COMITÉ CIBERSEGURIDAD REUNIÓN No. 6	Bogotá, marzo 8 de 2022

1. Reporte de eventos cibernéticos de ya las empresas del sector.

XM realiza presentación de algunos eventos cibernéticos

Celsia reporta de varios IOCs que han compartido a través de su SOC, como Wiper, movimientos laterales, ataques de DDoS. Va a compartir estos IOCs a través del ISOC de XM.

Diego Zuluaga comparte que hay movimientos a nivel global debido a la situación Rusia-Ucrania, especialmente en Ucrania donde se han presentado dos eventos contra el sector eléctrico. Se han presentado ataques en Colombia del APT-C36, para lo cual recomienda revisar si hay incidencia en el sector eléctrico. Diego también indica que el ColCERT se está reorganizando en el MINTIC.

AES comparte información sobre LAPSUS que estuvo detrás del ataque a Samsung y Mercadolibre, esta última después de hacer una encuesta sobre que empresas quisieran atacar y sobre BazarLoader EnAnalisis/2022-02-28_BazarLoader_DominiosComprometidos at main · CronUp/EnAnalisis · GitHub

GECELCA expresa una inquietud sobre la Directiva Presidencial en el punto 16: Las redes inalámbricas (WiFi) de servicio en las entidades, deben ser redes para acceso y consulta de internet y no para que por medio de estas se administren infraestructuras internas o se acceda a servicios misionales. internos desde dispositivos no corporativos. Se aclara que la Directiva aplica a todas las empresas públicas. Estos controles se exigen dado los recientes ataques como el de INVIMA.

XM reitera lo importante de compartir información y destaca lo nutrido de la reunión del día de hoy.

CON pregunta si se debe generar un comunicado a todo el sector. EPM manifiesta que se deben reforzar las actividades de sensibilización al interior de cada organización. GEB recomienda compartir los IOCs del APT-C36. Al respecto el secretario técnico indica que estamos en CAOP recomienda generar la alerta de manera muy cautelosa para no generar alarma en el sector, teniendo en cuenta tanto la situación global Rusia-Ucrania y la local de elecciones.

Se acuerda enviar un comunicado a los responsables de ciberseguridad de las empresas.

2. Revisión Plan Operativo 2022, definir acciones.

CNO lidera la revisión teniendo en cuenta la información que está disponible en la página del CNO.

El presidente del Comité solicita que se revise punto por punto con la finalidad de que todos los miembros del Comité tengan claridad de cada actividad, y si es necesario se definan responsables y seguimientos.

- Vigilancia, prácticas y señales normativas de ciberseguridad: Juan Carlos Carreño pregunta cuál es la expectativa frente a este punto.
- EPM manifiesta Inquietudes sobre los temas del Comité Operativo y de los asistentes, donde CNO da claridad a las inquietudes.

- Gestión y seguimiento CSIRT y aspectos regulatorios: Se solicita hacer el acercamiento desde el CNO a la CREG para revisar el avance regulatorio.

- Monitoreo y seguimiento mensual técnico de acuerdos de ciberseguridad: Se hará seguimiento mensual del acuerdo de ciberseguridad y alerta de riesgos en el cumplimiento de los plazos.

- Medición del nivel de madurez de ciberseguridad: Se tiene planeado para el segundo semestre.

- Medición del cumplimiento semestral, técnico de acuerdo de ciberseguridad: Se define realizar una revisión de la encuesta para aprobarla en la reunión del mes de abril. Juan David Molina envía el documento. Así mismo el compromiso de la auditoría del mes de abril, debe ser dirigida al secretario técnico del CNO.

- Participación en las mesas de infraestructura crítica: Reanudar acercamientos con ColCERT, CCOCI para la participación del sector eléctrico.

- Análisis de restricciones: Sin comentarios.

- Seguimiento regulatorio y acuerdos: Se hace ajustes en los subtemas.

- Indicadores de calidad de la operación: Se propone incluir en la agenda del Comité de Ciberseguridad en todas las reuniones.

- Resiliencia del SIN: Sin comentarios.

- Revisión de acuerdos: Sin comentarios.

- Matriz de riesgos operativos: El presidente propone generar una matriz de riesgos para el sector y el secretario Técnico resume lo que se ha trabajado sobre el tema.

- Análisis acuerdo 1502 en la función de AGC: hay un grupo de trabajo revisando el tema. Queda pendiente citar la segunda reunión del grupo de trabajo.

Se incluye en el plan las jornadas de supervisión y ciberseguridad para el mes de septiembre. Se propone incluir en la agenda de la próxima reunión la preparación de las jornadas de ciberseguridad.

3. Seguimiento CSIRT Sectorial.

Se hace la presentación de los avances del Grupo de Trabajo respecto a la implementación del MISP, especialmente en la arquitectura propuesta.

Diego Zuluaga recomienda que se use la taxonomía nacional definida por el ColCERT y CSIRT Américas.

Se aprueba un espacio para realizar definiciones del CSIRT.

4. Definir alcance, encargados y fechas para actividades de sensibilización, comunicación, entrenamiento y socialización de la Guía de Ciberseguridad del CNO y de los procesos de seguridad cibernética.

GEB indica que ese es el objetivo de las jornadas de Ciberseguridad.

Se indica que sería recomendable tener espacios adicionales a las jornadas de Ciberseguridad para realizar la capacitación sobre la guía de ciberseguridad.

CON manifiesta que con la experiencia que tiene en la socialización de los acuerdos, sería suficiente con las jornadas de ciberseguridad.

Se define que se tenga un espacio adicional en las jornadas de ciberseguridad para aclarar dudas que se tengan.

5. Presentación análisis resoluciones 171 y 148.

El ingeniero Isaza de ISAGEN presenta el análisis de la Resolución CREG No 148, 173 y 174, indicando que no tienen requisitos de seguridad obligatorios. Es importante tener en cuenta que estas plantas puedes ser supervisadas desde el CND, lo cual implica un riesgo para la operación en caso de un evento de ciberseguridad. También, de acuerdo con la 148 todas las plantas deben ser supervisadas por el operador de red. Tener presente que todos los comentarios y apreciaciones están enfocados al ámbito de ciberseguridad y cuando se expresa que no hay acuerdos del CNO es referente a la materia.

XM queda con el compromiso de llevar al Comité los requisitos de ciberseguridad que se le están exigiendo a las plantas menores para conectarse al CND.

AES indica que en los EE. UU. a las plantas pequeñas se les exige tener políticas de seguridad alineados con la NERC, sin exigirle la forma de cumplir los requisitos.

6. Varios.

Juan Molina de Colombia inteligente expone la metodología de medición del estado de madurez en ciberseguridad. AES propone cambiar la forma de compartir la información de la encuesta, para hacerlo de una forma más segura, ya que el método actual del Excel por correo electrónico no posee la suficiente seguridad.

AES expresa la inquietud sobre el requisito de la guía de ciberseguridad en la evaluación de la vida laboral de las personas que trabajan en ciberseguridad, sobre qué pasa si en una evaluación periódica y la persona lleva años ya trabajando, ¿cómo se debería proceder? La guía no lo establece. También hace el comentario sobre los siguientes puntos del procedimiento, pero no sobre el control:

6.3.4 Validación de cambios

Cada entidad responsable deberá asegurar que nuevos ciberactivos críticos y cambios en ciberactivos críticos existentes dentro del perímetro de seguridad electrónica, no afecten adversamente los controles de ciberseguridad existentes, esto debe incluir la aprobación de cambio por el responsable de ciberseguridad o su delegado

7.3.1 Procedimiento de control de cambios y gestión de configuraciones

La entidad responsable deberá documentar los cambios y la gestión de la configuración sobre los ciberactivos críticos y la evaluación del riesgo e impacto sobre ciberseguridad, Se deberá asegurar que nuevos ciberactivos críticos y cambios en ciberactivos críticos existentes dentro del perímetro de seguridad electrónica, no afecten adversamente los controles de ciberseguridad existentes.

5.2.4 Procedimiento información
5.2.5 Medidas para garantizar información
5.2.6 Procedimiento gestión acceso a la información
5.2.7 Procedimiento organizacional y técnico de puntos de acceso
6.2.1 Procedimiento gestión de acceso
6.2.2 Procedimiento control de acceso
6.2.3 Procedimiento de autenticación, autorización y registro
5.3.4 Programa de conciencia de seguridad
5.3.5 Programa de entrenamiento y capacitación
5.3.6 Administración de accesos
5.3.7 Verificación de los registros de autorización
5.3.8 Verificación de cuentas y privilegios de acceso
5.3.9 Procedimiento de revocación de accesos

6.3.1 Perímetros de seguridad electrónica
6.3.2 Listas de acceso
6.3.3 Procedimiento de monitoreo y registro de acceso
6.3.4 Validación de cambios
6.3.5 Procedimiento para habilitar los puntos de acceso
6.3.6 Procedimiento para la administración de conexiones temporales
6.3.7 Sistema de control intermedio
8.3.3 Registro de cambios del procedimiento de recuperación y resiliencia
8.3.4 Respaldos y almacenamiento de información
8.3.5 Pruebas a los respaldos y mecanismos de contingencia y continuidad
9.3.3 Registro de cambios del procedimiento de respuesta a incidentes

Se acuerda que AES envíe una comunicación al CNO y se revisará para definir la mejor forma de abordarlo.