# Laboratorio 3

Sergio Alberto Tarrifa Ramirez

En el caso de phishing en un inicio debe reconocerse el origen del ataque, sea un correo electrónico, un mensaje de texto o algún otro tipo, identificar archivos adjuntos, links fraudulentos y el objetivo del ataque.

**Log del servidor de correo electrónico:** En este se debe buscar cualquier información que indique la hora, la procedencia y el objetivo del ataque, tal vez este iba dirigido a un empleado y buscó explotar la vulnerabilidad humana o una vulnerabilidad en el sistema.

**Log del sistema de bases de datos:** Se debe buscar algún intento de modificación de la información contenida en la base de datos de la empresa, así como algún intento de lectura.

**Log de seguridad:** Se deben identificar avisos automatizados del sistema con el objetivo de identificar la vulnerabilidad explotada para ingresar y cubrirla para evitar futuros ataques.

Utilizando los logs anteriores se deben identificar los sistemas comprometidos, ya sean servidores, terminales o impresoras.

Con el objetivo de garantizar la disponibilidad, integridad y confidencialidad de la información.

Si ya se ingresó al sistema de manera fraudulenta, se deben, desconectar sistemas si no son estrictamente necesarios mientras se aísla el problema, los terminales y servidores deben recibir actualizaciones de seguridad y deben cambiar las credenciales de acceso con el objetivo de evitar mayores complicaciones o puertas traseras de acceso.

Si existe una modificación a la base de datos se debe regresar a las copias de seguridad previas al ataque para mantener la integridad de los datos.