

**COMITÉ CIBERSEGURIDAD
REUNIÓN No. 10**

Bogotá, julio 12 de 2022

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

En la próxima reunión GEB presentará el informe de avance el incidente reportado en el Comité Anterior.

XM: Alerta de agente del sector del 23 de junio: Ciberataques a corporación eléctrica de Israel.

Termoyopal: Se reporta que se están presentando muchos casos de phishing de migración Colombia.

2. Capacitación MISP.

XM realiza la capacitación de la plataforma del MISP.

Se recalca que el éxito del uso de esta plataforma está en el uso activo de la plataforma, se alimente con los casos y se explote su uso.

Se debería definir agenda periódica para revisar estadísticas e indicadores de la plataforma.

Invitar de manera formal a otras empresas para brindar capacitación, divulgación.

Se propone enviar comunicación a los agentes desde el CNO a todos los representantes de ciberseguridad del sector. XM estructura la invitación.

Importante separar espacio donde todos los agentes comprendan la importancia del uso de la herramienta.

Aprovechar la jornada de ciberseguridad sobre la charla del MISP.

Definir las políticas de administración de los usuarios del MISP.

EPM manifiesta la importancia de evolucionar el CSIRT 0 y conformar un equipo de respuesta de incidentes, integrado por especialistas de diferentes empresas que puedan apoyar un incidente grave. Se puede empezar a desarrollar un mapa de capacidades para la conformación de la capacidad de respuesta de incidentes del sector.

3. Avances en temas del CSIRT sectorial.

Se tuvo conversación con la experta comisionada de la CREG con quien se está tocando el tema y manifiesta que no se ha avanzado en el tema. Lo anterior indica que los esfuerzos del sector para un CSIRT deben ser propios.

Además de la CREG también tener en cuenta los apoyos que se puedan tener de MINTIC y lo definido en el Decreto 338 de marzo de 2022.

4. Avances de preparación de la jornada de Ciberseguridad.

Se va a agendar una Reunión del grupo que está trabajando en la agenda para definir la agenda y confirmar a los expositores. El CNO citará la reunión.

5. Presentación indicadores de calidad de la operación - XM.

XM hace la presentación de los indicadores. No se tienen comentarios ni inquietudes.

6. Tabulación inicial de las encuestas de cumplimiento del Acuerdo 1502.

CNO y Colombia Inteligente presentan los resultados de la encuesta.

Se presentan dudas sobre el cumplimiento de algunos puntos, ya que se reportan actividades que se debieron cerrar en el 2021 y aún no están al 100%.

Se aclara que la presentación muestra los datos crudos y queda el documento para realizar los respectivos análisis.

Se propone realizar la revisión de los resultados del seguimiento del semestre I de la 1502, en la reunión de análisis del acuerdo 1502. CNO agenda la reunión.

Se manifiesta que hay información muy valiosa tomada de la encuesta.

EBSA propone que se den respuestas formales a las inquietudes y comentarios presentados en la encuesta, para lo que define realizar un plan de trabajo.

7. Varios.

1. Revisión del plan operativo: Adriana Perez

Se actualizan los siguientes puntos:

- Vigilancias prácticas y señales normativas de ciberseguridad.
- Gestión y seguimiento CSIRT y aspectos regulatorios de ciberseguridad
- Monitoreo y seguimiento mensual técnico
- Medición del nivel de madurez de ciberseguridad
- Medición del cumplimiento semestral técnico del acuerdo de ciberseguridad
- Participación en las mesas de infraestructuras críticas.
- Análisis de restricciones

- Seguimientos regulatorios y acuerdos
 - Resiliencia del SIN.
 - Revisión de acuerdos.
 - Análisis de las implicaciones del acuerdo 1502 de ciberseguridad en AGC.
 - Jornada de ciberseguridad.
 - Se retiran los siguientes ítems del plan operativo:
 - Monitoreo y seguimiento mensual técnico al cumplimiento de la guía de ciberseguridad
2. Citación a los GT:
- AGC: Para el 25 de julio de 2:00 a 4:00
 - Plantas menores: 29 de julio 2:00 a 4:00
 - Grupo de medida: 27 de julio de 2:00 a 4:00
3. Feedback de los agentes sobre los puntos de la agenda: Se manifiesta que sería muy importante que los demás agentes propongan temas para discutir en las reuniones. Se incluyen los puntos:
- Incluir el operador del evento de la jornada de ciberseguridad para la sesión de agosto.
4. Compartir información sobre cumplimiento de controles: XM propone construir guías específicas para compartir con todo el sector sobre el cumplimiento de los controles de la guía de ciberseguridad para lo cual están de acuerdo.
5. Llegó una consulta de Gecelca en la cual solicita información sobre el Acuerdo 1502, numeral 4 y 5 donde la elaboración del plan y la implementación del control están para la misma fecha, la cual queda pendiente de revisión en el grupo de trabajo que está revisando la guía de ciberseguridad.