

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

	<b>NOMBRE</b>	<b>CARGO</b>	<b>FIRMA</b>
<b>ELABORÓ</b>	Ana María Espinosa Ángel	Directora Administrativa y Financiera	
	Heidy Yohanna Jimenez Rodriguez	Coordinadora de Servicios Administrativos	
<b>REVISÓ</b>	Lina Victoria Hoyos Jaramillo	Directora Ejecutiva	
	Juan Esteban Hoyos Acosta	Jefe de asuntos legales y Secretaria General	
<b>APROBÓ</b>	Monica Julieta Pinzón Bueno (*)	Presidente Consejo Directivo	

(\*) Política aprobada en sesión ordinaria N 306 del Consejo Directivo de la Fundación EPM el 27 de noviembre de 2024

### **CONTROL DE CAMBIOS**

<b>Versión</b>	<b>Fecha de Aprobación</b>	<b>Descripción del Cambio (Qué y Por qué)</b>
01	27/11/2024	Versión original

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

## 1. Contenido

1. CONSIDERACIONES.....	4
2. LINEAMIENTO .....	5
Protección de la información, activos críticos y ciberactivos.....	5
Firma Electrónica y firma Digital.....	5
Mantenimiento del inventario de activos críticos y ciber activos.....	5
Respuesta oportuna a incidentes o ataques .....	5
Continuidad del negocio y resiliencia .....	6
Competencia y concienciación.....	6
3. VIGENCIA Y DEROGATORIAS.....	6
4. ANEXOS .....	7

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

La Fundación EPM adapta la **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA EL GRUPO EPM** y sus lineamientos buscando optimizar y transformar sus operaciones desde una perspectiva de seguridad digital. La política del Núcleo Grupo EPM fue aprobada por la Junta Directiva de EPM en el acta 1604 del 15 de diciembre de 2015.

Las adaptaciones a esta política se refieren a:

- Integra también los lineamientos que se desprenden de esta política.
- Se estableció como una política corporativa según la normatividad interna de la Fundación.
- Se incluye la definición de firma certificada a sus lineamientos

### Política de seguridad de la información y ciberseguridad para el Grupo EPM

El Grupo EPM se compromete en proteger la información, los activos críticos y ciberactivos 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 críticos y ciberactivos, de forma que se garantice la continuidad en la prestación de los servicios. Esto lo realiza mediante la Arquitectura TI mayormente de EPM y otros terceros.

Área responsable en el acta: VP Desarrollo humano y Capacidades Organizacionales. Aprobada acta 1619 de Junta Directiva 13/12/2016

LINEAMIENTO 2023-LINGG-115

LINEAMIENTO PROCESO SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍA

EL GERENTE GENERAL de EMPRESAS PÚBLICAS DE MEDELLÍN E.S.P. en adelante EPM, en uso de sus facultades legales y estatutarias, y teniendo en cuenta las consideraciones que a continuación se exponen, expide el Lineamiento sobre Seguridad Digital y Continuidad de los Servicios de Tecnología:

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

## 1. CONSIDERACIONES

El numeral 8 del Artículo 2 de la Ley 1341 de 2009, señala que conforme al principio orientador de “Masificación del Gobierno en Línea” hoy Gobierno Digital, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

El Artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, dispone que la Política de Gobierno Digital se compone de varios elementos, entre ellos, la Seguridad y Privacidad de la Información y las Iniciativas Dinamizadoras, dentro de las cuales están los proyectos de Transformación Digital.

El Artículo 2.2.2.47.9 del Decreto 1074 de 2015, modificado por el Decreto 1789 de 2021, establece que el uso de firmas electrónicas y digitales es una herramienta para la transformación digital, y que, en el marco del proceso de transformación digital los servidores públicos y los particulares que cumplen funciones públicas o administrativas deben utilizar firmas electrónicas o digitales.

La Resolución 0500 de 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, modificada por la Resolución 746 de 2022 de la misma entidad, impone la obligación de adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

El Acuerdo 1502 del 2021 “Guía de Ciberseguridad” expedido por el Consejo Nacional de Operación CNO establece la necesidad de coordinar acciones eficientes e integrales que permitan prevenir y/o mitigar potenciales amenazas cibernéticas que pongan en riesgo la disponibilidad y continuidad del servicio de energía eléctrica por amenazas cibernéticas.

Los Lineamientos del proceso Seguridad Digital y Continuidad de los Servicios de Tecnología, aquí definidos, permiten desplegar en EPM la Política de Seguridad de la Información y Ciberseguridad e impactan a todos los procesos del Modelo de Procesos de EPM.

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	Código <b>PL_050</b> Versión <b>01</b>
		Vigente desde 27/11/2024

La expedición del presente Lineamiento se hace teniendo en cuenta lo previsto en el Decreto 2130 de 2016, mediante el cual se define el Modelo Normativo Interno de EPM, y en consecuencia, con su entrada en vigencia se derogan los Lineamientos 2017-LINGG-20 de mayo 3 de 2017 y 2019-LINGG-49 del 11 de septiembre de 2019.

## **2. LINEAMIENTO**

### **Protección de la información, activos críticos y ciberactivos**

La información, los activos críticos y ciberactivos, deben ser valorados y protegidos a través de la implementación de los controles necesarios que permitan realizar una operación segura y confiable y contar con información íntegra y completa, con los niveles de confidencialidad requeridos para la toma de decisiones.

### **Firma Electrónica y firma Digital**

Para mitigar los riesgos propios de la información electrónica, como la alteración de contenidos y la suplantación de identidad, se establecen las firmas electrónicas y digital como mecanismos oficiales para la aprobación y firma de documentos electrónicos en Fundación EPM. Los productores de documentos, en los casos que así se requiera, deberán acogerse a los mecanismos de firma electrónica y digital, aceptados y regulados internamente para garantizar mayores niveles de seguridad y confianza en la producción de documentos en la organización, contribuyendo de esta manera, a las estrategias de transformación digital y la política cero papel.

### **Mantenimiento del inventario de activos críticos y ciber activos**

El inventario de activos críticos y ciber activos se debe mantener actualizado, para facilitar el aseguramiento y la implementación de los controles requeridos, de acuerdo con su función para la prestación del servicio de una manera segura y confiable. Esto se solicita periódicamente al total de los proveedores de estos activos críticos por parte de nuestra área de servicios TI a EPM y otros terceros.

### **Respuesta oportuna a incidentes o ataques**

Se debe monitorear permanentemente la infraestructura tecnológica, con el fin de detectar y anticiparse a la ocurrencia de incidentes y ciberataques (ciber inteligencia). Frente a la ocurrencia de un 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

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

internos y externos que sean requeridos. Esta acción se despliega desde servicios TI según las instrucciones recibidas por el proveedor servicio al que le ocurra el incidente o ataque.

#### **Continuidad del negocio y resiliencia**

En el marco de la gestión de la seguridad de la información y la ciberseguridad, se implementan mecanismos de prevención, atención y recuperación en caso de un incidente, con el fin de darle continuidad a la prestación de los servicios en el nivel predefinido como aceptable. 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. Esto se solicita periódicamente a los proveedores de estos activos por parte de nuestra área de servicios TI a EPM y otros terceros.

#### **Competencia y concienciación**

Se deben desarrollar estrategias de sensibilización, capacitación y entrenamiento permanente para los empleados y contratistas, con el objetivo de crear conciencia sobre la necesidad de proteger los activos y ciber activos críticos, el conocimiento y la información de la empresa, para que con sus actuaciones y comportamientos contribuyan a la operación continua y segura de los servicios que presta la organización.

### **3. VIGENCIA Y DEROGATORIAS**

Este lineamiento rige desde la fecha de su expedición y deroga íntegramente los Lineamientos: 2017-LINGG-20 de mayo 3 de 2017 y 2019-LINGG-49 del 11 de septiembre de 2019 y las demás disposiciones que le sean contrarias.

	<b>POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>	<b>Código PL_050</b> <b>Versión 01</b>
		Vigente desde 27/11/2024

#### **4. ANEXOS**

Ver glosario de términos:  
[https://webapp.epm.com.co/site/SIG/DVG/DTL\\_ISO\\_27001/Documentos%20de%20referencia/O- \\_SGSI-A01-002%20Glosario%20de%20Terminos%20SGSI.docx](https://webapp.epm.com.co/site/SIG/DVG/DTL_ISO_27001/Documentos%20de%20referencia/O- _SGSI-A01-002%20Glosario%20de%20Terminos%20SGSI.docx)

Dado en Medellín, en FEBRERO 23 DE 2023 GERENTE GENERAL JORGE  
ANDRES CARRILLO CARDOSO