Módulo 1

Día 1

El CSIRT Nacional de la Agencia Nacional de Ciberseguridad (ANCI) publica una Alerta relacionada a una variante nueva de Ransomware. Este Ransomware es usado en una campaña enfocada en afectar a prestadores de servicios esenciales del país..

Día 2

Ha pasado un año desde que el desarrollador del sistema operativo de tu organización anunció que no seguirán desarrollando parches de ciberseguridad. El último parche fue instalado la semana pasada. Este problema fue identificado en la última evaluación de riesgo anual de tu institución.

Día 4

Un empleado de tu institución informa a su jefatura que su computador de trabajo fue robado desde su auto la última noche. El computador contenía información sensible de la organización.

Día 6

Integrantes del departamento de finanzas de tu institución reciben un correo electrónico que parece ser de la directora de finanzas de la organización. En el correo, se pide acceder a un PDF conteniendo detalles sobre una cuenta impaga de un proveedor externo apoyando la organización. Varios empleados llaman a la directora de finanzas para verificar la autenticidad de la comunicación. Ella contesta que no lo envió, y que no hay una cuenta pendiente de pago. Sin embargo, algunos empleados abren el PDF.

Preguntas de discusión

Discutan las siguientes preguntas durante el módulo, las cuales están diseñadas para explorar los distintos aspectos de resiliencia operacional de la institución. Las preguntas en negrita deben ser contestadas por escrito, además de ser discutidas.

1. **¿Cuáles son las mayores ciber amenazas que pueden afectar su organización?**
2. **¿Cuáles son los procesos de tecnologías de la información más críticos?**
3. **¿Cómo debería guardar tu organización sus respaldos? ¿Qué tan seguido? ¿Por cuánto tiempo deberían guardar respaldo? ¿Dónde deberían estar esos respaldos? ¿Cuánto tomaría restaurar los respaldos? ¿En qué formatos deben ser guardados?**
4. **¿En qué temas entrenarías a los empleados de tu organización para prevenir los efectos de incidentes de ciberseguridad? ¿Cada cuánto tiempo deben completar el entrenamiento? ¿En qué momento debería hacerse el primer entrenamiento? ¿Cómo debiese cambiar el entrenamiento si el usuario tendrá privilegios administrativos? ¿Qué métodos de entrenamiento encuentras más efectivos?**
5. **¿Qué opinas del impacto de los ejercicios de phishing que hacen las empresas a sus empleados? ¿Qué debería hacer el departamento IT cuando correos sospechosos son**

reportados? ¿Cómo debería entregarse retroalimentación a los empleados que reportan phishing?