**DESARROLLO DEL LABORATORIO NRO 3. BOOTCAMP DE CIBERSEGURIDAD**

**Estudiante: Paola Barros**

***Actividad 1: Recolectar información sobre los primeros signos del incidente.***

Se debe realizar una investigación exhaustiva sobre el origen del incidente o el origen de lo que provocó el incidente. Un ejemplo sería un mensaje de texto con un link malicioso o un correo electrónico haciéndose pasar por una persona o empresa y que contenga un link malicioso también. De esta forma se puede encontrar una manera de encontrar la solución.

***Actividad 2: Evaluar la evidencia para identificar el vector de ataque.***

Dependiendo del ataque, se debe evaluar la evidencia. En el caso que sean archivos infectados, se debe revisar de dónde provienen y también los logs para saber qué otras partes del sistema pudieron ser afectados.

***Actividad 3: Describir los logs que deben revisarse en los sistemas afectados.***

En el visor de eventos podemos ver los diferentes logs del sistema. Desde aquí se pueden ver y revisar los logs para saber qué partes fueron infectadas en el sistema. Se recomienda revisar los logs de seguridad, base de datos y correo electrónico.

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

***Actividad 4: Analiza los logs en busca de patrones inusuales.***

Algunos patrones sospechosos que nos pueden dar idea de si el sistema fue comprometido son: inicios de sesión inusual, actividad desde una cuenta privilegiada en horarios inusuales, accesos inusuales a bases de datos, Conexiones salientes a IPs desconocidas o maliciosas, ejecución de procesos sospechosos, modificaciones inusuales en los logs.

***Actividad 5: Evalúa cómo el incidente ha afectado la disponibilidad, integridad y confidencialidad de los datos.***

¿Pudieron los usuarios acceder a los datos/sistemas cuando lo necesitaban?

¿Fueron los datos modificados, eliminados o manipulados sin autorización?

¿Accedió alguien no autorizado a información sensible?

***Actividad 6: Implementar medidas para detener el ataque y prevenir una mayor propagación.***

* Aislar los sistemas comprometidos, ya sea desconectándolos de su fuente de poder.
* Revocar accesos sospechosos inmediatamente, ya sea cambiado credenciales o revocando permisos.
* Detener los procesos o servicios maliciosos que puedan estar corriendo.
* Hacer escaneos con antivirus y actualizar sus firmas.

***Actividad 7: Determina a quién se debe informar sobre la situación y las medidas tomadas.***

* Altos mandos de la empresa
* Personas y usuarios afectados
* El equipo de seguridad o IT de la empresa
* Autoridades dependiendo del caso

***Actividad 8:******¿Qué medidas se deben llevar a cabo después de haber pasado por un incidente?***

* Detección y erradicación de la amenaza.
* Restauración de sistemas afectados.
* Cambios de credenciales
* Reporte y documentación de incidentes.