**UNIVERSIDAD NACIONAL DE JUJUY - FACULTAD DE INGENIERÍA**

**INGENIERÍA INFORMÁTICA – LICENCIATURA EN SISTEMAS**

**AUDITORÍA INFORMÁTICA – SEGURIDAD EN SISTEMAS**

**TRABAJO PRÁCTICO Nº 1**

**Fecha de presentación: 07/09/2023**

1. Identifique el/los objetivo/s (parámetro/s) de seguridad que se ven afectados en los siguientes casos. Justifique su respuesta
   1. Un atacante obtiene acceso a las cuentas bancarias en línea de varias personas al robar sus credenciales de inicio de sesión, lo que le permite acceder a información financiera y realizar transacciones no autorizadas.
   2. Un atacante altera los resultados de una elección manipulando los sistemas de votación en línea, lo que socava la confianza en el proceso democrático y elige candidatos incorrectos.
   3. Un empleado resentido copia y comparte información interna y secreta de la empresa con competidores, poniendo en peligro la ventaja competitiva y la propiedad intelectual.
   4. Un corte de energía masivo afecta los centros de datos que alojan servicios en línea cruciales, como sistemas bancarios y comunicaciones.
   5. Un ciberdelincuente ataca una tienda en línea y roba información de tarjetas de crédito de los clientes.
   6. Un hacker accede a los registros médicos electrónicos y modifica los datos de diagnóstico y tratamiento de pacientes, lo que podría conducir a decisiones médicas incorrectas y riesgos para la salud.
   7. Un ransomware se propaga rápidamente por la red de una empresa, cifrando archivos y sistemas y deteniendo las operaciones comerciales hasta que se pague un rescate.
   8. Un proveedor de servicios en la nube experimenta una interrupción importante, lo que afecta a múltiples clientes y hace que sus servicios y aplicaciones sean inaccesibles.
   9. Un estudiante modifica sus calificaciones en la base de datos de la facultad, creando un expediente falso y obteniendo oportunidades académicas indebidas.
   10. Se descubre una alteración de los datos de las transacciones financieras en una base de datos, causando discrepancias y pérdidas financieras para la empresa.
2. Para cada uno de los siguientes escenarios realice lo siguiente:
   1. Identifique las posibles amenazas que podrían afectar.
   2. Proponga las medidas de seguridad activa y pasiva para abordar estas amenazas.

Escenario 1: Confidencialidad en una Empresa Financiera

En una empresa financiera que maneja información altamente confidencial de sus clientes, la confidencialidad es de vital importancia. Los empleados tienen acceso a datos sensibles, como números de cuenta bancaria y detalles de transacciones. Sin embargo, un empleado descuidado podría dejar su computadora desbloqueada mientras se ausenta de su escritorio, lo que podría permitir que otro empleado o incluso un intruso acceda a la información confidencial.

Escenario 2: Integridad de Datos en un Hospital

En un hospital, la integridad de los registros médicos es esencial para garantizar que los diagnósticos y tratamientos sean precisos. Sin embargo, un ataque de ransomware logra infectar el sistema de gestión de registros médicos y cifra los archivos, lo que impide el acceso a la información vital para el cuidado de los pacientes.

Escenario 3: Disponibilidad en una Institución Educativa en Línea

Una institución educativa en línea que ofrece cursos y material de estudio a miles de estudiantes experimenta un ataque de denegación de servicio (DDoS) justo antes de un importante examen en línea. El ataque causa una interrupción en el sitio web de la institución, impidiendo que los estudiantes accedan a los recursos necesarios para el examen.

1. Busque y describa brevemente tres fallos de seguridad ocurridos recientemente. Indique el/los objetivo/s seguridad que fueron afectados.
2. Si necesito tener un 100% de redundancia de información y el factor económico no es un problema ¿Qué tipo de Raid debería usar?
3. Investigue que tipos de Raid seria recomendable usar en una PYME.
4. Busque y describa brevemente las características principales de dos aplicaciones gratis o pagas para realizar backup.
5. Describa el tipo y la periodicidad de backup que realiza en su pc o notebook personal.