

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

GEB informa sobre un incidente que se tuvo, donde descargando un firmware, descargó un ransomware que cifró el computador del contratista. El ransomware es de la familia De-Javú, que se descargó mediante un .zip e inició el cifrado de los archivos. Como medida de contención se aisló el equipo de la red.

También se detectó que el equipo tenía antivirus kasperky pero no estaba actualizando correctamente. También menciona que Caracol y Blu Radio fueron afectados por un ransomware.

AES: Resalta la importancia del Cyber Awareness, que muy probablemente no fue implementado por el contratista, así como la validación del estado de los controles.

AES también menciona la vulnerabilidad de Microsoft relacionado con la posibilidad de insertar Código malicioso que se ejecuta sin requerir las macros.

Así mismo menciona los grupos de ransomware que atacaron al gobierno de Costa Rica, y están extorsionando al gobierno para que pague el rescate, afectando los servicios de administración pública. Un hecho que ha trascendido a los medios de comunicación está asociado a que los respaldos no eran funcionales.

GECELCA: Hace mención del control de UMBRELLA, que es una solución de CISCO para sanitización del tráfico de internet, evitando conexiones a sitios.

C N O menciona que XM alerta sobre los ataques con ransomware a noticias Caracol y la importancia de alertar desde el Comité de Ciberseguridad, de cara a las elecciones de segunda vuelta presidencial.

ENEL COLOMBIA y AES COLOMBIA resaltan la importancia de establecer procedimientos de respuesta de incidentes e incluso de la implementación de botones de pánico.

2. Avances en temas del CSIRT Sectorial.

C N O informa que envió la comunicación sobre el Decreto Presidencial y los cambios en gobernanza en seguridad digital y no se ha obtenido respuesta. Está pendiente discutirlo en la próxima reunión que se tiene para la CREG.

3. Avance preparación jornadas de ciberseguridad.

XM presenta el logo y slogan propuesto para las jornadas, del cual se hacen algunas recomendaciones y se envía al C N O para que la empresa encargada de la logística del evento realice los ajustes.

Se presentan los ponentes que se han confirmado y se acuerda que en la próxima sesión del grupo de trabajo se consolidará la información.

4. Presentación indicadores de calidad de la operación.

XM presenta los indicadores de calidad, sin comentarios por los asistentes.

5. Tabulación inicial de las encuestas de cumplimiento del Acuerdo 1502. – Colombia Inteligente.

C N O informa que se está realizando la tabulación, sin embargo, no se tiene el informe final.

COLOMBIA INTELIGENTE resalta el incremento de las empresas que dieron respuesta a la encuesta.

Una vez se cierre esta fase, se estará enviando la herramienta para identificar las prácticas de madurez de ciberseguridad en el sector y poder tener ambas para socializarlas en las jornadas de ciberseguridad.

EPM menciona que hay preguntas de la encuesta que no aplican para la temática del comité de ciberseguridad, sin embargo, COLOMBIA INTELIGENTE y el C N O confirman que son las mismas preguntas que se han venido formulando en los ejercicios anteriores.

6. Varios.

Se recuerda la reunión faltante del GT de AGC, la cual se va a coordinar para la semana del 20 de junio.

C N O informa que va a verificar con Diego Zuluaga cómo va el tema de las mesas de infraestructuras críticas, para la citación a las actividades acordadas.

