

ALUMNO: JONATHAN ALEJANDRO RAMIREZ GONZALEZ

MATRÍCULA: 1954

CUATRIMESTRE: NOVENO

CARRERA: LICENCIATURA EN INGENIERIA SISTEMAS COMPUTACIONALES

ASIGNATURA: AUDITORIA DE LA INFORMACIÓN

DOCENTE: ING. MORALES TERRONES JOSÉ CARLOS

FECHA DE ENTREGA: 13/04/2025

# Parte 1: Investigación sobre Seguridad Informática

## 1. ¿Qué es la seguridad informática?

La seguridad informática es el conjunto de prácticas, tecnologías y políticas diseñadas para proteger los sistemas informáticos, redes y datos contra accesos no autorizados, daños o robos. Su objetivo es garantizar que la información se mantenga segura, disponible solo para usuarios autorizados y sin alteraciones.

**Ejemplos de su importancia en empresas actuales:**

1. **Protección de datos de clientes:** Las empresas manejan información sensible como números de tarjetas de crédito o datos personales. Un fallo puede afectar la confianza del cliente.
2. **Evitar pérdidas económicas:** Un ciberataque puede detener operaciones, generar multas o exigir pagos (como en casos de ransomware).
3. **Cumplimiento legal:** Existen leyes como el GDPR o la Ley Federal de Protección de Datos en México que exigen buenas prácticas de seguridad.

## 2. Modelo CID: Confidencialidad, Integridad y Disponibilidad

|  |  |  |
| --- | --- | --- |
| Componente | Descripción | Ejemplo real |
| Confidencialidad | Asegura que solo personas autorizadas accedan a la información. | WhatsApp usa cifrado de extremo a extremo para que solo el emisor y receptor puedan leer los mensajes. |
| Integridad | Garantiza que la información no sea alterada sin autorización. | Los sistemas bancarios verifican transacciones con hash para detectar cambios o fraudes. |
| Disponibilidad | Asegura que los datos estén accesibles cuando se necesiten. | Google Cloud tiene centros de datos replicados para garantizar el acceso constante a la información. |

## 3. Caso real de brecha de seguridad: Ataque a Equifax (2017)

* **Descripción:** La empresa Equifax sufrió una filtración masiva donde se expusieron los datos personales de 147 millones de personas, incluyendo números de seguridad social y fechas de nacimiento.
* **Componentes CID vulnerados:**
  + **Confidencialidad:** Se filtró información personal sensible.
  + **Integridad:** Se teme que algunos datos pudieron haber sido alterados.
  + **Disponibilidad:** Durante la investigación, partes del sistema fueron desconectadas temporalmente.
* **Consecuencias:**
  + Pérdida de confianza de los usuarios.
  + Multas millonarias por incumplimiento de medidas de seguridad.
  + Cambios en la directiva y demandas colectivas.

# Parte 2: Comparación entre Auditoría Informática y Financiera

|  |  |  |
| --- | --- | --- |
| Criterio | Auditoría Informática | Auditoría Financiera |
| Objetivo principal | Evaluar controles de sistemas y datos. | Verificar precisión de estados financieros. |
| Herramientas usadas | Software de análisis de logs, scanners de red. | Software contable (ej: SAP, QuickBooks). |
| Riesgos que detecta | Hackeos, fallos de software, acceso no autorizado. | Fraude, errores contables, malversación. |
| Normas de referencia | ISO 27001, COBIT. | Normas IFRS, GAAP. |

**Pregunta de reflexión (opcional):**

**¿Por qué crees que ambas auditorías son complementarias en una empresa?**  
Porque una asegura la integridad de los sistemas informáticos y la otra la veracidad de los datos contables. Ambas trabajan juntas para garantizar que la información financiera sea confiable y esté protegida contra amenazas tecnológicas.

# Parte 3: Aplicación Práctica

**Escenario:**

*La empresa ‘TechSecure’ sufrió un ataque de phishing. Los hackers accedieron a datos de clientes. No tenían auditorías ni respaldos.*

**1. ¿Qué componentes del modelo CID fallaron?**

* **Confidencialidad:** Se filtraron datos sensibles de los clientes.
* **Disponibilidad:** Al no tener respaldos, podrían haber perdido acceso a la información.
* **Integridad:** Es posible que los datos hayan sido alterados por los atacantes.

**2. ¿Cómo una auditoría informática pudo haber prevenido esto?**

* Habría identificado la falta de capacitación en seguridad del personal (reduciendo el riesgo de phishing).
* Habría detectado la ausencia de respaldos y alertado sobre esa vulnerabilidad.
* Habría revisado los controles de acceso y métodos de autenticación.

**3. Dos medidas correctivas:**

1. **Capacitación periódica en seguridad digital para empleados**, especialmente sobre cómo identificar correos sospechosos y no compartir credenciales.
2. **Implementar respaldos automáticos y en la nube**, para asegurar la recuperación de información en caso de ataque.