Asignación 1 — Fundamentos de la Ciberseguridad y Vulnerabilidades (Módulo 1)

Puntos: 20pts
Entrega: 1 PDF con la tabla de análisis y con las preguntas y respuestas. (**NO SOLO CONTESTACIÓN; PREGUNTA Y RESPUESTA EN SU DOCUMENTO**)

Fecha de Entrega: 5 de septiembre de 2025

Nombre del Archivo: *Juan del Pueblo_#estudiante_Asignacion1.**pdf***

Donde Entregar: Favor entregar por el área de mensajes en su blackboard.

Objetivos

- **Definir** ciberseguridad y la **Tríada CIA**.
- **Identificar y clasificar** vulnerabilidades por categoría y por impacto en C/I/A.
- **Aplicar** métricas (escalas) CVSS v3.1 para **estimar** severidad (bajo–crítico).
- **Presentar** recomendaciones a nivel de tratamiento (remediar/mitigar/aceptar).

Caso de uso — Red de la Compañía CyberCorp (12pts)

Durante una revisión de seguridad en la **red de la compañía CyberCorp**, usted como especialista en ciberseguridad encontró las siguientes vulnerabilidades y problemas dentro de dicha red:

1. **2019 — BlueKeep — 0708**

    - Un **servidor de Escritorio Remoto** accesible desde internet tiene el puerto **3389/TCP** abierto y sin medidas de seguridad adicionales.

    - Riesgo: un atacante podría conectarse y tomar control del servidor sin necesidad de credenciales.

2. **2021 — PrintNightmare — 34527**

    - El **servicio de impresión (Print Spooler)** está activo en un **servidor de archivos y en el controlador de dominio**, aunque no se usan para imprimir.

    - Riesgo: un atacante con usuario válido puede aprovechar el servicio y obtener control del sistema.

Tareas del estudiante

1. **Para cada hallazgo llenar la información que se le pida en la siguiente tabla**.

2. **Responde 5 preguntas teóricas** (al final).

Tabla “estilo reporte” — Ejemplo lleno (para guiar)

#	Activo / Ubicación	Vulnerabilidad	Categoría (técnica/lógica/humana)	Impacto C-I-A	Escala CVSS (Ej 0.0 - 10.0)	Recomendación (Remediar / Mitigar / Aceptar)
1						
2						

Justificación de CIA

Favor explicar en que impacta la vulnerabilidad a cada uno de los conceptos de la Triada CIA (Confidencialidad, Integridad y Disponibilidad de Datos).

Preguntas teóricas (8pts)

1. **¿Qué es la seguridad cibernética y cuáles son sus componentes principales (Tríada CIA)?** Incluye 1 ejemplo práctico de C, I y A.

2. **Diferencia entre vulnerabilidad, amenaza y riesgo.** Proporciona un ejemplo breve que las conecte.

3. **CVSS v3.1:** ¿qué miden AV, AC, PR, UI y cómo influyen en el resultado base? Indica los **rangos** Bajo/Medio/Alto/Crítico.

4. **Tratamiento del riesgo:** diferencia **remediar, mitigar, aceptar**; da un ejemplo realista de cada uno.

5. Elige **uno** de tus dos hallazgos. Supón que **parchear tarda 10 días**. Escribe **mínimo 3 oraciones** explicando:
    - **2–3 acciones sencillas** que aplicarías mientras llega el parche (cosas que puedes hacer tú mismo en el equipo/servicio).

    - Cómo esas acciones **mantienen la Disponibilidad** y ayudan a **proteger la Confidencialidad e Integridad** (Tríada CIA).

    - Qué **riesgo residual** quedaría aún con esas acciones temporales.

Nota: Riesgo residual: es el **riesgo que permanece** después de aplicar controles (remediaciones o mitigaciones).