LINEAMIENTO 2017-LINGG-20

MAYO 03 DE 2017

Sistema de Gestión Seguridad de la Información y Ciberseguridad

CONSIDERACIONES

Con base en lo dispuesto en el Decreto 2573 de 2014 - Lineamientos Generales para la Estrategia de Gobierno en Línea, Acuerdo CNO 788/2015 – Guía de Ciberseguridad y con el fin de garantizar el cumplimiento de la "Política de seguridad de la información y ciberseguridad para el Grupo EPM", en relación con la protección de la información, de los activos y ciberactivos críticos, la respuesta oportuna a incidentes o ataques, la resiliencia y continuidad del negocio frente a los riesgos que los pudieran afectar, se definen los lineamientos para el Sistema de gestión de seguridad de la información.
De acuerdo con el Decreto 2130 de agosto 18 de 2016 contenido del modelo normativo vigente para EPM, se derogan los lineamientos del proceso Gestión de la Seguridad de Tecnología de Información (TI), incluidos en el Decreto 1866 del 2012.

Los lineamientos del Sistema de Gestión Seguridad de la Información y Ciberseguridad impactan a todos los procesos de los ciclos y macroprocesos del Modelo de Procesos Grupo EPM

LINEAMIENTOS

1. 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.

2. 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.

3. 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.

4. 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

5. 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.

Dado en Medellín, en MAYO 03 DE 2017

GERENTE GENERAL | **JORGE LONDOÑO DE LA CUESTA**