Manual Sistema de Gestión de Seguridad de la Información y Ciberseguridad

Vicepresidencia Nuevos Negocios Innovación y Tecnología

Dirección Ciberseguridad

M-SGSI-A01-001

Rev. No.	MODIFICACION EFECTUADA		FECHA
1	Version Inicial		1/06/2018
2	Revisión general del manual		4/10/2019
3	Actualización Manual		16/09/2020
4	Se actualizan responsabilidades de la Dirección Ciberseguridad. Se adecua el manual al cumplimiento de los numerales de la NTC-ISO-IEC 27001 Sistemas de Gestión de Seguridad de la Información		4/03/2022
ÍTEM	**ELABORÓ**	**REVISÓ**	**APROBÓ**
CARGO	Profesional Informático	Profesional Informático	Director Ciberseguridad
NOMBRE	Gloria Patricia Arcila Arias	Héctor Valencia Valencia	Germán Uribe Jiménez

EMPRESAS PÚBLICAS DE MEDELLIN E.S.P

Tabla de Contenido

INTRODUCCION

El desarrollo de las Tecnologías de Operación (TO), Tecnologías del Consumidor (TC) y las Tecnologías de Información y Comunicación (TIC) ha generado un nuevo espacio de relación en el que la rapidez y facilidad de los intercambios de información y comunicaciones han eliminado las barreras de distancia y tiempo. El ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas.

Los ataques derivados de estas amenazas, denominados ciberataques, comparten generalmente una serie de características que les son comunes:

- *Bajo Costo:* muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un costo muy reducido.
- Ubicuidad y fácil ejecución: la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos.
- *Efectividad e impacto*: si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado.
- *Reducido riesgo para el atacante*: la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción. (Departamento de Seguridad Nacional de España, 2013)

La tarea de proteger la información y la infraestructura crítica del Grupo EPM es compleja por sí sola; si a eso se le suma la velocidad a la que se están produciendo cambios tecnológicos, el crecimiento y poder de los dispositivos móviles, la información en la nube, el big data, el internet de las cosas, la cuarta revolución industrial (4RI), el aumento en la interconectividad y la interacción social hace que la tarea se vuelve aún más compleja. Adicionalmente, se debe dar cumplimiento a toda la normatividad que aplica a la organización y que requiere, no solo de la implementación de controles de seguridad, sino contar con un sistema de gestión que garantice que estos controles permanezcan en el tiempo con la efectividad requerida y cumpliendo el propósito para el cual fueron implementados.

La seguridad de la información y ciberseguridad se consiguen mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos que se haya elegido y gestionado por medio de un sistema de gestión, incluyendo políticas, procesos, procedimientos, estructuras organizacionales, software y hardware para proteger los activos de información y ciberactivos críticos identificados. Estos controles necesitan ser especificados, implementados, realizarles seguimiento, revisados y mejorados cuando sea necesario, para que la seguridad de la información y los objetivos de negocio específicos se cumplan. Se espera que los controles de seguridad de la información pertinentes se integren de forma coherente con los procesos de negocio de una organización. (ICONTEC, 2017).

Este documento está compuesto por los siguientes capítulos: Contexto, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño, mejora y documentos de referencia, cumpliendo con los numerales de la norma NTC-ISO-IEC 27001 Sistemas de Gestión de Seguridad de la Información.

1. CONTEXTO

1.1. Objetivo del manual

Este manual ha sido elaborado para guiar el cumplimiento de los requisitos de la norma internacional ISO/IEC 27001 que permite visualizar la organización como un sistema que interactúa en forma alineada y articulada con los objetivos de la organización y su modelo de procesos, buscando agregar valor a la organización, funcionarios, proveedores, comunidad, su entorno y demás partes interesadas, especialmente nuestros usuarios.

Describir el Sistema de Gestión de Seguridad de la Información y Ciberseguridad de EPM, su alcance, las interacciones de los procesos, determinar autoridades, responsabilidades, referenciar los procedimientos generales para todas sus actividades y señalar aspectos relacionados con las normas y estándares internacionales de Seguridad de la Información y Ciberseguridad para integrarlos a los sistemas de gestión que actualmente tiene implementados EPM.

1.2. Referencia legal y normativa

Normograma

La documentación legal y los referentes normativos que guían el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, están contenidos en el Normograma que puede ser consultado en el sitio del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en el vínculo:

https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx?InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence

1.3. Definiciones

Glosario de términos

Las definiciones y los términos de este manual pueden ser consultados en el glosario de términos en el siguiente vínculo:

https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx?RootFolder=%2Fsite%2FSIG%2FDVG%2FDTL%5FISO%5F27001%2FDocumentos%20de%20referencia&FolderCTID=0x0120009F6CB89B3665904FAE752A7FFB1AF40F&View=%7BFECE6DF8%2D5028%2D4815%2D9EC2%2D062FA33DEDAE%7D.

2. CONTEXTO DE LA ORGANIZACIÓN

2.1. Empresas Públicas de Medellín

Empresas Públicas de Medellín, EPM es una empresa de servicios públicos domiciliarios que tiene una historia para contar, con cifras y hechos de una responsabilidad social y ambiental que le da sentido a su origen, a su desarrollo y a su estrategia de negocios. En su primera etapa, EPM sólo atendió a los habitantes de Medellín, la ciudad donde inició sus actividades en 1955. Desde entonces ha alcanzado un alto desarrollo que la sitúa a la vanguardia del sector de los servicios públicos en Colombia.

Organizada bajo la figura de "empresa industrial y comercial del Estado", de propiedad del Municipio de Medellín, EPM imprime los más altos estándares internacionales de calidad a los servicios que presta: energía eléctrica, gas por red, agua y saneamiento. Experiencia, fortaleza financiera, transparencia y capacidad técnica, son los principales rasgos que identifican a esta organización, cuyo enfoque principal es su responsabilidad social y ambiental. EPM llega a 123 municipios de Antioquia. En Medellín y el Área Metropolitana del Valle de Aburrá atiende a 3.6 millones de habitantes.

Propósito: Contribuir a la armonía de la vida para un mundo mejor

El propósito moviliza la estrategia y marca nuestra ruta como organización, nos permite orientar decisiones empresariales, nos conecta con nuestro planeta y marca el compromiso con las futuras generaciones. En la medida en que exista una interconexión en red de muchos actores con iniciativas que apuntan a un propósito común, como son los objetivos de desarrollo sostenible y la arquitectura para un mundo mejor, lograremos sumar a la transformación del mundo.

Porque cuando nos unimos en torno a un propósito, construyendo a partir de las diferencias, con las acciones y cambios que conscientemente realizamos día a día, logramos contribuir a la armonía de la vida para un mundo mejor.

Valores

Valores EPM	Atributos de marca
Transparencia	Abierta / Fiable
Responsabilidad	Global / Eficiente / Responsable
Calidez	Humana

EPM, como entidad pública prestadora de servicios, instaura la responsabilidad social como eje transversal que guía sus acciones como parte constitutiva de su estrategia de crecimiento y propósito de sostenibilidad. En su devenir como grupo, EPM se ve convocada a establecer un puente entre la organización y la sociedad, apostándole a la responsabilidad y proceder de su tejido humano.

Direccionamiento estratégico:

Busca orientar la gestión corporativa y competitiva del grupo empresarial hacia el logro de sus proyecciones de largo, mediano y corto plazo y su posicionamiento en el sector, unificando las directrices y lineamientos como elementos direccionadores de la organización.

Para conocer más acerca del Direccionamiento estratégico del Grupo Epm y los elementos que lo componen https://cu.epm.com.co/institucional/sobre-epm/quienes-somos/direccionamiento-estrategico

2.2. Comprensión de las necesidades y expectativas de las partes interesadas

Partes Interesadas

Los Grupos de interés, también llamados comúnmente “Partes interesadas” o Stakeholders, se definieron para EPM a partir de los siguientes criterios:

- Claridad visible en los intereses bidireccionales de la relación EPM-Grupo de Interés
- Constitución legítima de los Grupo de Interés
- Capacidad de impacto del Grupo de Interés sobre la sociedad y sobre la empresa

Los grupos de interés en el caso de Empresas Públicas de Medellín son, en orden de proximidad a la actividad empresarial: dueño, socios (EPM matriz no tiene socios, EPM Grupo Empresarial sí), directivos y funcionarios (Servidores), proveedores y contratistas, clientes, comunidad y Ambiente, competidores, estado.

El plan de relacionamiento con los grupos de interés puede ser consultado en

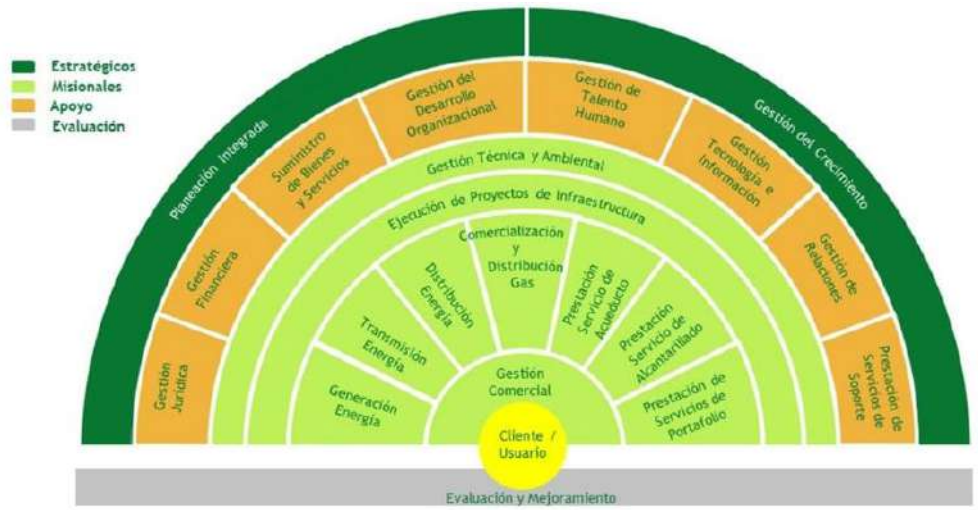
https://www.epm.com.co/site/portals/0/documentos/planes-de-relacionamiento-resumen-ITA.pdf

Identificación de necesidades y expectativas de las partes interesadas

PARTE INTERSADA	NECESIDADES IDENTIFICADAS	ACCIONES
Dueño, socios, inversionistas, Directivos.	• Mantener la confidencialidad, disponibilidad, integridad en los activos de información de la Entidad. • Marco regulatorio organizacional relacionado con la confidencialidad, integridad y disponibilidad de la información. • Gestión de riesgos e implementación de controles para la protección de los activos de información y la tecnología de operación. • Cumplimiento del marco regulatorio externo relacionado con la seguridad de la información y ciberseguridad. • Gestión de incidentes de seguridad de la información y ciberseguridad en la organización. • Toma de conciencia y adopción de buenas prácticas en seguridad de la información. • Resultados de la gestión de la seguridad de la información y ciberseguridad.	• Política y lineamientos de seguridad de la información y ciberseguridad • Reglas de negocio del proceso seguridad digital y continuidad de los servicios de tecnología. • Roles y responsabilidades para la gestión de la seguridad de la información y ciberseguridad – Dirección Ciberseguridad. • Metodología de valoración y clasificación de activos de información. • Índice de información clasificada y reservada. • Etiquetado de información. • Instructivo para el análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos. • Declaración de aplicabilidad de controles • Normograma • Procedimiento de gestión de incidentes de seguridad de la información. • Plan de concienciación y comunicación • Indicadores de gestión.
Estado	• Cumplimiento de las directrices relacionadas con la política de gobierno digital – seguridad y privacidad de la información. • Cumplimiento de las directrices relacionadas con la política de seguridad digital. • Cumplimiento con la implementación de la guía de	• Sistema de gestión de seguridad de la información y ciberseguridad. • Política y lineamientos de seguridad de la información y ciberseguridad. • Roles y responsabilidades para gestionar la seguridad de la información y ciberseguridad – Dirección Ciberseguridad.

PARTE INTERSADA	NECESIDADES IDENTIFICADAS	ACCIONES
	ciberseguridad para infraestructura críticas • Cumplimiento del marco regulatorio relacionado con la seguridad de la información y ciberseguridad (seguridad digital)	• Plan de trabajo Dirección Ciberseguridad.
Gente EPM	• Protección de la información para garantizar su administración y control. • Actividades de toma de conciencia, educación y formación, con referencia a temas de seguridad de la información y ciberseguridad. • Directrices que orienten el actuar de los empleados en lo que respecta a la seguridad de la información y ciberseguridad.	• Política y lineamientos de seguridad de la información y ciberseguridad • Reglas de negocio del proceso seguridad digital y continuidad de los servicios de tecnología. • Roles y responsabilidades para la gestión de la seguridad de la información y ciberseguridad – Dirección Ciberseguridad. • Metodología de valoración y clasificación de activos de información. • Índice de información clasificada y reservada. • Etiquetado de información. • Instructivo para el análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos. • Declaración de aplicabilidad de controles • Plan de concienciación y comunicación
Proveedores y Contratistas	• Requisitos contractuales relacionados con la seguridad de la información y ciberseguridad.	• Política y lineamientos de seguridad de la información y ciberseguridad • Anexo de ciberseguridad
Clientes y usuarios	• Garantizar el tratamiento de los datos personales obtenidos por la entidad para la prestación de sus servicios. • Disponibilidad e integridad de la información a la que requieren acceder.	• Política y lineamientos de seguridad de la información y ciberseguridad • Política de protección de datos personales. • Declaración de aplicabilidad de controles
Comunidad	• Garantizar el tratamiento de los datos personales obtenidos por la entidad en el relacionamiento. • Disponibilidad e integridad de la información a la que requieren acceder.	• Política y lineamientos de seguridad de la información y ciberseguridad • Política de protección de datos personales. • Declaración de aplicabilidad de controles

2.3. Determinación del alcance del sistema de gestión de seguridad de la información

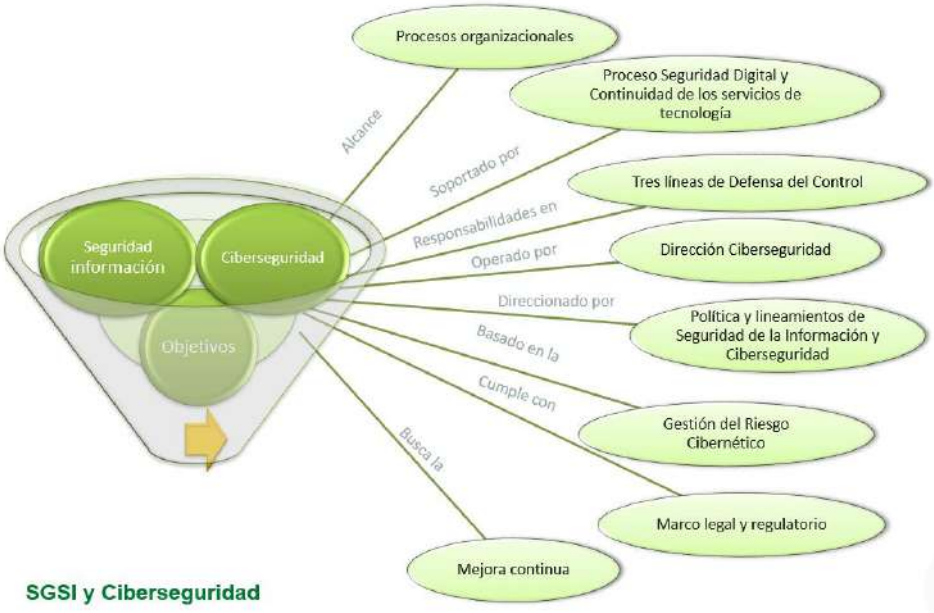


El alcance del Sistema de Gestión de Seguridad de la Información y Ciberseguridad es el modelo de procesos de EPM, enfocado en la protección de la infraestructura y la información críticas requerida para los servicios que presta la organización en sus diferentes negocios.

El modelo de procesos de EPM puede ser consultado en 00. Modelo de Procesos (epm.com.co)

Los controles del ANEXO A de la NTC-ISO-IEC 27001 que aplican a la organización con sus responsables de implementación se describen en la “Matriz de Aplicabilidad”

2.4. Sistema de Gestión de Seguridad de la Información y Ciberseguridad



EPM decide establecer, implementar, mantener y mejorar continuamente sus Sistema de Gestión de Seguridad de la Información y Ciberseguridad, de acuerdo con los requisitos de la norma internacional ISO/IEC 27001 y al cumplimiento regulatorio a que está obligado, e integrarlos a los sistemas de gestión de Grupo EPM.

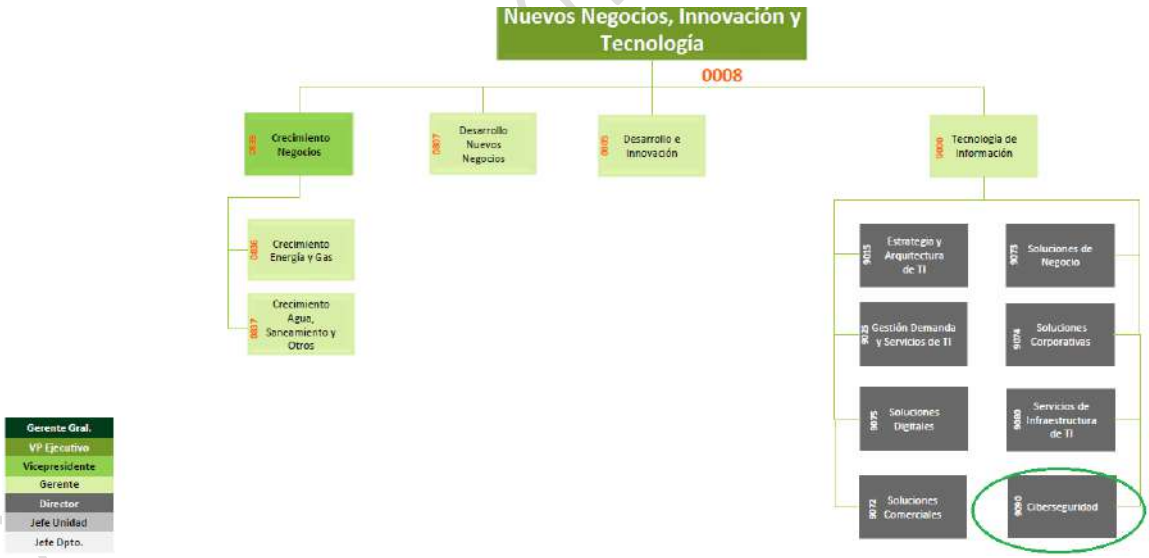
El sistema de gestión de seguridad de la información y ciberseguridad está orientado a mitigar el riesgo 14 - Ataques Cibernéticos: "Vulnerabilidades en los Sistemas de Información y de los Sistemas de Supervisión y Control de Infraestructuras Criticas que permiten ataques con afectación en la prestación de los servicios o en los activos de información del Grupo EPM", cuya atención ha sido priorizada por la Junta Directiva del Grupo EPM, el cual está enfocado principalmente en:

- Velar por la continuidad de las operaciones de los negocios y la optimización de los sistemas de información con seguridad.
- Que los servicios y la información del Grupo EPM a nivel nacional e internacional se brinden de manera segura a sus grupos de interés, minimizando los riesgos que afecten su reputación, su imagen, sus finanzas y la continuidad en los servicios e información que ofrece.

3. LIDERAZGO

3.1. Liderazgo y compromiso

Alta Dirección



La Dirección Ciberseguridad adscrita a la Gerencia de Tecnología e Información de la Vicepresidencia Nuevos Negocios, Innovación y Tecnología está a cargo del Sistema de Gestión de Seguridad de la información y ciberseguridad. Acorde con la estructura organizacional, se identifica como la alta dirección del SGSI y Ciberseguridad a la Vicepresidencia Nuevos Negocios, Innovación y Tecnología y a la Gerencia de Tecnología e Información.

3.2. Política

Marco normativo Grupo EPM

El marco normativo del Grupo EPM orienta el actuar de la organización, partiendo de unas políticas y lineamientos ubicados en los niveles estratégicos y tácticos, para llegar a unas reglas de negocio y procedimientos que se ubican en el nivel operativo, tal como se muestra en el siguiente gráfico:

La política y lineamientos de seguridad de la información y ciberseguridad son con alcance de Grupo EPM y las reglas de negocio se definen en cada filial.

Política de Seguridad de la Información y Ciberseguridad

"El Grupo EPM se compromete en proteger la información, los activos críticos y ciberactivos críticos que posee, con el fin de contar con información íntegra, completa y con los niveles de confidencialidad requeridos para la toma de decisiones, la operación segura y la respuesta oportuna a incidentes o ataques sobre sus activos y ciberactivos, de forma que se garantice la continuidad en la prestación de los servicios".

La política fue aprobada mediante el acta 1619 de Junta Directiva del 13 de diciembre de 2016. Las políticas organizacionales pueden ser consultadas en la página web de EPM: https://www.epm.com.co/site/home/institucional/politicas

Lineamientos Seguridad de la Información y Ciberseguridad

Para desplegar la política se definieron los siguientes lineamientos:

- ***Protección de información, activos críticos y ciberactivos****: "la información, los activos críticos y ciberactivos objeto de protección, deben ser valorados mediante las metodologías definidas en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, e implementar los controles necesarios para realizar una operación segura y confiable y contar con información integra y completa, con los niveles de confidencialidad requeridos para la toma de decisiones."*
- ***Mantenimiento del inventario de activos críticos y ciberactivos****: "Las dependencias responsables por la administración, operación y mantenimiento de los activos críticos y ciberactivos, deben mantener actualizado el inventario de éstos, a través de las metodologías definidas en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad."*

- ***Respuesta oportuna a incidentes o ataques****: "Las dependencias responsables por gestionar los incidentes de seguridad y ciberataques, deben monitorear permanentemente, con el fin de detectar y anticiparse a la ocurrencia de los mismos (ciberinteligencia). Frente a la ocurrencia del incidente o ataque, se debe realizar con celeridad la contención, erradicación y las operaciones de respuesta, defensa y recuperación (ciberdefensa) a las que haya lugar, involucrando a los actores internos y externos que sean requeridos."*
- ***Continuidad del negocio y resiliencia****: "La Empresa implementa mecanismos de prevención, atención y recuperación en la gestión de Seguridad de la Información y Ciberseguridad, con el fin garantizar la continuidad en la prestación de los servicios en el nivel predefinido como aceptable, después de un incidente de seguridad o ciberataque. Dichos mecanismos propenden por aumentar la capacidad de adaptación y respuesta de la Empresa, de manera oportuna, salvaguardando los intereses propios y de los grupos de interés, mitigando los efectos sobre los objetivos estratégicos de la organización."*
- ***Competencia y concienciación****: "La Empresa debe desarrollar estrategias de sensibilización, capacitación y entrenamiento permanente para los empleados y contratistas, con el objetivo de crear conciencia sobre la necesidad de proteger el conocimiento y los datos de la empresa y para que en sus actuaciones no afecten el desempeño de la seguridad de la información y la ciberseguridad."*

Los lineamientos de seguridad de la información y ciberseguridad pueden ser consultados en la ruta. https://enter2.epm.com.co/gd-aa/ActosAdministrativos/DTL_PUB_LINGG/LINEAMIENTO%20GERENCIA%20GENERAL-2017-LINGG-20.pdf

Reglas de negocio del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología

La regla de negocio es una disposición mediante al cual se fijan o describen los parámetros de las actividades o tareas que integran un proceso y la forma como el personal responsable debe cumplir con estas. Para el caso del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, las reglas de negocio corresponden a las definidas por el proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología.

En las reglas de negocio del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología se abordan las siguientes temáticas:

- Responsabilidad Compartida
- Perímetro de Seguridad Electrónica
- Identificación y documentación de los sistemas bajo consideración
- Análisis de amenazas, vulnerabilidades y controles de seguridad digital
- Declaración de Aplicabilidad de Controles de Seguridad
- Planes de tratamiento de riesgos de seguridad digital
- Gestión de vulnerabilidades en los activos y ciberactivos
- Requisitos regulatorios relacionados con seguridad de la información y ciberseguridad
- Seguridad de la información y ciberseguridad en la cadena de suministro de tecnología e información
- Adquisición de nueva tecnología
- Segregación de funciones
- Gestión de acceso de usuarios

- Evaluación de personal con acceso a ciberactivos críticos
- Uso de información secreta para la autenticación
- Uso de cuentas técnicas de sistemas
- Cuentas de usuario compartidas
- Cuentas predeterminadas
- Procedimiento de autenticación
- Firma electrónica
- Restricciones de acceso a Información y funcionalidad de los sistemas de información
- Información de activos críticos y ciberactivos
- Uso de programas de software utilitario privilegiado
- Gestión de derechos de acceso privilegiado
- Controles de acceso lógico y físico
- Acceso de contratistas o proveedores a información organizacional
- Toma de conciencia, educación y formación
- Protección de los datos personales
- Protección de la información clasificada y reservada
- Pruebas de aceptación del sistema
- Pruebas de aceptación de Tecnologías de Operación
- Desarrollo contratado externamente
- Transferencia de información
- Ambientes de desarrollo, pruebas y producción
- Control de los datos de prueba
- Uso de controles criptográficos
- Ciberseguridad en diseño e ingeniería tecnología de operación
- Líneas base de seguridad
- Desarrollo seguro
- Control de cambios
- Gestión de la configuración
- Respaldo de la información
- Restricciones sobre la instalación de software
- Disposición de Medios
- Devolución de los activos de información y ciberactivos
- Conexiones temporales a sistemas de control y monitoreo
- Registros de auditoría
- Gestión de medios removibles
- Dispositivos móviles
- Monitoreo de infraestructura
- Revisión del cumplimiento técnico
- Herramientas de prevención de software Malicioso (malware)
- Software autorizado
- Cooperación y colaboración
- Reporte de eventos de seguridad de la información
- Planes de contingencia y recuperación de TI /TO
- Análisis de Impacto de tecnología
- Estrategia de recuperación tecnológica

3.3. Roles, responsabilidades y autoridades en la organización

Líneas de defensa del control

La responsabilidad por la seguridad de la información es una "Responsabilidad Compartida", acorde con lo establecido por la organización en las líneas de defensa del control, como se describe a continuación:

- Línea estratégica: la alta Dirección del SGSI y Ciberseguridad y el Comité de Gerencia de EPM tienen a su cargo definir la estrategia y directrices en temas de seguridad digital de Tecnología de Información, Tecnología de Operación y Tecnología del Cliente (TI,TO Y TC).
- 1 línea de defensa - Autocontrol: en esta línea de defensa están todos los empleados de la organización quienes tienen la responsabilidad de asegurar la gestión del riesgo mediante la ejecución efectiva de los controles de seguridad de la información y ciberseguridad que le apliquen al proceso al cual pertenecen. En esta línea de defensa está la responsabilidad por la implementación y monitoreo de los controles de seguridad de la información y ciberseguridad, asignada a los responsables de procesos y proyectos.
- 2 línea de defensa -Autoevaluación: esta línea de defensa está a cargo de asegurar que los controles de seguridad de la información y ciberseguridad estén diseñados y operen de manera efectiva. La segunda línea de defensa está a cargo de la Dirección Ciberseguridad.
- 3. Línea de Defensa: Conformada por la Vicepresidencia Auditoría Corporativa, Gerente Auditoría Negocios, Gerente Auditoria Proyectos y Suministros y Gerente Auditoría Soporte. Este nivel proporciona aseguramiento independiente sobre la eficacia de la gestión de riesgos y control interno.

Dirección Ciberseguridad

La Dirección Ciberseguridad tiene como función básica definir y dirigir el despliegue y el control de la estrategia de seguridad digital con el fin de prevenir riesgos y proteger la infraestructura, los activos digitales y la información críticos, para mantener una operación sostenible y segura en EPM.

Sus funciones principales son:

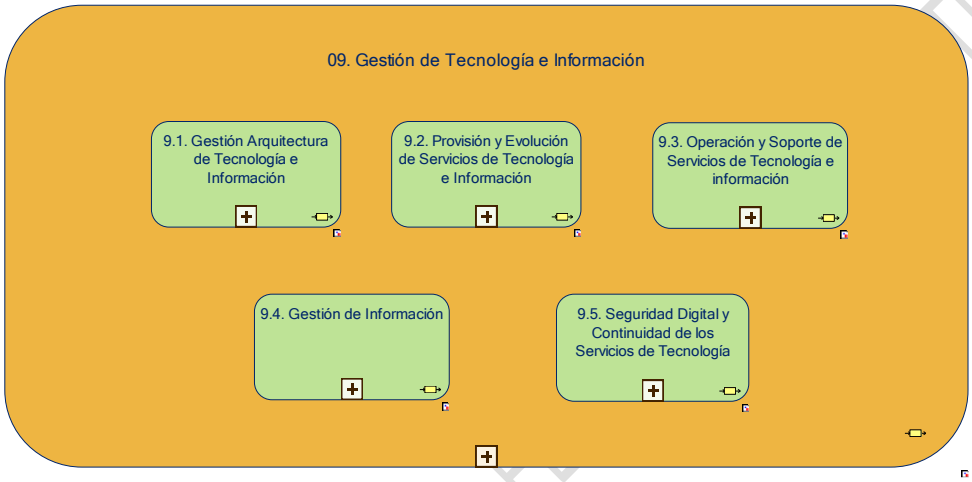
- Liderar la definición de prácticas y metodologías de seguridad digital, socializarlas y someterlas a aprobación.
- Dirigir el SGSI y Ciberseguridad para EPM.
- Definir y coordinar la implantación de la arquitectura de seguridad digital para EPM.
- Dirigir la definición, seguimiento y actualización de los planes y marco normativo de la seguridad digital según el direccionamiento estratégico.
- Dirigir la propuesta y socialización de los asuntos críticos de seguridad de la información y ciberseguridad.
- Orientar la definición y actualización del mapa de riesgos y controles de seguridad digital en las TI, TO y TC y coordinar la elaboración y ejecución de plan de tratamiento.
- Dirigir la identificación y recomendaciones para la adopción de soluciones de seguridad digital que se requieran en EPM.
- Liderar el seguimiento a los costos y riesgos asociados a la evolución y sostenimiento del SGSI y Ciberseguridad en EPM.
- Orientar el análisis de amenazas y vulnerabilidades de la seguridad digital en los procesos y proyectos del Grupo EPM.
- Coordinar el análisis y resolución de incidentes de seguridad digital.
- Liderar el diseño y ejecución de las diferentes estrategias de asimilación que eleven la conciencia situacional en lo que respecta a la seguridad digital en la organización.

4. PLANIFICACIÓN

4.1. Acciones para tratar riesgos y oportunidades

Proceso Seguridad Digital y Continuidad de los Servicios de Tecnología

Para implementar y operar la seguridad de la información y la ciberseguridad, se definió el proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología que hace parte del macroproceso Gestión de Tecnología e Información.



Objetivo del proceso:
Implementar los controles de seguridad requeridos para mitigar los riesgos de ataques cibernéticos y proteger los activos organizacionales como: Información crítica, activos críticos de operación y ciberactivos del Grupo EPM.

Alcance del proceso:
Inicia con la Identificación de los requisitos de seguridad de la información y ciberseguridad que deben ser implementados por la organización en los activos de información y ciberactivos y finaliza con la implementación de estrategias que apoyen la mejora de la capacidad de resiliencia organizacional, frente a los riesgos que afecten la seguridad digital. Comprende: la integración e interacción de la seguridad de TO, seguridad de TI, seguridad física y la seguridad en IoT.

Actividades del proceso:

- ***Gestión Seguridad Digital***: Implementar los controles de seguridad requerido para mitigar los riesgos de ataques cibernéticos y proteger los activos organizacionales como: Información crítica, activos críticos de operación y ciberactivos del Grupo EPM. De esta actividad se desprenden las siguientes tareas:
  - Identificar necesidades de seguridad digital.
  - Proteger los activos y ciberactivos críticos
  - Detectar anomalías internas y externas.
  - Responder incidentes de seguridad digital
  - Recuperar activos y ciberactivos

- ***Continuidad de los Servicios de TI***: Desarrollar, implementar y mantener estrategias de continuidad para los servicios de TI, en línea con los acuerdos de niveles de servicios pactados con el cliente (Negocio). De esta actividad se desprenden las siguientes tareas:

- Analizar el impacto del servicio de TI
- Formular estrategias de continuidad del servicio de TI
- Gestionar plan de recuperación de TI (DRP).
- Realizar pruebas y ejercicios y simulaciones del DRP.

La caracterización del proceso de Seguridad Digital y Continuidad de los Servicios de Tecnología puede ser consultada en https://megahopex.epm.com.co/pages/85578a515bab0bd1.htm

Centro de Operaciones de Ciberseguridad SOC

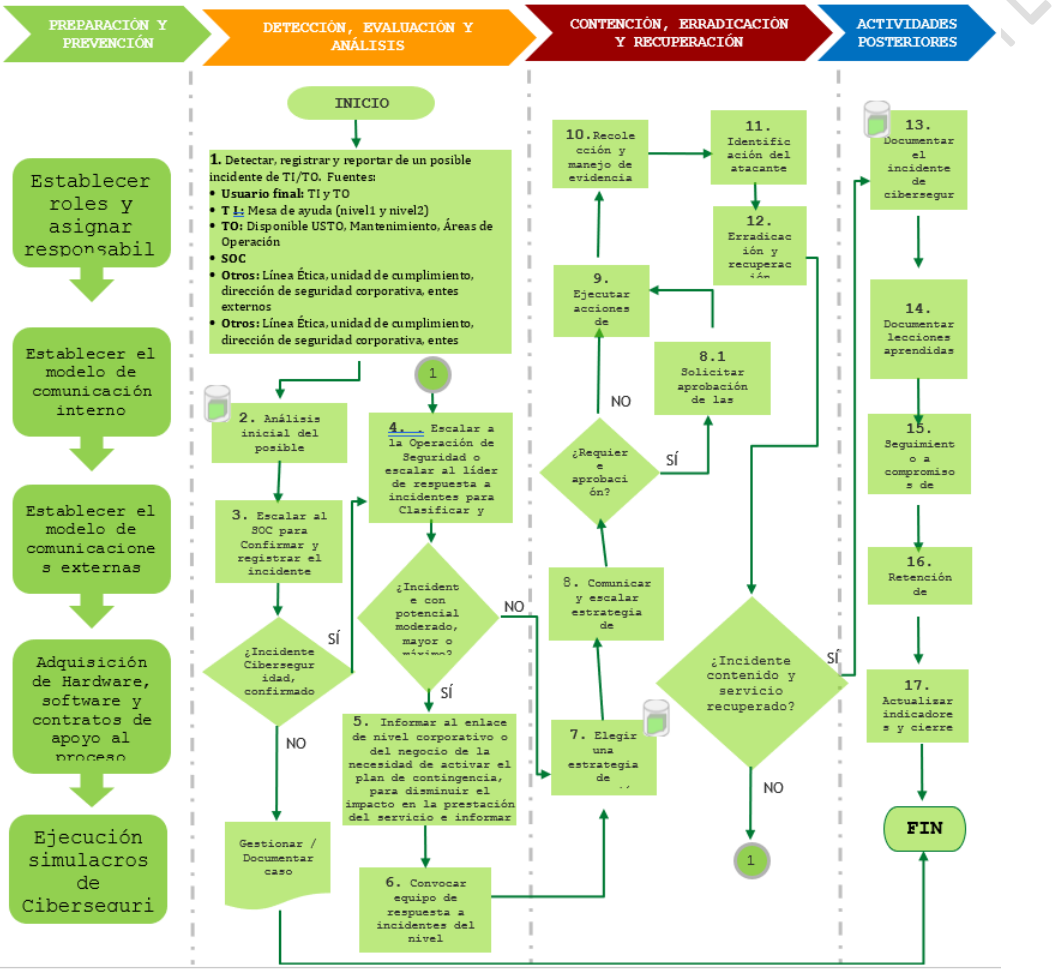
En EPM se cuenta con un Centro de Operaciones de Ciberseguridad, en sus siglas en inglés; Security Operation Center (SOC) es un servicio que se presta de forma transversal a la organización con alcance a las tecnologías de operación (TO) y tecnologías de información (TI) está conformado por personal especializado en ciberseguridad, procesos, tecnología y concienciación, en modalidad 7×24, la prestación del servicio tiene la capacidad de predecir, detectar, analizar, responder y recuperar ante amenazas, ataques cibernéticos e incidentes de Ciberseguridad.

El centro de operaciones de ciberseguridad presta servicios relacionados con:

- La monitorización y análisis de la actividad que se genera en los activos de la empresa, es decir en la infraestructura hardware y software (firewall, IPS, IDS, proxys, redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web empresariales, dominios, usuarios, cuentas, redes sociales, otros activos y ciberactivos) todo este ecosistema requiere un monitoreo constante, en busca de actividades anómalas que puedan ser indicativas de un posible incidente o compromiso de seguridad.
- Gestión de vulnerabilidades.
- Analítica avanzada de red.
- Inteligencia de amenazas cibernéticas (CTI).
- Orquestación de seguridad, automatización y respuesta (SOAR)
- Análisis de comportamiento de usuarios y entidades (UEBA)
- Tecnología de engaño (DT).
- Cacería de amenazas (Threat Hunting)

Los servicios que presta el SOC tienen un enfoque basado en fuentes de datos integradas que permiten analizar el ecosistema y la superficie de ataques, de manera interna y externa, a través de herramientas que monitorean, analizan y automatizan el comportamiento de la data, de acuerdo con los hallazgos y eventos detectados, permiten identificar y prevenir a tiempo, tomar acciones de mitigación, implementar controles y adelantarnos de forma proactiva a los incidentes de ciberseguridad.

Gestión de Incidentes de Seguridad de la Información



El procedimiento de gestión de incidentes de seguridad de la información establece las directrices y procedimientos generales para la gestión de incidentes de seguridad de la información y ciberseguridad en el Grupo Empresarial EPM, con el fin de prevenir y mitigar el impacto de los mismos en la organización, conforme a lo establecido en la norma ISO 27001:2013 “Sistemas de Gestión de Seguridad de la Información” e ISO 27002:2013 “Código de buenas prácticas para la gestión de seguridad de la información” y NIST SP 800-61 Rev 2.

4.2. Objetivos de la Seguridad de la Información y planes para lograrlos

Objetivo General

"Fortalecer la capacidad de ciberseguridad y la resiliencia del Grupo EPM, logrando tener una operación sostenible de los negocios actuales y los servicios del futuro, de manera segura, protegiendo la infraestructura y la información críticas y la prestación de los servicios dentro de los niveles de riesgo aceptables."

Para el logro del objetivo general, se han venido adelantando acciones asociadas a cada uno de los objetivos específicos del sistema, las cuales se describen a continuación:

Proteger las infraestructuras Tecnológicas críticas e información crítica de EPM

- Identificar activos críticos
- Asegurar las infraestructuras e información de los negocios y de las tecnologías de Información.
- Gestionar las vulnerabilidades.
- Servicios de Operaciones de Seguridad.

Gestionar adecuadamente los incidentes y las crisis

- Prepararnos proactivamente para minimizar el impacto en los incidentes.
- Atender los incidentes en el menor tiempo posible.
- Mejorar la recuperación y resiliencia de los servicios críticos y servicios impactados.

Concienciación en las personas

- Formación y capacitación
- Concienciación.
- Simulacros y simulaciones.
- Juegos de guerra.

Asegurar negocios (actuales y futuros) y productos digitales

- Arquitectura de Ciberseguridad desde el diseño.
- Seguridad en ciclo de desarrollo en aplicaciones
- Pruebas de Ethical Hacking e intrusión.
- Identificación de nuevas tecnologías de Ciberseguridad.
- Inteligencia de amenazas

Gestión proactiva del riesgo, gobierno y cumplimiento normativo

- Análisis de riesgos en los negocios.
- Análisis de riesgos en las Tecnologías de Información.
- Análisis de riesgos en procesos críticos.
- Aseguramiento de requisitos regulatorios.
- Implementación de mejores prácticas en Ciberseguridad.

El plan de trabajo de la Dirección Ciberseguridad apunta al cumplimiento de los objetivos del SGSI y Ciberseguridad.

5. SOPORTE

5.1. Recursos

El Sistema de Gestión de Seguridad de la Información y Ciberseguridad, cuenta con un presupuesto formal en la organización, el cual puede ser consultado en el plan de acción de la organización en la dirección: https://www.epm.com.co/site/home/transparencia/transparencia-y-acceso-a-informacion-publica#6-Metas-e-indicadores-5320

5.2. Competencia

EPM cuenta con el manual de cargos que incluye el perfil basado en educación, conocimiento, experiencia y actuaciones**.** EPM desarrolla, fortalece y hace seguimiento a las actuaciones (comportamientos que dan cuenta de la presencia de los rasgos culturales del grupo EPM declarados para habilitar su direccionamiento estratégico), para contribuir de manera integral al logro de los objetivos empresariales, a la vez que, en equilibrio, aporta al crecimiento integral de las personas.

En lo relacionado con la seguridad de la información y ciberseguridad, se cuenta con un mapa de conocimiento para apalancar el desarrollo de competencias del personal. A continuación, se resumen las áreas de conocimiento y los conocimientos identificados relacionados que debe adquirir el personal:

Área de Conocimiento	Conocimiento
Gestión de Seguridad Digital	"• Marcos normativos internos y externos en seguridad digital. • Marcos de referencia de seguridad digital (Frameworks) • Modelo de arquitectura empresarial (Estrategia, gobierno, procesos, tecnología) • Sistemas de gestión de seguridad digital. • Practicas de Gobierno de seguridad de la información y ciberseguridad. • Diseño de métricas."
Arquitectura de Seguridad Digital	"• Marcos de referencia en arquitecturas de seguridad digital (Frameworks) • Modelo de arquitectura empresarial. • Modelamiento de las arquitecturas y herramientas. • Modelos de referencia de industrias. • Arquitecturas de referencias de los dominios tecnológicos. • Estándares tecnológicos del mercado y de EPM. • Plataformas tecnológicas de EPM. • Metodologías de experimentación y pruebas. • Arquitecturas para ciberseguridad en plataformas cloud."
Conciencia Situacional	"• Juegos de guerra (Ejercicios, simulaciones, pruebas de ciberataques) • Diseño de estrategias de sensibilización, capacitación y entrenamiento en SD."
Respuesta a Incidentes de Seguridad Digital, Ciberdefensa y Ciberinteligencia	"• Procedimientos en respuesta a incidentes (Preparación, prevención, detección, evaluación, contención, erradicación y recuperación) • Respuesta a incidentes. • Simulacros de incidentes de seguridad digital. • Pruebas de penetración. • Monitoreo y correlación de eventos. • Analítica avanzada. • Ciberinteligencia externa (Vigilancia) • Gestión de vulnerabilidades. • Análisis forense."

Área de Conocimiento	Conocimiento
Gestión de Identidad y gestión de accesos	"• Mecanismos de identidad, autorización y autenticación. • Segregación de funciones y definición de perfiles (Asignación de privilegios) • Mecanismos de aprovisionamiento y desaprovisionamiento de usuarios. • Gestión de cuentas privilegiadas. • Integración con aplicaciones en nube e identidades sociales. • Gestión de cuentas de usuario."
Gestión de Riesgos y Controles	"• Metodologías de riesgos y controles. • Análisis de amenazas y vulnerabilidades. • Diseño y evaluación de controles. • Planes de tratamiento."
Gestión de la Continuidad de los Servicios de Tecnologia	"• Marcos de referencia en continuidad del negocio (Frameworks) • Análisis de impacto del negocio (BIA) • Análisis de impacto en las aplicaciones (AIA) • Definición de estrategias de continuidad. • Gestión del Plan de recuperación de Tecnología (DRP) • Pruebas, ejercicios y simulaciones (DRP)"
Redes, infraestructura y aplicaciones	"• Seguridad en Redes y comunicaciones. • Seguridad en Sistema operativo (servidores y bases de datos) • Practicas de Desarrollo seguro de aplicaciones. • Encriptación y enmascaramiento de datos • Practicas para protección de Endpoint"

5.3. Toma de conciencia

Se cuenta con un plan de concienciación y comunicación 2019 – 2023, que se toma como referencia para la planeación anual.

En el proceso de inducción corporativa se incorporó una sesión de ciberseguridad para las personas que ingresan nuevas a la empresa. Adicionalmente, para comunicar a la organización temas relacionados con seguridad de la información y ciberseguridad, se cuenta con un micrositio en: https://mibitacora.epm.com.co/areas/gti/seg/Paginas/HomeMiBitacora.aspx

5.4. Comunicación

En la “matriz de impactos y públicos involucrados” se identifican las necesidades de comunicación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

5.5. Información documentada

Los documentos que soportan el SGSI están almacenados en la ruta electrónica https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx

Para la gestión de la documentación se cuenta con el Manual para la producción y control de documentos y registros en EPM, Instructivo para la producción y control de documentos y la Guía de usuario para la producción y control de documentos y procesos de gestión en ENTER.

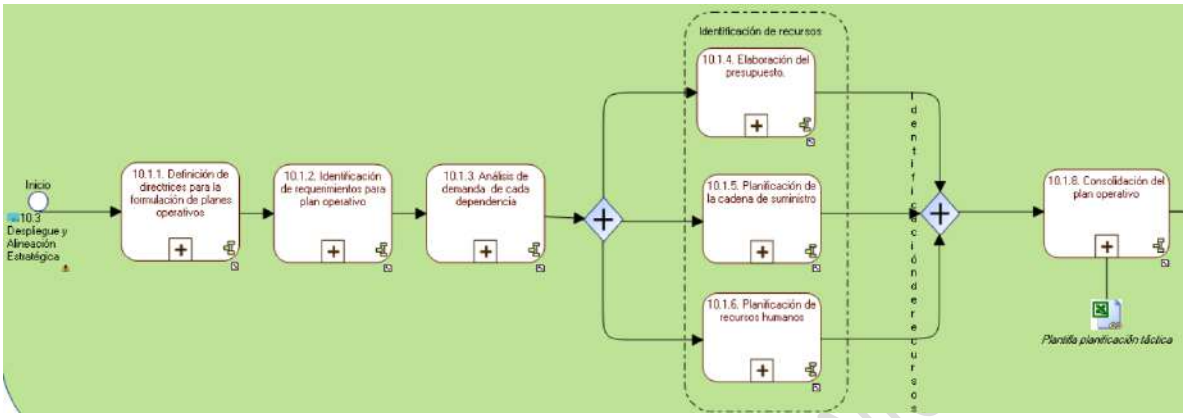
El sistema cuenta con un listado maestro de documentos que puede ser consultado en: *https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx?RootFolder=%2Fsite%2FSIG%2FDVG%2FDTL%5FISO%5F27001%2FDocumentos%20de%20referencia&FolderCTID=0x0120009F6CB89B3665904FAE752A7FFB1AF40F&View=%7BFECE6DF8%2D5028%2D4815%2D9EC2%2D062FA33DEDAE%7D*

Adicionalmente se cuenta con el instructivo “Edición y control de la información documentada” que tiene como propósito: Establecer los pasos para crear, actualizar y controlar la información documentada (documentos y registros) de origen interno y externo, que soportan el Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

Está en proceso de construcción de la tabla de retención documental de la Dirección Ciberseguridad.

6. OPERACIÓN

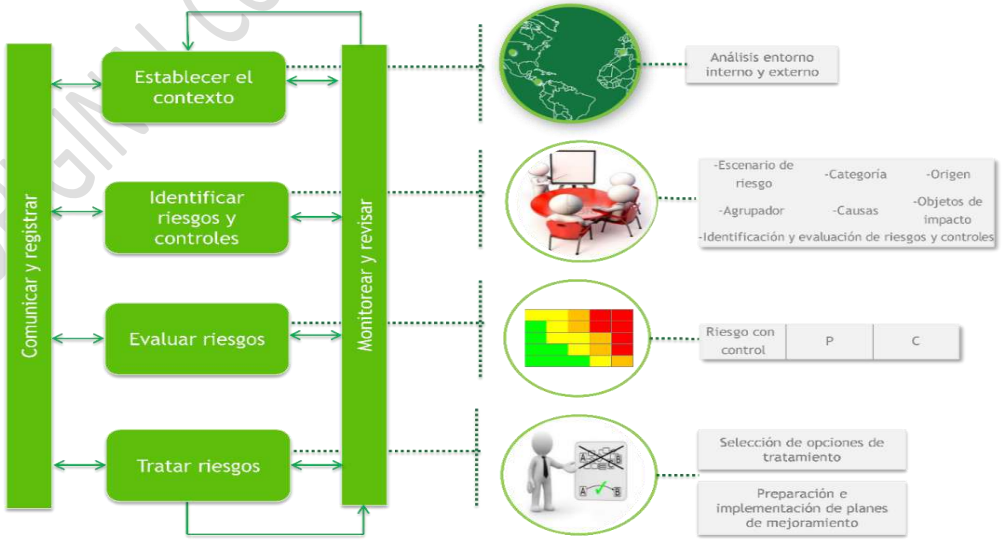
6.1. Planificación y Control Operacional



EPM cuenta con un proceso de planificación operativa que puede ser consultado en detalle en https://megahopex.epm.com.co/pages/f112f23256de53e5.htm

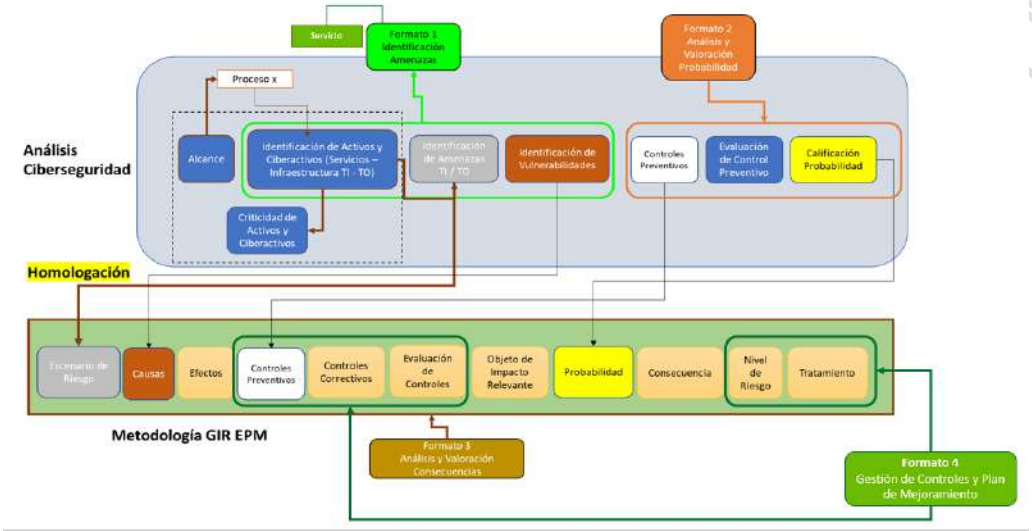
El proceso de planificación operativa de EPM tiene como objetivo planear de forma detallada en cada dependencia de la organización: las funciones, los procesos y sus mejoras, los proyectos priorizados, las acciones necesarias para atender mandatos normativos, regulatorios y/o administrativos, asignando los recursos humanos, técnicos y financieros e identificando las necesidades de contratación requeridos para la adecuada ejecución del Plan Operativo. El proceso inicia con la entrega de orientaciones para la elaboración de los planes operativos y demás entregables (presupuesto, plan de contratación, plan de TI, planeación del talento humano, entre otros) clave del proceso y termina con la divulgación de los planes operativos para su ejecución.

6.2. Valoración de riesgos de seguridad de la información y ciberseguridad



En EPM la gestión integral de Riesgos se lleva a nivel corporativo, con el fin de soportar la toma de decisiones, generar confianza frente a los grupos de interés, facilitar el cumplimiento de los objetivos de la organización y el desarrollo de las capacidades organizacionales. La Gestión de Riesgos en EPM se da por medio de la Dirección Ingeniería de Riesgos, quien, con base en la Guía Metodológica para la Gestión Integral de Riesgos, se apoya para la implementación. En términos generales, la gestión de los riesgos se lleva a cabo como se ilustra en la siguiente gráfica:

Metodología para el análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos.



Los procesos y proyectos que manejen tecnología de información y operación aplican la metodología de análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos a su cargo, para identificar el nivel de riesgo y las oportunidades de mejora. Esta metodología está documentada en el "Instructivo para el análisis de amenazas, vulnerabilidades y controles de seguridad digital en los activos y ciberactivos" que puede ser consultado en:

https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Forms/AllItems.aspx?RootFolder=%2Fsite%2FSIG%2FDVG%2FDTL%5FISO%5F27001%2FInstructivos&FolderCTID=0x0120009F6CB89B3665904FAE752A7FFB1AF40F&View=%7BFECE6DF8%2D5028%2D4815%2D9EC2%2D062FA33DEDAE%7D

6.3. Tratamiento de los riesgos de seguridad de la información y ciberseguridad.

Como parte de los análisis de riesgos se evalúa el estado de los controles y se formula un plan de tratamiento de riesgos. Los planes de tratamiento de riesgos están a cargo de los responsables de los procesos o proyectos donde se realiza la evaluación del riesgo.

7. EVALUACIÓN DEL DESEMPEÑO

7.1. Seguimiento, medición, análisis y evaluación

El proceso “Seguimiento y mejora a la gestión” que hace parte del Macroproceso evaluación y mejoramiento, permite gestionar la evaluación y mejora del desempeño empresarial, en el marco de las dimensiones de la Arquitectura Empresarial, para incrementar la eficiencia y eficacia en el logro de los objetivos estratégicos.

Indicadores de gestión

Se cuenta con indicadores de gestión que permiten medir el logro de los objetivos, estos indicadores se describen a continuación:

- La relación inversión Seguridad Digital Vs Inversión tecnología permite establecer la tendencia del presupuesto de seguridad digital para poder determinar la pertinencia de cambios, adiciones u optimización de costos e inversiones.
- El nivel de cubrimiento de Monitoreo de la plataforma tecnológica permite medir la gestión proactiva y correlación de eventos con el fin de anticipar y prevenir ataques cibernéticos antes que se materialicen.
- El indicador de pruebas de recuperación de las aplicaciones en el CAP permite medir el cumplimiento de pruebas de recuperación de los aplicativos alojados en el CAP (Centro Alterno de Procesamiento de Datos - Bogotá).
- Los indicadores de atención del incidente MTTR y detección del evento MTTD permiten medir la oportunidad en la atención de incidentes garantizando la continuidad del servicio.
- Los indicadores generación de conciencia situacional y ejercicio phishing – usuarios que dieron clic, permiten conocer el avance que va adquiriendo la organización frente al nivel de conciencia, sobre los riesgos de seguridad digital, desarrollado por los empleados.

Medición del nivel de madurez seguridad de la información tomando como referente herramienta Mintic basada en NTC-ISO-IEC 27001

Con el diligenciamiento de la herramienta de autoevaluación de la seguridad de la información proporcionada con el MINTIC, se ha realizado seguimiento a la implementación de los controles de la 27001 y al nivel de madurez de la seguridad de la información en la organización.

En esta evaluación se puede observar el grado de avance en la implementación de los dominios de seguridad de la información.

Medición de la madurez de la capacidad de la ciberseguridad como referente C2M2

Se realiza medición de la capacidad de ciberseguridad basado en modelo de madurez de la capacidad de ciberseguridad (C2M2)

7.2. Auditoría Interna

En EPM a través del proceso verificación independiente se realizan auditorías internas de control que tienen como propósito proporcionar asesoría y aseguramiento objetivo e independiente sobre la eficacia y eficiencia de los procesos de gobierno, gestión de riesgos y control interno, generando confianza a los grupos de interés.

Además, la auditoría interna al SGC se efectúa según lo definido en la "Guía de auditorías internas de sistemas de gestión", en la que se describen las acciones para la programación, planificación, ejecución y evaluación de las auditorías internas combinadas que determinan tanto el estado del SGC, según NTCGP 1000, como de los demás Sistemas de Gestión certificados y acreditados en los diferentes referentes adoptados por la organización.

7.3. Revisión por la dirección

Anualmente la alta Dirección realiza revisión al SGSI y Ciberseguridad donde se abordan temas como:

- Cumplimiento de los objetivos del sistema de gestión
- Procesos impactados por el sistema de gestión
- Resultados de los indicadores de gestión
- Resultados de las auditorías
- Estado de los planes de mejoramiento
- Retroalimentación de las partes interesadas
- Cumplimiento de acciones de revisión anterior
- Cambios que podrían impactar el sistema de gestión
- Riesgo cibernético – gestión de incidentes
- Propuesta para la mejora del sistema de gestión
- Conclusiones sobre la conveniencia, adecuación, eficacia, eficiencia y efectividad del sistema de gestión.

La revisión por la dirección se hace teniendo en cuenta la "*Guía Metodológica para la Revisión por la Dirección de Sistemas de Gestión".*

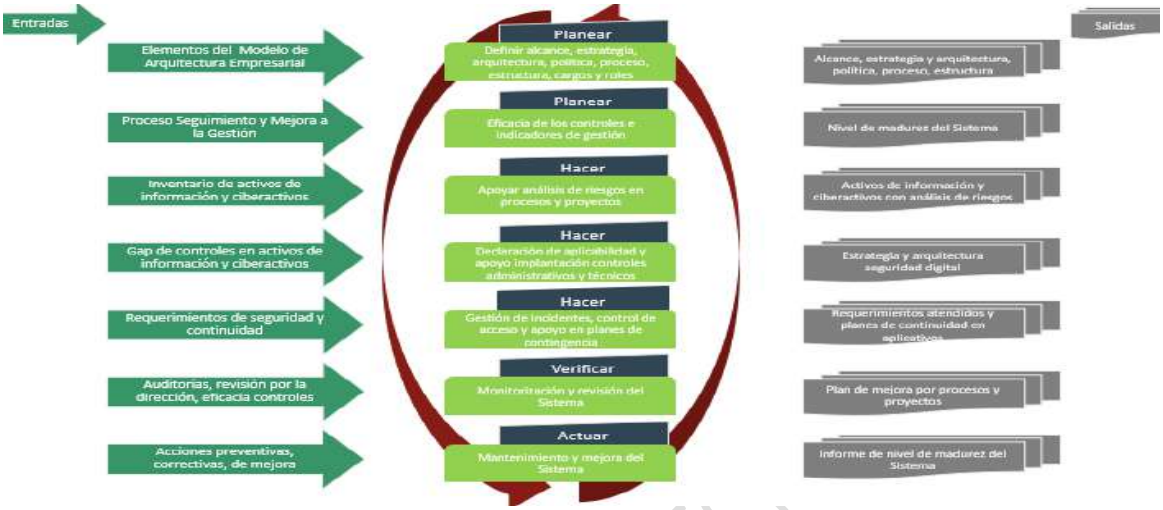
8. MEJORA

8.1. No conformidades y acciones correctivas

Se entiende por una no conformidad el incumplimiento de un requisito del Sistema de Gestión de Seguridad de la Información y ciberseguridad, tomando como referencia la norma ISO IEC 27001. Para atender las no conformidades encontradas dentro del sistema de gestión, se debe definir un plan de mejoramiento que contenga las acciones correctivas que permitan cerrar la brecha (subsanar) y así cumplir con los requisitos establecidos por el sistema.

8.2. Mejora Continua

La mejora continua del Sistema de Gestión de Seguridad de la Información y Ciberseguridad está basada en el ciclo PHVA, en cada una de las etapas del ciclo.



La mejora del SGSI y Ciberseguridad, se apalanca igualmente en los resultados de las evaluaciones internas y externas realizadas por la Auditoría, así como las revisiones por la dirección, los análisis de amenazas, vulnerabilidades y controles de seguridad digital, así como la gestión de la vulnerabilidad técnica. Se definen acciones correctivas, preventivas y de mejora que buscan eliminar las causas de las no conformidades reales y potenciales, con su respectivo seguimiento, según lo indicado en la “Guía metodológica para la gestión de planes de mejoramiento”.

Actualmente, la empresa cuenta con el sistema de información Avanza a través del cual se hace la formulación y seguimiento de los planes de mejoramiento definidos en cada uno de los niveles de gestión del Grupo Empresarial.

9. DOCUMENTOS DE REFERENCIA

CNO. (2019). *Guía de ciberseguridad*.

CONPES. (2016). *Política Nacional de Seguridad Digital*. 91. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ�micos/3854.pdf

Departamento de Seguridad Nacional de España. (2013). *Estrategia de Ciberseguridad Española 2013*. Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

EPM. (2016). *GUÍA METODOLOGÍCA PARA LA GESTIÓN INTEGRAL DE* RIESGOS

ICONTEC, I. (2017). *COLOMBIANA NTC-ISO / IEC 27000*. (571).

Técnica, N., Riesgo, G. D. E. L., & Directrices, P. Y. (2011). Norma Tecnica NTC/ISO/IEC 27000.