# LINEAMIENTO 2023-LINGG-115

FEBRERO 23 DE 2023

## 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:

## CONSIDERACIONES

**1.** 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.

**2.** 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 estan los proyectos de Transformación Digital.

**3.** 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.

**4.** 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.

**5.** 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.

**6.** 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.

**7.** 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.

## LINEAMIENTO

### 1. 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 integra y completa, con los niveles de confidencialidad requeridos para la toma de decisiones.

### 1.1. Firma Electrónica[1] y Firma Digital[2]

---

[1] *La firma electrónica está definida en el numeral 3 del artículo 2.2.2.47.1. del Decreto 1074 de 2015, en los siguientes términos: "Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente".*

[2] *La firma digital está definida en el literal c) del artículo 2 de la Ley 527 de 1999 en los siguientes términos: "Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido,*

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 digitales como mecanismos oficiales para la aprobación y firma de documentos electrónicos en 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.

**2. Mantenimiento del inventario de activos críticos y ciberactivos**

El inventario de activos críticos y ciberactivos 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.

**3. 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 (ciberinteligencia). 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 internos y externos que sean requeridos.

---

*vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".*

## 4. 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.

## 5. 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 ciberactivos 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.

## 6. 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.

## 7. 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

Dado en Medellín, en FEBRERO 23 DE 2023

**GERENTE GENERAL** | **JORGE ANDRES CARRILLO CARDOSO**