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

**INGENIERÍA INFORMÁTICA – LICENCIATURA EN SISTEMAS**

**AUDITORÍA INFORMÁTICA – SEGURIDAD EN SISTEMAS**

**TRABAJO PRÁCTICO Nº 1**

**Fecha de presentación: 10/09/2024**

1. Identifique el/los objetivo/s (parámetro/s) de seguridad que se ven afectados en los siguientes casos. Justifique su respuesta
   1. Un ciberdelincuente accede a las cuentas de correo electrónico de varios usuarios, permitiéndole leer mensajes privados y enviar correos en nombre de las víctimas.
   2. Un fallo en el sistema de autenticación de una aplicación bancaria móvil permite a usuarios no autorizados acceder a cuentas de otros clientes, realizando transacciones y consultas sin restricciones.
   3. Un ex empleado filtra el código fuente de un software propietario a través de internet, poniendo en riesgo la seguridad del producto y afectando la competitividad de la empresa.
   4. Una falla en el sistema de refrigeración de un centro de datos provoca un sobrecalentamiento, lo que interrumpe temporalmente los servicios de múltiples aplicaciones críticas.
   5. Un empleado insatisfecho instala un programa malicioso en la red interna de la empresa, registrando contraseñas y datos confidenciales para obtener acceso no autorizado a sistemas críticos.
   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 proveedor de software distribuye una actualización contaminada con un troyano, permitiendo a los atacantes tomar control de las máquinas que instalan el software comprometido.
   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 usuario descarga un archivo adjunto malicioso que contiene un virus, el cual se propaga por la red corporativa, infectando múltiples estaciones de trabajo y servidores.
   10. Un atacante explota una vulnerabilidad en un sistema de gestión de contenido (CMS) de un sitio web gubernamental, lo que le permite modificar páginas oficiales y publicar información falsa.
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 de Consultoría Legal

En una empresa de consultoría legal, la confidencialidad es crucial debido a la naturaleza sensible de los casos legales manejados. Los abogados y sus asistentes tienen acceso a documentos confidenciales que incluyen estrategias legales, acuerdos y contratos. Sin embargo, un empleado podría inadvertidamente enviar un correo electrónico que contiene documentos sensibles al destinatario equivocado, lo que podría resultar en la exposición de información crítica.

Escenario 2: Integridad de Datos en un Laboratorio de Investigación Científica

En un laboratorio de investigación científica, la integridad de los datos experimentales es fundamental para garantizar la validez de los resultados. Sin embargo, un investigador descontento manipula los datos en un experimento clave antes de su publicación, alterando las conclusiones del estudio y comprometiendo la reputación del laboratorio y la confianza en los resultados científicos.

Escenario 3: Disponibilidad en una Plataforma de Servicios Financieros

Una plataforma en línea que proporciona servicios financieros, como la gestión de inversiones y transacciones bancarias, experimenta un ataque de denegación de servicio (DDoS) durante un pico de actividad en el mercado financiero. El ataque interrumpe el acceso de los usuarios a sus cuentas en un momento crítico, lo que impide la ejecución de transacciones importantes y causa potenciales pérdidas económicas para los clientes.

1. Busque y describa brevemente tres fallos de seguridad ocurridos recientemente. Indique el/los objetivo/s seguridad que fueron afectados.
2. Investigue que tipos de Raid seria recomendable usar en una PYME.
3. Busque y describa brevemente las características principales de dos aplicaciones gratis o pagas para realizar backup.