COMITÉ CIBERSEGURIDAD REUNIÓN No. 42	Bogotá, enero 14 de 2025

1. Informe secretarios técnico – CNO.

Se hace la lectura del Informe CNO No 778 del 9-01-25, sin comentarios por parte de los asistentes.

2. Reporte de eventos cibernéticos de y a las empresas del sector.

XM presenta los eventos más relevantes de ciberseguridad para el sector, así mismo presenta las métricas de accesos y eventos publicados en la plataforma MISP.

Un supuesto ataque Ransomware habría filtrado datos sensibles de la Comisión Nacional de Energía Atómica**.**

Investigadores de Claroty han identificado IOCONTROL**,** un malware modular empleado por actores iraníes como CyberAv3ngers para comprometer dispositivos IoT y sistemas OT/SCADA en Israel y EE. UU.

3. Avances grupos de trabajo.

XM, presenta los avances de los grupos de trabajo así:

GT Reporte de incidentes: No hubo quorum para la última reunión y no se logró avanzar en la revisión del acuerdo de confidencialidad; se debe volver a agendar el grupo de trabajo.

GT Mejoras del acuerdo: Se presentaron comentarios de ITCO-Gecelca-ISAGEN y Promigas y CELSIA, los cuales están en revisión para la próxima sesión del grupo de trabajo.

GT Plantas menores: Se incluyó en el acuerdo de la guía de ciberseguridad, en el anexo con la tabla de controles, iría una columna especificando si aplica a las plantas menores, teniendo en cuenta que los requisitos está redactado el "QUE" y no el "COMO".

Se acuerda citar los grupos de trabajo antes de finalizar el mes de enero, dando espera que regresen de vacaciones la totalidad de los integrantes de los grupos.

4. Estado de confirmación o elección del presidente del comité para el año 2025.

Se confirma EPM para asumir la Presidencia del Comité de Ciberseguridad y como presidente a David Sierra.

5. Construcción del plan operativo 2025.

Se coordina la planeación del Plan Operativo del año 2025, el cual queda publicado en el sitio y pendiente de aprobación por parte del CNO.

6. Varios.

Se propone crear un grupo de trabajo para planear un ejercicio de simulación de un incidente de ciberseguridad, el cual tendrá como meta, definir el alcance para el comité de marzo.