**SAUL HERNANDEZ CASTILLA**

## PARTE 1

## DEFINA CONFIDEBILIDAD, INTEGRIDAD Y DISPONIBILIDAD

**CONFIDEBILIDAD:** Busca garantizar que la información solo esté disponible para las personas autorizadas. Esto es esencial para proteger datos sensibles, como información personal, financiera o médica, y evitar que terceros no autorizados accedan, vean o roben esa información. Para lograrlo, se aplican técnicas como el cifrado, autenticación de usuarios, control de accesos y segmentación de redes. La pérdida de confidencialidad puede tener consecuencias graves, como filtraciones de datos, robo de identidad y sanciones legales.

**INTEGRIDAD**: La integridad asegura que los datos se mantengan precisos, completos y sin alteraciones no autorizadas. Este principio es vital para que la información sea confiable y útil en la toma de decisiones. Si los datos son modificados maliciosamente o por error, pueden generar fraudes, diagnósticos incorrectos o transacciones equivocadas. Para proteger la integridad se utilizan mecanismos como sumas de verificación (hash), firmas digitales, controles de acceso a la edición de datos y registros de auditoría que permitan detectar y revertir cambios no deseados.

**DISPONIBILIDAD:** La disponibilidad se enfoca en asegurar que los sistemas, servicios y datos estén accesibles cuando los usuarios los necesiten. En contextos críticos como la salud o el comercio electrónico, la interrupción de servicios puede causar pérdidas económicas, afectar la atención a pacientes o impedir operaciones comerciales. Para garantizar la disponibilidad se implementan infraestructuras redundantes, respaldos automáticos, sistemas de monitoreo y protección contra amenazas como ataques DDoS o fallas técnicas. Una buena gestión de la disponibilidad es clave para mantener la continuidad operativa y la confianza del usuario

## ¿QUÉ CONCEPTO CONSIDERAS MAS CRITICOS EN UNA EMPRESA DE SALUD?

**DISPONIBILIDAD**: Asegurar que los datos clínicos, historiales, diagnósticos, tratamientos y demás información de los pacientes solo sean accesibles por personal autorizado.

## ¿Y EN UNA EMPRESA DE COMERCIO ELECTRONICO?

**CONFIDEBILIDAD**: Proteger la información de tarjetas de crédito, datos bancarios y las transacciones de los clientes.

## ¿COMO PODRIA PRIORIZAR LA IMPLEMENTACION A UNA EMPRESA CON RECURSOS LIMITADOS?

Es fundamental priorizar la implementación de medidas de ciberseguridad basándose en una evaluación de riesgos clara. Esto significa identificar primero los activos más críticos para el negocio y las amenazas más probables, y luego aplicar medidas que ofrezcan el mayor nivel de protección con el menor costo. Se recomienda comenzar con acciones básicas pero efectivas, como la capacitación del personal, el uso de contraseñas seguras con autenticación de dos factores, la realización de copias de seguridad frecuentes y mantener los sistemas actualizados. De esta forma, la empresa puede construir una base sólida de seguridad y avanzar progresivamente hacia soluciones más complejas, sin comprometer la operatividad ni la sostenibilidad financiera.

# PARTE 2

## 1.VIRUS

- Programa malicioso que se adjunta a archivos o programas legítimos. Un ejemplo sería Cuando se ejecuta el archivo infectado, el virus se activa, se copia y se propaga.

---

## 2. GUSANO

- Malware que se replica a sí mismo y se propaga por redes sin necesidad de adjuntarse a otro archivo, lo podemos ver en propagación automáticamente (por correo, red, USB) y puede saturar redes o instalar otros tipos de malware.

---

## 3. TROYANO

- Parece un programa legítimo, pero esconde funciones maliciosas. Abre una "puerta trasera" para que un atacante controle el equipo o robe información..

---

## 4. RANSOMWARE

- Malware que **cifra (bloquea)** tus archivos o sistema y pide un rescate para liberarlos. Inutiliza tu sistema o datos y exige un pago (usualmente en criptomonedas).

---

## 5. SPYWARE

- Programa que se instala en secreto para espiar tus actividades. Recoge información como contraseñas, hábitos de navegación, correos o mensajes.

# PARTE 3

## Mi Conocimiento Comprueba el Resultado

Share Your Feedback | Print

| Learner Name | Total Score | Completed On |
|---|---|---|
| **Saul Enrique Hernand...** | **68** | **24 Apr 2025** |

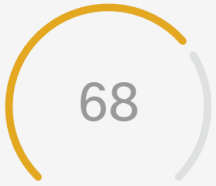
Filter Modules

| MODULE | SCORE | ACHIEVEMENT LEVEL |
|---|---|---|
| Modulo 1: Introducción a la Ciberseguridad | **62** | Intermediate |
| Módulo 2: Ataques, conceptos y técnicas | **73** | Intermediate |
| Módulo 3: Protegiendo sus datos y su priva... | **69** | Intermediate |

My Knowledge Check Result For

**Introducción a Ciberseguridad**

on **24 Apr 2025**




**INTERMEDIATE**

LEARNER

Beginner (<60) | Intermediate (≥60)

Advanced (≥80) | Mastered (≥90)