COMITÉ CIBERSEGURIDAD REUNIÓN No. 34	Bogotá, mayo 7 de 2024

1. Informe secretario técnico - CNO.

Se presentó el informe correspondiente a la reunión 748 del C N O.

ENEL pregunta por el motivo de los bloqueos, a lo cual se informa que son por temas sociales y puntuales y no de manera general dirigidos al sector eléctrico.

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

XM hace la presentación de los indicadores de calidad, sin preguntas por parte de los asistentes.

Se propone separar un espacio en el próximo comité para tratar el tema de eventos del sistema SOE o Scada.

3. Protocolo de asistencia a reuniones de Ciber del CNO.

Se propone lo siguiente:

Que se utilice la nomenclatura de empresa – nombre.

Quien tenga invitados, es responsable que se conecten al momento indicado.

ENEL y Energía de Colombia hacen referencia a la seguridad de los documentos del CNO que se publican en internet, por lo cual se debería hacer una revisión. Al respecto el CNO informa que los documentos que se publican en el sitio del CNO tienen control de acceso. Sin embargo, Adriana Pérez aclara que la información del CNO es pública y CNO no es responsable del manejo que le den los integrantes a información sensible que se trate en las reuniones preparatorias y demás.

- ENEL hace énfasis en que la esencia del comité de ciberseguridad es tratar temas sensibles y por lo cual se debería establecer criterios de seguridad
- https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/Acta%20CNO%20700.pdf
- https://es.scribd.com/document/463487056/Avances-Ciberseguridad-Lecciones-aprendidas-Acuerdo-CNO-788
- https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/informe_cciberseguridad_17_vao_0.pdf
- https://www.cno.org.co/content/acta-reunion-cno-694
- https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/evucc_cno.pdf

Adriana Perez, confirma que revisa los enlaces y no ve problemas de fuga de información y que la información relacionada es pública, lo mismo confirma Juan David Molina con el documento de Colombia Inteligente, ya que fue una presentación que se hizo en las jornadas de ciberseguridad. Sin embargo, la Asesora Legal aclara que va a revisar si estos enlaces debieran estar protegidos, y va a confirmar que para la sesión de documentos y actas de Ciberseguridad el acceso si esté restringido y protegido.

C N O confirma que las personas que no se identifiquen adecuadamente en las sesiones virtuales son expulsadas y los demás integrantes ayudamos en el control validando que los miembros de cada empresa si sean los que se identifican.

En conclusión, para participar en las reuniones de ciberseguridad virtuales el nombramiento es Nombre Empresa - Nombre Persona, Ejemplo, XM - Juan Ortiz

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

XM hace la presentación de los principales eventos de ciberseguridad presentados durante el último mes y que pueden afectar al sector y muestra las estadísticas de uso de la herramienta MISP.

XM también manifiesta que las noticias falsas pueden ser un problema para la operación y se debe de revisar en el grupo de trabajo de reporte de incidentes.

AES pregunta sobre el tipo de acciones que se toman desde XM, indicándoles que estas son de acciones preventivas en la red de TI, siempre tratando de establecer primero la comunicación con el agente.

ENEL pide que estas acciones se tomen de manera conjunta con el agente tratando de verificar la ocurrencia e impacto del incidente.

TEBSA comparte la experiencia relacionada con los falsos positivos en los buzones de correo, especialmente con los buzones donde se reciben las quejas y se ven muchos correos que pasan los filtros. También informa que hace uso recurrente del MISP, informando que ha encontrado IP de Microsoft entre los IOC y eso podría causar indisponibilidad en algún servicio.

Termocandelaria informa sobre un caso presentado con un phishing a nombre de AFINIA que enviaba un descuento en los valores de energía, estafando a los usuarios.

5. Avances grupos de trabajo.

Colombia Inteligente hace una presentación sobre los puntos más relevantes del estudio de cumplimiento de la guía de ciberseguridad.

AES pide verificar la posibilidad de realizar el análisis por rango de tipo de plantas y poder entender la gestión que han estado realizando las diferentes plantas y plantear la opción de disminuir los requisitos de los activos críticos.

XM presenta los avances de los grupos de trabajo de seguridad en plantas menores, mejoras al acuerdo 1502 y reporte de incidentes, indicando los siguientes pasos y las fechas de las próximas sesiones: Seguridad en plantas menores: 16 de junio (virtual), Mejoras al acuerdo 1502: 31 de mayo (híbrida), Reporte de incidentes: 7 de junio (virtual).

También se realizan algunas preguntas que han surgido durante las sesiones de trabajo.

1. Plantas menores:

    - Revisar si los acuerdos son penalizables en caso de no cumplimiento.

      RESPUESTA: Los Acuerdos son de obligatorio cumplimiento de los agentes del SIN y el operador del Sistema, por mandato legal. Son objeto de vigilancia, inspección y control de la SSPD.

    - Si las plantas menores no tienen participación ¿cómo sería la divulgación de los acuerdos?

      RESPUESTA: Actualmente, por mandato legal (Ley 2099 de 2021) uno de los miembros del CNO es un representante de las empresas que generan de forma exclusiva con FNCER. Se consideran FNCER las siguientes actividades, de acuerdo con lo previsto en la Ley 1715 de 2014 modificada por la Ley 2294 de 2023: “17. Fuentes No Convencionales de Energía Renovable (FNCER). Son aquellos recursos de energía renovable disponibles a nivel mundial que son ambientalmente sostenibles, pero que en el país no son empleados o son utilizados de manera marginal y no se comercializan ampliamente. Se consideran FNCER la biomasa, los pequeños aprovechamientos hidroeléctricos, la eólica, la geotérmica, la solar y los mares. Otras fuentes podrán ser consideradas como FNCER según lo determine la UPME.” En el Numeral 10 del artículo 5 de la Ley 1715 de 2014 modificado por el artículo 235 de la Ley 2294 de 2023: se prevé lo siguiente sobre pequeños aprovechamientos hidroeléctricos: “10. Energía de pequeños aprovechamientos hidroeléctricos: Energía obtenida a partir de cuerpos de agua de pequeña escala, instalada a filo de agua y de capacidad menor a los 50 MW." Teniendo en cuenta la definición regulatoria de las plantas menores, que corresponde a aquellas que tienen una capacidad inferior a 20 MW, se entiende que las empresas representantes de estas plantas se incluyen en el grupo que selecciona el miembro del CNO que representa a los generadores que de forma exclusiva lo hacen con FNCER. Por lo anterior, el CNO tiene un representante de los generadores FNCRE, que para el 2024 es Energía del Suroeste. Es importante tener en cuenta lo anterior, para efectos de divulgación y revisión del Acuerdo. La divulgación en este caso se hace

a la base de datos que XM tiene sobre empresas que representan plantas menores y a través de su representante en el CNO

- Revisar los estatutos para plantas menores en cuanto a la participación de los comités del CNO.

  RESPUESTA: Ver respuesta anterior.

- Implicación legal documento del DOCUMENTO CREG-065 30 DE AGOSTO DE 2019 o si esto ya no es vigente (adjunto archivos).

  RESPUESTA: El Documento CREG 065 de 2019, Estrategia integral de ciberseguridad del sector eléctrico, fue un documento en consulta (Proyecto) que se sometió a consideración para consulta y comentarios públicos el 11 de septiembre de 2019 y con un plazo hasta el 31 de octubre de 2019 para enviar comentarios. Teniendo en cuenta que fue un documento en consulta y no un documento definitivo, no es un documento de obligatorio cumplimiento, si no de referencia. Sobre la gobernanza de la seguridad digital debe tenerse en cuenta lo previsto en el Decreto 338 de 2022.

2. Ajustes al acuerdo:

   - Si el acuerdo 1502 sufre cambios tenemos, entendido que su actualización sale como un nuevo acuerdo. Siendo de esta forma, ¿quisiéramos saber si el tiempo de implementación empezaría nuevamente desde su nueva publicación?

     RESPUESTA: cualquier cambio que se haga a un ACUERDO CNO entra en vigencia a partir de la fecha de su expedición y hacia el futuro. El tema de los plazos no se desconoce y se generan nuevos plazos a partir de la fecha de expedición del nuevo acuerdo. Los nuevos requisitos se empiezan a exigir a partir del momento de entrada en vigencia. A la hora de redactar se debe tener cuidado con las obligaciones del pasado.

   - El tema de capacitaciones sobre conciencia de ciberseguridad, políticas, lineamientos, entre otros para terceros que implicaciones legales puede tener para una empresa la empresa contratante. También que consideraciones legales se debe de tener para hacer estudios de seguridad a los terceros (punto 5.2.3, 5.3.3, 5.3.5 del acuerdo).

     RESPUESTA: Con los terceros se maneja a través del contrato, solicitando al tercero que se cumplan los puntos de la guía. En la guía se debe establecer puntos que sean cumplibles.

6. Temas jornada de ciberseguridad 2024.

Los temas tratados en este comité se extienden y se pospone este ítem para el próximo comité, sin embargo, se deja el compromiso de llevar propuestas de temas que se podrían presentar en las jornadas de ciberseguridad, las cuales están previstas para el 27 de septiembre de 2024.

7. Varios.

Este punto de la agenda no se llevó a cabo, pues otros puntos del comité se extendieron.