|  |  |
| --- | --- |
| **COMITÉ CIBERSEGURIDAD REUNIÓN No. 8** | **Bogotá, mayo 10 de 2022** |

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

XM, presenta una alerta reportada por un agente sobre la amenaza Voodoo Bear reportada en abril.

Así mismo informa que ya se tiene una instancia de MISP en la nube para desarrollar la PoC y está pendiente publicarla a internet para que los agentes puedan empezar a usarla.

XM realiza la presentación de la arquitectura implementada por XM para la supervisión de plantas menores: Se acuerda crear un grupo de trabajo de ciberseguridad para identificar los requisitos de seguridad que se deben cumplir por parte de quienes se conecten a esta infraestructura de supervisión, para luego ser presentada al comité de supervisión y finalmente presentarla al CNO para definir el tema regulatorio y validar si se puede generar mediante Acuerdo.

Se aclara que esta infraestructura es para plantas menores a 19.9 MW y que es una alternativa al enlace ICCP.

Empresas que revisan la arquitectura y definir controles mínimos:

* XM.
* EPM.
* CELSIA.
* TERMOCANDELARIA.

1. **Presentación COLCERT.**

Se da la bienvenida a la doctora Angela Cortés y en forma general se le presenta el Comité de Ciberseguridad del CNO.

La doctora Angela Cortés hace una presentación sobre el ColCERT -Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT- y sobre el Decreto 338.

Hace un recuento de cómo funcionan los temas de acuerdo con los cambios definidos por el gobierno:

* Las mesas técnicas de trabajo se harán con MINTIC.
* Las mesas de infraestructura críticas se van a seguir haciendo, con coordinación desde MINTIC.
* Se recibieron las BD del comando conjunto cibernético y trabajarán en su actualización.
* La información del sector eléctrico se actualizará la información a través del CON.
* En la página de MINTIC ya se encuentra funcional el micrositio de ColCERT, donde compartirán la información.
* El ingeniero Zamudio de ENEL COLOMBIA, interviene e informa que se tiene un avance de un acuerdo de cooperación, para retomarlo.
* XM cuenta sobre el estado del CSIRT del sector.
* Se pregunta por estándares para proceso de vinculación al COLCERT, la respuesta es que se está trabajando en los lineamientos y se informará posteriormente.

La doctora Angela Cortés manifiesta el interés que el ColCERT tiene en trabajar con las empresas del sector eléctrico y con el Comité de Ciberseguridad del CNO.

Teniendo en cuenta la reestructuración del ColCERT informa que en los próximos meses se entregará información que permita trabajar de forma coordinada los temas de cibersegurirdad con los diferentes sectores.

1. **Avance preparación jornadas de ciberseguridad.**

El presidente del Comité presentó la propuesta de agenda para la jornada de ciberseguridad, confirmando la fecha que es para el 30 de septiembre de 2022, se buscará hacerla presencial en la ciudad de Bogotá.

Se propone generar recomendaciones para las charlas magistrales.

Se propone hacer contactos con diferentes universidades para preparar una de las presentaciones.

Se propone seguir avanzando en un grupo de trabajo independiente para continuar la preparación de la agenda.

El CNO citará a segunda reunión del grupo de trabajo de preparación de las jornadas.

1. **Presentación indicadores de calidad de la operación.**

XM presenta los indicadores del mes de abril 2022. No se presentaron comentarios por parte de los asistentes.

1. **Avances relación con la CREG y MINTIC sobre normatividad en ciberseguridad.**

La asesora jurídica del CNO, comparte el borrador de la carta que se va a enviar a la CREG con el asunto: Nueva Gobernanza de seguridad digital (Decreto 338 de 2022), con la cual los asistentes están de acuerdo y se propone enviar copia al Colcert.

Se enviará carta a la CREG, con copia a ColCERT, sobre la nueva gobernanza de seguridad digital.

1. **Nueva normatividad y Acuerdo CNO 1502.**

La asesora jurídica del CNO comenta que se debe incluir la nueva gobernanza de seguridad digital en el acuerdo, haciendo revisión de las definiciones del anexo, teniendo en cuenta que la guía está basada en normas y estándares, contra las definiciones del Decreto 338.

Todos los miembros del comité deben revisar el acuerdo 1502, la parte normativa del acuerdo debe hacer referencia al nuevo decreto.

Se debe compatibilizar las definiciones del anexo del acuerdo 1502, considerando los estándares.

Luego se realizó la socialización de cómo se implementa actualmente el tema de aseguramiento de antecedentes del personal AES, EPM y otros.

AES informa a los asistentes sobre el proceso que se lleva en su empresa para la evaluación de antecedentes de personal, teniendo en cuenta que se rige por normas como la NERC y tiene la experiencia de la norma en otros países como estados unidos.

EPM hace una presentación sobre el proceso que se tiene en EPM sobre la evaluación del personal para el cumplimiento del acuerdo 1502.

ENEL COLOMBIA, interviene informando que han tenido inconvenientes desde el punto de vista laboral.  Ellos solicitan consentimiento a cada trabajador, para los que llevan más de 5 años en la compañía. El estudio de antecedentes lo tienen tercerizado.

AES comenta que en Estados Unidos se puede mover del cargo o despedirse (siempre y cuando el antecedente tenga relación directa con riesgos en los ciberactivos críticos).

1. **Varios**.

* Resumen de AGC: EPM presenta un resumen de la última Reunión de AGC. Mencionó los tres puntos que se discutieron, haciendo énfasis en las pruebas que se realizarían. Se confirma que XM enviará las memorias de esa reunión el próximo martes 17 de mayo.

* Envío del instrumento de medición: La asesora jurídica C N O confirma que para finales de esta semana se estará enviando a las empresas para su diligenciamiento. Se tiene como fecha límite el 09 de junio para diligenciar la encuesta.