portal de la Entidad.	Oficina de Planeación y Gestión Internacional.	Semana 4 Mes 3

Fuente: Grupo TICS

7.1.2 Gestión de Riesgos de Seguridad de la Información

A continuación se describe como se debe realizar la gestión de riesgos de Seguridad de la Información:

El análisis de riesgos de SI debe realizarse periódicamente, por lo que es necesario que los propietarios de los riesgos ejecuten esta actividad como mínimo una vez al año.

Las actividades por ejecutar para este análisis se pueden consultar en la **Tabla *4***.

Tabla 4

Seguimiento al Análisis de Riesgos de Seguridad de la Información

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA ENTREGA
1	Entregar Riesgos Gestión TICS y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información a OPGI	Profesional delegado Grupo TICS	Semana 1 Mes 1
2	Comunicar las fechas de inicio y fin de la actualización de riesgos de seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Semana 3 Mes 1
3	Ejecutar análisis de riesgos de seguridad.	Responsables de los activos de información (directivos).	Semana 1 Mes 4
4	Comunicar finalización del análisis de riesgos por dependencia.	Responsables de los activos de información (directivos).	Semana 1 Mes 5
5	Revisión del análisis de riesgos efectuado por todas las dependencias.	Oficial de seguridad de la información o quien haga sus veces.	Semana 2 Mes 5
6	Generar la hoja de ruta del plan de tratamiento de riesgos.	Oficial de seguridad de la información o quien haga sus veces.	Semana 4 Mes 5
7	Aprobar análisis de riesgos.	Oficina de Planeación y Gestión Internacional.	Semana 1 Mes 6

Fuente: Grupo TICS

7.1.3 Tratamiento de Riesgos

Atendiendo las indicaciones y recomendaciones de la Oficina de Planeación y Gestión Internacional, en el sentido que, para la presente vigencia este Plan, se adaptara y adoptara la misma metodología de trabajo dispuesta desde la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6”, expedida por el DAFP en noviembre de 2022, para lo cual los riesgos descritos tanto en el Plan de Tratemiento de Riesgos de Seguridad y Privacidad de la Informacación, como los riesgos de la gestión TIC, tendrán seguimiento y control trimestral durante la vigencia 2024.

7.1.4 Gestión de políticas y procedimientos

Es necesario hacer una revisión y ajuste a las políticas y normas de seguridad con base en los incidentes presentados en el periodo anterior, los resultados del análisis de riesgos, las auditorías de seguridad, los cambios organizacionales que haya surtido la Entidad y la revisión por la dirección.

Las actividades por ejecutar para la actualización de políticas y procedimientos se pueden consultar en la **Tabla *5***.

Tabla 5

Gestión de Políticas y Procedimientos de Seguridad de la Información

No	Descripción de la Actividad	Responsable	Fecha
1	Revisar los incidentes del periodo anterior, los resultados del análisis de riesgos, las auditorías de seguridad, los cambios organizacionales que haya surtido la Entidad y la revisión por la dirección.	Oficial de seguridad de la información o quien haga sus veces.	Semana 3 Mes 2
2	Establecer plan de ajustes para las políticas y procedimientos de seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Semana 4 mes 2
3	Efectuar los cambios necesarios a las políticas y procedimientos de seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Semana 1 Mes 3
4	Aprobar las políticas de seguridad.	Comité institucional de gestión y desempeño.	Semana 1 Mes 4
5	Divulgar las políticas de seguridad.	Oficina de Planeación y Gestión Internacional.	Semana 4 Mes 4

Fuente: Grupo TICS

7.1.5 Gestión de Recursos de Seguridad de la Información

Cada año se deben gestionar los recursos económicos para el mantenimiento de la seguridad de la información, esto debe ser una salida de la revisión por la Alta Dirección, de tal forma que estas solicitudes tengan respaldo directivo para su aprobación.

Las actividades por ejecutar para este análisis se pueden consultar en la **Tabla 6**.

Tabla 6

Gestión de Recursos de Seguridad

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Establecer las necesidades de presupuesto en seguridad de la información.	Oficial de seguridad de la información o quien haga sus veces.	Semana 1 Mes 3
2	Efectuar la revisión por la dirección del SGSI.	Comité institucional de gestión y desempeño.	Semana 3 Mes 3
3	Generar informe de salidas de revisión por la Dirección.	Comité institucional de gestión y desempeño.	Semana 4 Mes 3

4	Formalizar la solicitud de presupuesto en seguridad de la información para el próximo periodo.	Oficial de seguridad de la información o quien haga sus veces.	Semana 2 Mes 4
5	Aprobación de presupuesto.	Alta dirección	Semana 4 Mes 4

Fuente: Grupo TICS

7.2 Plan de Seguimiento y Evaluación de la Implementación y Mantenimiento de la Seguridad de la Información

A continuación se describe como realizar el seguimiento y evaluación de la implementación de Sistema de Gestión de Seguridad de la Información:

7.2.1 Gestión de Indicadores

Los indicadores deben resvisarse y actualizarse según el resultado de la revisión por la dirección en la cual se establece la información que esta requiere, para valorar la gestión realizada en el periodo anterior.

Las actividades por ejecutar para este análisis se pueden consultar en la **Tabla *7***.

Tabla 7

Gestión de Indicadores

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Preparar el resultado de los indicadores para la revisión por la dirección.	Oficial de seguridad de la información o quien haga sus veces.	Entregas trimestrales acorde programación OPGI
2	Efectuar la revisión por la dirección del SGSI.	Comité institucional de gestión y desempeño.	Entregas trimestrales acorde programación OPGI
3	Generar informe de salidas de revisión por la dirección.	Comité institucional de gestión y desempeño.	Entregas trimestrales acorde programación OPGI
4	Realizar ajustes a los indicadores solicitadas por la revisión por la dirección.	Oficial de seguridad de la información o quien haga sus veces.	Entregas trimestrales acorde programación OPGI
5	Aprobar indicadores de seguridad que han surtido cambios.	Comité institucional de gestión y desempeño.	Entregas trimestrales acorde programación OPGI

Fuente: Grupo TICS

7.2.2 Gestión de Vulnerabilidades

La norma ISO 27001 en el anexo A plantea el control de gestión de vulnerabilidades técnicas, en lo cual se debe tener en cuenta no solo la ejecución de pruebas de vulnerabilidad, sino

que también su acción correctiva y verificación de que las actividades ejecutadas eliminaron la falencia encontrada.

Las actividades para tener en cuenta en la gestión de vulnerabilidades técnicas se pueden consultar en la **Tabla *8***.

Tabla 8

Gestión de Vulnerabilidades Técnicas

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Realizar el listado de los activos de información (equipos, servicios, plataformas, SO, BD, programas, SI, entre otros) a los cuales se les van a realizar pruebas de vulnerabilidades técnicas.	Administradores de los sistemas de información en conjunto con el Oficial de Seguridad de la información o quien haga sus veces.	Semana 1 Mes 7
2	Realizar ejecución de pruebas.	Hacker ético.	Semana 2 Mes 7
3	Generar informe de hallazgos.	Hacker ético.	Semana 3 Mes 7
4	Ejecutar acciones de remediación a las vulnerabilidades detectadas.	Administradores de los sistemas de información.	Semana 2 Mes 8
5	Ejecutar pruebas de re-test para verificar que efectivamente se hayan cerrado las vulnerabilidades.	Hacker ético.	Semana 2 Mes 11

Fuente: Grupo TICS

7.2.3 Plan de Auditorías de Seguridad de la Información

Para el SGSI se requiere realizar auditorías de seguridad para evidenciar el seguimiento y gestión del sistema, para ello se debe tener en cuenta lo siguiente:

Objetivo de la auditoría: Revisar el funcionamiento y mantenimiento del Sistema de Gestión de Seguridad de la Información del MINENERGÍA.

Alcance de la auditoría: El alcance de la auditoría abarca a todo el MINENERGÍA y sus procesos, teniendo como base de revisión la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de MINTIC. Los procesos por auditar son:

- Direccionamiento estratégico y control internacional.
- Gestión internacional.
- Administración del sistema integrado de gestión.
- Comunicación institucional.
- Formulación y adopción de planes, programas, reglamentos y lineamientos sectoriales.
- Ejecución de políticas, proyectos y reglamentación sectorial.
- Seguimiento, vigilancia y control a políticas, planes, programas, proyectos y reglamentación sectorial.
- Gestión de talento humano.
- Gestión documental.

- Gestión financiera.
- Gestión tecnológica, de información y comunicación.
- Gestión de recursos físicos.
- Gestión jurídica.
- Auditoría y evaluación.
- Control interno disciplinario.
- Servicio al ciudadano.

Criterios de auditoría: Normatividad vigente que aplique a la fecha, así mismo las Políticas, Procedimientos, Instructivos, Planes, Mapas de Riesgos de Seguridad de la Información, Informe de Revisión por la Dirección y el Plan de Seguridad de la información.

Las actividades para tener en cuenta en la realización de las auditorías de seguridad se pueden consultar en la **Tabla *9***.

Tabla 9

Plan de Auditorias de Seguridad de la Información

NO	ACTIVIDADES	RESPONSABLE	FECHA
1	Establecimiento del perfil del equipo auditor.	Oficina de Control Interno	Semana 3 Mes 11
2	Definición del grupo auditor.	Oficina de Control Interno	Semana 1 Mes 12
3	Generar el listado de procesos a auditar con la fecha y hora en la que se realizará la auditoría (Instrumento de evaluación del MSPI de MINTIC, análisis de riesgos, revisión por la dirección, políticas de seguridad, entre otros).	Oficina de Control Interno	Semana 3 Mes 12
4	Entrega de listado de información a entregar al auditor previa ejecución de la auditoría.	Oficina de Control Interno	Semana 1 Mes 1
5	Reunión de Apertura de Auditoría	Auditor	Semana 3 Mes 1
6	Ejecución de auditoría.	Auditor	Semana 3 Mes 1
7	Reunión de Cierre de auditoría	Auditor	Semana 4 Mes 1
8	Redacción de informe de auditoría	Auditor	Semana 4 Mes 1
9	Presentación de informe de auditoría	Auditor	Semana 1 Mes 2
10	Plan de subsanación de no conformidades.	Administradores de los sistemas de información en conjunto con el Oficial de Seguridad de la información o quien haga sus veces.	Semana 2 Mes 2

Fuente: Grupo de TICS

7.2.4 Plan de Mejoramiento Continuo

El mejoramiento continuo de seguridad de la información está estrechamente ligado a la ejecución de auditorías, con base en la auditoría realizada para el periodo se deben ejecutar las siguientes actividades una vez se cuente con el informe de auditoría:

Tabla 10

Mejoramiento Continuo

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Identificar las no conformidades documentadas en el informe de auditoría.	Oficina de Control Interno y/o ente externo.	Semana 3 Mes 2
2	Evaluar las necesidades de acciones para eliminar las causas de la no conformidad con el fin de que no vuelva a ocurrir.	Oficial de seguridad de la información o quien haga sus veces.	Semana 3 Mes 2
3	Establecer las acciones para controlar y corregir las no conformidades.	Oficial de seguridad de la información o quien haga sus veces.	Semana 1 Mes 3
4	Ejecutar las acciones para controlar y corregir las no conformidades.	Oficial de seguridad de la información o quien haga sus veces.	Semana 2 Mes 3
5	Revisar la eficacia de las acciones correctivas tomadas.	Oficial de seguridad de la información o quien haga sus veces.	Semana 2 Mes 5
6	Realizar los cambios al SGSI de ser necesario.	Oficial de seguridad de la información o quien haga sus veces.	Semana 4 Mes 5
7	Establecer un mecanismo de contacto para las sugerencias de las partes interesadas que propongan mejoras al SGSI.	Oficial de seguridad de la información o quien haga sus veces.	Semana 4 Mes 6
8	Implementar el mecanismo de contacto para las sugerencias de las partes interesadas que propongan mejoras al SGSI.	Oficial de seguridad de la información o quien haga sus veces.	Semana 1 Mes 7

Fuente: Grupo TICS

7.2.5 Revisión por la Alta Dirección

La revisión por la dirección debe ejecutarse a intervalos planificados; para ello se debe tener como entrada lo siguiente:

- Estado de las acciones con relación a las revisiones previas por la Alta Dirección.
- Cambios en cuestiones externas e internas que le apliquen al SGSI.
- Realimentación sobre el desempeño de la Seguridad de la Información.
- Resultados de la auditoría.
- Realimentación de las partes interesadas.
- Resultados del análisis y tratamiento de riesgos.

- Oportunidades de mejora continua.

Las actividades a tener en cuenta para la revisión por la dirección se pueden consultar en la **Tabla *11***.

Tabla 11

Revisión por la Alta Dirección

NO	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Alistamiento de las entradas para la revisión por la dirección.	Oficial de Seguridad de la información o quien haga sus veces.	Semana 1 Mes 3
2	Ejecución de la revisión por la dirección.	Comité institucional de gestión y desempeño.	Semana 3 Mes 3
3	Redacción de informe de la revisión por la dirección.	Comité institucional de gestión y desempeño.	Semana 4 Mes 3

Fuente: Grupo TICS

7.3 Plan de Comunicaciones

A continuación, se detalla el plan de comunicaciones de seguridad.

7.3.1 Caracterización de Interesados

En la Tabla 12, se detalla la caracterización de interesados, para ello, es importante tener en cuenta la clasificación de las características de los grupos de interés:

a) Los **internos** incluyen directivos y trabajadores (empleados).
b) Los **externos** a los clientes, proveedores, entidades financieras, sindicatos, comunidad local, organizaciones sociales, entre otros.
c) **Primarios**, mantienen relaciones contractuales con la Entidad.
d) **Secundarios**, influyen de manera menos formal.

Tabla 12

Caracterización de Interesados

GRUPO DE INTERÉS	DESCRIPCIÓN	CARACTERÍSTICAS DE LOS GRUPOS DE INTERÉS
Ministra o Ministro del MINENERGÍA	Personal que trabaja directamente con el(la) Ministro(a) del MINENERGÍA.	• Internos. • Primarios.
Comité Institucional de Gestión y Desempeño	Acorde con lo definido en el Decreto 1499 de 2017 debe incluir todos los temas que atiendan la implementación y desarrollo de las	• Internos. • Primarios.

GRUPO DE INTERÉS	DESCRIPCIÓN	CARACTERÍSTICAS DE LOS GRUPOS DE INTERÉS
	políticas de gestión definidas en el MIPG.	
Colaboradores de TI	Todos los colaboradores que trabajan en la Gerencia de Tecnologías de Información.	• Internos y externos. • Primarios y Secundarios.
Oficina de planeación y gestión organizacional	Todos los colaboradores que trabajan en la Gerencia de Planeación Institucional.	• Internos y externos. • Primarios y Secundarios.
Oficina de Control Interno	Personal que trabaja directamente en la Oficina de Control Interno.	• Internos. • Primarios.
Ciudadanos	Ciudadanía de Colombia.	• Externos. • Secundarios.
Todos los colaboradores del MINENERGÍA	Funcionarios y contratistas del MINENERGÍA	• Internos y externos. • Primarios y Secundarios.
Secretaría General	El(la) Secretario(a) General de MINENERGÍA.	• Internos. • Primarios.

Fuente: Grupo TICS

7.3.2 Comunicaciones

Es importante que para que la Seguridad de la Información tenga el resultado esperado al interior de la Entidad, se definan los documentos que serán comunicados y los grupos de interés (tal como se realizó en la Tabla 12), además de algunos aspectos inherentes a la comunicación como lo son el canal, el formato, el responsable y la frecuencia de la comunicación. En la Tabla 13 se muestra el modelo de comunicaciones de Seguridad de la Información.

Tabla 13

Comunicaciones

MENSAJE	GRUPO DE INTERÉS	CANAL	FORMATO	RESPONSABLE	FRECUENCIA
Políticas y procedimientos de seguridad	Comité Institucional de Gestión y Desempeño	Reunión de comité	.DOC	Oficial de Seguridad de la información o quien haga sus veces.	Anual o cada vez que se cree o modifique una política o procedimiento
	Todos los colaboradores del MINENERGÍA	Correo electrónico para ingresar a la herramienta GRC	.PDF		

MENSAJE	GRUPO DE INTERÉS	CANAL	FORMATO	RESPONSABLE	FRECUENCIA
Sensibilización en seguridad	Todos los colaboradores del MINENERGÍA	Charlas, conferencias, capacitaciones.	.PPT	Oficial de Seguridad de la Información o quien haga sus veces.	Anual
Análisis de riesgos	Comité Institucional de Gestión y Desempeño Oficina de planeación y gestión organizacional Oficina de Control Interno Ministro del MINENERGÍA Todos los colaboradores del MINENERGÍA	Herramienta GRC (Gobierno, Riesgo y Cumplimiento)	Formato del Aplicativo	Oficial de Seguridad de la información o quien haga sus veces.	Anual
Incidentes de seguridad	Comité Institucional de Gestión y Desempeño Ministro del MINENERGÍA Secretaría General	Correo electrónico con informe del incidente	.DOC	Oficial de Seguridad de la información o quien haga sus veces.	Cada vez que se requiera.
Comunicados de prensa	Ciudadanos	Entrevista	Impreso y/o audiovisual	Secretaría General	Cada vez que se requiera.

Fuente: Grupo TICS

7.4 Plan de sensibilización y capacitación

Como resultado de la aplicación del *Procedimiento de capacitación y sensibilización de personal*, el plan de sensibilización y capacitación es uno de los mecanismos por medio del cual la Entidad hace que sus usuarios tomen conciencia de la política de Seguridad de la Información, su contribución a la eficacia del sistema de gestión de la SI, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y las implicaciones de la no conformidad con los requisitos del sistema de gestión de la SI.

7.4.1 Sensibilización

La comunicación es uno de los procesos más relevantes y complejos que lleva a cabo el ser humano. Por ello, es importante tomar conciencia y asumir el control de lo que se comunica para ser eficientes y obtener el máximo de las personas y las situaciones.

Se estima que más de un 60% de las actividades diarias de las personas involucran alguna forma de comunicación. (Rankin, citado por McEntee. Comunicación Oral. Alhambra Editorial, 1988), como se presenta en la siguiente ilustración:

Ilustración 1

Porcentaje de tiempo dedicado a la comunicación

Fuente: Rankin, citado por McEntee. Comunicación Oral. Alhambra Editorial, 1988

La comunicación asertiva es la clave para llevar a cabo campañas de sensibilización, en adelante, se listan las actividades que se deben realizar para diseñar campañas de sensibilización relacionadas con el SGSI.

7.4.1.1 Selección de temas

Inicialmente la Entidad debe seleccionar los temas que, dependiendo la etapa de madurez en la que se encuentre el SGSI, es necesario comunicar y fortalecer. De acuerdo con la norma técnica ISO/IEC 27002:2022, entre los temas que no pueden faltar en la sensibilización, se encuentran:

a. La política general de Seguridad de la Información.
b. Las responsabilidades en Seguridad de la Información y los medios por los cuales se cumplen dichas responsabilidades.
c. Las políticas y procedimientos de Seguridad de la Información.
d. La necesidad de conocer y cumplir con las reglas y obligaciones de seguridad de la información aplicable, tal como se definen en las políticas, normas, leyes, reglamentos, contratos y acuerdos.
e. La rendición personal de cuentas por las acciones y omisiones propias, y las responsabilidades generales relacionadas con la seguridad y la protección de la información que pertenece a la Entidad y a las partes externas.
f. Los puntos de contacto y los recursos para información adicional y asesoría sobre asuntos de Seguridad de la Información, incluidos los materiales de educación y formación sobre Seguridad de la Información.

Entre algunas de las fuentes que se deben consultar para identificar el temario para la sensibilización se encuentran:

a. Las actualizaciones que se realicen en la documentación del SGSI.
b. Los incidentes de Seguridad de la Información.
c. Los resultados de otras campañas de sensibilización.
d. Los resultados de las auditorías internas y externas.
e. La mejora continua del SGSI.
f. Las amenazas externas y tendencias en Seguridad de la Información.
g. La legislación aplicable vigente.
h. Cualquier modificación, actualización o mejora al SGSI.
i. Los News informativos como los días internacionales declarados para celebrar los temas más representativos de seguridad de la información

7.4.1.2 Modalidad

El siguiente paso, es seleccionar la modalidad más acorde con el tipo de información a comunicar, entre las diferentes opciones con las que cuenta la Entidad, se encuentran:

a. **E-card:** Consiste en diseñar una tarjeta virtual llamativa, con poco texto y más imágenes, esta modalidad es más efectiva a la hora de trasmitir mensajes muy puntuales y concisos.
b. **Infografía**: es una representación gráfica que pretende explicar o resumir una información, combinando iconos como imágenes, gráficos, entre otros, con descripciones, narraciones, interpretaciones y datos. Son interpretaciones visuales de los propios textos y resultan más atractivas para el lector.
c. **Videos animados:** Consiste en diseñar presentaciones animadas y videos explicativos animados muy cortos de máximo de cinco minutos de duración.
d. **Papel tapiz:** Conocido además como **wallpaper**, fondo de escritorio o fondo de pantalla, se trata de la fotografía o la ilustración que el administrador de una computadora (ordenador), escoge como fondo de la pantalla.

7.4.1.3 Medios

Posteriormente, se deben seleccionar los medios o canales por los cuales se realizará el envío o publicación de las piezas gráficas que se han diseñado, entre los canales existentes en la Entidad se encuentran:

a. **Correo**: Se trata del correo institucional en Microsoft Teams con dominio minienergia.gov.co establecido por la Entidad para todos los comunicados oficiales.
b. **Portal web:** Se trata de la página web oficial: https://www.MINENERGÍA.gov.co/ de la Entidad.
c. **Pantallas**: Se trata de pantallas ubicadas en diferentes sitios estratégicos de la Entidad para su consulta en sitio.

Finalmente, el Oficial de Seguridad de la Información o quien haga sus veces, en consenso con los encargados del Grupo de Comunicaciones y Prensa, procede a asignar las fechas en las que se debe emitir cada pieza grafica consolidando así el cronograma para la

sensibilización. Ver Anexo 1_Cronograma para Capacitación, Sensibilización y Gestión del Cambio.

7.4.2 Capacitación

El programa de capacitación debe estar enfocado a asegurar que los usuarios que realizan, bajo su control, un trabajo que afecte el desempeño de la Seguridad de la Información, sean competentes y tengan la formación adecuada para desarrollar dicha labor. En línea con la norma técnica ISO/IEC 27002:2022, la educación y la formación en Seguridad de la Información se deben llevar a cabo periódicamente. La educación y entrenamiento iniciales aplican a quienes se transfieren a nuevos cargos o roles con requisitos de Seguridad de la Información considerablemente diferentes, no solo para los nuevos usuarios, y se debe llevar a cabo antes de que el usuario asuma el nuevo rol.

7.4.2.1 Selección de temas

La Entidad debe desarrollar el programa de educación y de formación para impartir la educación y la formación eficazmente. El programa debe estar en línea con las políticas y procedimientos pertinentes de Seguridad de la Información del SGSI, teniendo en cuenta la información de la entidad que se va a proteger, y los controles que se han implementado para proteger la información. Entre los temas que no pueden faltar en el programa de capacitación, pero con un nivel de detalle e intensidad horaria mayor, se encuentran:

a. La política general de Seguridad de la Información.
b. Las responsabilidades en Seguridad de la Información y los medios por los cuales se cumplen dichas responsabilidades.
c. Las políticas y procedimientos de Seguridad de la Información.
d. La necesidad de conocer y cumplir con las reglas y obligaciones de Seguridad de la Información aplicable, tal como se definen en las políticas, normas, leyes, reglamentos, contratos y acuerdos.
e. La rendición personal de cuentas por las acciones y omisiones propias, y las responsabilidades generales relacionadas con la seguridad y la protección de la información que pertenece a la organización y a las partes externas.
f. Los puntos de contacto y los recursos para información adicional y asesoría sobre asuntos de Seguridad de la Información, incluidos los materiales de educación y formación sobre SI.

Entre algunas de las fuentes que se deben consultar para identificar el temario para la capacitación se encuentran:

a. Los resultados del diagnóstico de capacitación en Seguridad de la Información.
b. Las actualizaciones que se realicen en la documentación del SGSI.
c. Los incidentes de Seguridad de la Información.
d. Los resultados de las auditorías internas y externas.
e. La mejora continua del SGSI.
f. Las amenazas externas y tendencias en Seguridad de la Información.
g. La legislación aplicable vigente.

h. Formación de auditores internos en la NTC/ISO 27001:2013.
i. Formación en gestión de riesgos de seguridad de la información.
j. Cualquier modificación, actualización o mejora al SGSI.
k. Seguridad Informática.
l. Análisis de vulnerabilidades.
m. Los resultados de las evaluaciones de las capacitaciones.

7.4.2.2 Modalidad

El siguiente paso, es seleccionar la modalidad más acorde con el tipo de capacitación a dictar y las normas sanitarias vigentes en su momento, entre las diferentes opciones con las que cuenta la Entidad, se encuentran:

a. **Presencial**: Catedra dirigida en las instalaciones de la Entidad.
b. **Virtual**: Catedra dirigida y realizada por medio de herramientas virtuales de comunicación como los son Google meet, Microsoft teams, entre otros.
c. **Estudio autónomo**: Consiste en sesiones organizadas por módulos y precargadas en herramientas de aprendizaje para que los usuarios realicen los cursos sin la presencia del catedrático.

7.4.2.3 Medios

Posteriormente, se deben seleccionar los medios o canales por los cuales se realizarán las capacitaciones virtuales, entre los canales se encuentran:

a. Herramientas virtuales de comunicación como lo son: Microsoft teams.

7.4.2.4 Definición de públicos objetivos

No todos los usuarios se deben capacitar en los mismos temas ni con el mismo enfoque, de ahí la importancia de identificar primero las necesidades de capacitación y luego consolidar los diferentes grupos de usuarios que se requiere reforzar con los temas seleccionados. Entre los diferentes públicos objetivo a tener en cuenta, pero sin limitarse a este listado, se encuentran:

a. Ministro y directores.
b. Jefes de oficina y coordinadores.
c. Líderes de proceso.
d. Comité institucional de gestión y desempeño.
e. Oficial de seguridad de la información.
f. Profesionales de seguridad de la información.
g. Grupo de soporte informático.
h. Propietarios de la información.
i. Responsable del riesgo.

Finalmente, el Oficial de Seguridad de la Información o quien haga sus veces procede a asignar las fechas en las que se debe impartir las sesiones de capacitación consolidando así el cronograma para la capacitación. Ver Anexo No. 1. Cronograma para Capacitación, Gestión del Cambio y Sensibilización.

7.5 Hoja de Ruta

En la siguiente tabla, se ilustra la hoja de ruta a seguir para el plan de Seguridad de la Información, teniendo en cuenta el mapeo de todos los planes relacionados con seguridad que se consolidan en el año:

Tabla 14

Hoja de Ruta del SGSI

Pendiente inclir hoja de ruta nueva

Fuente: Grupo TICS

Las actividades que tienen un mismo color tienen puntos en común y se relacionan entre sí para su ejecución bien sea por temas de auditoría, revisión, riesgos, ajustes o sensibilización.

Ver Anexo No. 2 Hoja de Ruta de Plan de Seguridad y Privacidad de la Información 2024

8. Recomendaciones

a) Es importante que las pruebas de seguridad contemplen ingeniería social y hacking ético, para este último se debería hacer re-test.

b) El plan de seguridad debe actualizarse siempre a final de año.

c) Las auditorías deben contemplar actividades de auditorías técnicas.

9. Mejores prácticas

La norma ISO/EIC 27002:2022, ofrece las mejores prácticas de la industria para la implementación del sistema de gestión de Seguridad de la Información, este estándar contiene varios capítulos relacionados con los controles de red, host y auditoría que fueron útiles a la hora de generar las recomendaciones de seguridad en el host, red, ciberseguridad, monitoreo y control.

Publicaciones de la NIST 800-39, 800-82, y 800-53, estos estándares brindan mejores prácticas basadas en los controles de seguridad y privacidad para sistemas de información federales y de control industrial, y en gestión de riesgo corporativo. Estas publicaciones fueron de gran utilidad en la definición de la arquitectura de seguridad y gestión de riesgos.

10. Glosario

- **Activo:** Cualquier cosa que tiene valor para la organización. (ISO/IEC 27000:2014)
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo aceptable. (ISO/IEC 27000:2014)
- **Archer:** Sistema de información proporcionado por el fabricante RSA ARCHER, mediante el cual se llevan el registro y control de actividades inherentes a la seguridad y privacidad de la información del Ministerio de Minas y Energía a través de los Módulos: Activos, Riesgos, BIA, Incidentes, Eventos, Planes, Normatividad, Cumplimiento, Balanced Score Card, Arquitectura Empresarial y Ciberseguridad.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000:2022)
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000:2022)
- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo. (ISO/IEC 27001:2022)
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad. (ISO/IEC 27000:2022)
- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (ISO/IEC 27000:2022)
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (ISO/IEC 27000:2022)
- **Guía DAFP:** Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6.
- **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 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. (ISO/IEC 27000:2022)
- **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 funcionarios, servidores públicos, contratistas, proveedores, ciudadanos y agencias relacionadas con el MINENERGÍA.
- **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. (ISO/IEC 27000:2022).
- **Procedimiento:** Es la forma especificada para llevar a cabo una actividad o un proceso. (ISO/IEC 27000:2022).
- **Riesgo:** Toda posibilidad de ocurrencia de aquella situación que pueda entorpecer el desarrollo normal de las funciones de la Entidad y le impidan el logro de sus objetivos. (ISO/IEC 27000:2022).

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000:2022).
- **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. (ISO/IEC 27000:2022).
- **SÍGAME:** Sistema Integrado de Gestión del Ministerio de Minas y Energía.
- **Tratamiento del riesgo:** Proceso de selección e implementación de acciones de mejorar que permita gestionar el riesgo. (ISO/IEC 31000:2018).
- **Valoración del riesgo:** Proceso de análisis y evaluación del riesgo. (ISO/IEC 31000:2018)
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000:2022)

11. Referencias

- ISO. (2013). *ISO 27001 Sistema de Gestión de Seguridad de la Información.* ISO.
- ISO. (2018). ISO/IEC 27000:2018. *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario*.
- MINTIC. (2 de Junio de 2016). *Lo que usted debe saber del Conpes de Seguridad Digital*. Obtenido de Portal del Ministerio de Tecnologías de la Información y las Comunicaciones: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15410:Lo-que-usted-debe-saber-del-Conpes-de-Seguridad-Digital
- MinTIC. (2019). *Manual de Gobierno Digital.* Bogotá: MinTIC.
- NIST. (21 de Junio de 2020). *CSRC NIST - COMPUTER SECURITY RESOURCE CENTER*. Obtenido de NIST: https://csrc.nist.gov/glossary