# LABORATORIO #2
# DIFERENCIAR ENTRE CONFIDENCIALIDAD INTEGRIDAD Y DISPONIBILIDAD


**PRESENTADO POR:**

**NAYIBE ESTHER ALTAMAR SERRANO**


**EJECUTOR TÉCNICO**
**JUAN SUÁREZ**

**MENTOR**
**ELISEO RODRÍGUEZ**

**CIBERSEGURIDAD – NIVEL BÁSICO**

**TALENTO TECH - UNIVERSIDAD LIBRE**

**JUNIO - 2025**

## OBJETIVOS DEL LABORATORIO

1. Comprender y definir los principios fundamentales de la ciberseguridad (Confidencialidad, Integridad y Disponibilidad)

2. Aplicar los conceptos de Confidencialidad, Integridad y Disponibilidad a escenarios prácticos

3. Analizar y diferenciar los impactos de las brechas en Confidencialidad, Integridad y Disponibilidad

## ESTRUCTURA DEL LABORATORIO

### I. Paso 1: Definir los Términos Claves: Confidencialidad, Integridad y Disponibilidad

**Confidencialidad:**

**Definición:** Explica que la confidencialidad se refiere a la protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella. Es uno de los pilares fundamentales de la seguridad de la información.

**Conceptos Relacionados:** Incluye el cifrado, controles de acceso, y autenticación como métodos para garantizar la confidencialidad

**Integridad:**

**Definición:** Define la integridad como la protección contra la modificación no autorizada de datos. La integridad asegura que la información es confiable y que no ha sido alterada o manipulada.

**Conceptos Relacionados:** Menciona el uso de sumas de verificación (hashes), firmas digitales y controles de versiones como métodos para asegurar la integridad.

**Disponibilidad**

**Definición:** Explica que la disponibilidad garantiza que la información y los recursos estén accesibles a los usuarios autorizados cuando lo necesiten. Esto implica que los sistemas sean robustos y que estén disponibles incluso ante fallos o ataques.

**Conceptos Relacionados:** Discute la redundancia, los sistemas de respaldo, y la planificación ante desastres como formas de garantizar la disponibilidad.

**Resultados Esperados:**

Al final de este paso, los participantes deben tener una comprensión clara de los términos y estar preparados para aplicar estos conceptos en ejemplos prácticos.

## II. Paso 2: Proporcionar y Analizar Ejemplos Prácticos

**Ejemplo de Confidencialidad**

**Contexto:** Explicar cómo una empresa de salud maneja los registros médicos de los pacientes.

**Aplicación Práctica:** Describa cómo se utiliza el cifrado para proteger la información sensible, asegurando que solo el personal médico autorizado pueda acceder a estos datos.

**Discusión:** Pregunta a los participantes qué otros métodos podrían usarse para garantizar la confidencialidad de los datos en este contexto (por ejemplo, autenticación multifactorial).

**Ejemplo de Integridad:**

**Contexto:** Explica cómo una empresa de software distribuye sus productos a los clientes.

**Aplicación Práctica:** Detalla cómo se utilizan sumas de verificación (hashes) para verificar que los archivos de instalación no han sido alterados durante la descarga.

**Discusión:** Solicita a los participantes que piensen en qué podría suceder si la integridad no estuviera asegurada (por ejemplo, software malicioso podría ser introducido sin que el usuario lo sepa).

**Ejemplo de Disponibilidad**

**Contexto:** Describe cómo un banco gestiona sus servicios en línea.

**Aplicación Práctica:** Explica cómo el banco implementa servidores redundantes y sistemas de respaldo para asegurar que sus servicios en línea estén disponibles incluso durante fallos de hardware.

**Discusión:** Pide a los participantes que discutan las implicaciones de la falta de disponibilidad para un banco, y cómo podría afectar a los clientes y la reputación de la entidad.

**Resultados Esperados:** Los participantes deben ser capaces de asociar cada concepto (Confidencialidad, Integridad, Disponibilidad) con un ejemplo práctico, entendiendo cómo se aplican en diferentes contextos.

## III. Paso 3: Reflexión y Comparación de Conceptos

### Análisis Comparativos

**Actividad:** Pide a los participantes que comparen los tres conceptos, reflexionando sobre cómo se complementan entre sí en un sistema de seguridad completo. Por ejemplo, cómo un fallo en la confidencialidad podría comprometer la integridad, o cómo la falta de disponibilidad puede afectar la integridad de los datos.

### Preguntas de Reflexión:

- ¿Qué concepto consideras más crítico en el contexto de una empresa de salud ¿Y en una empresa de comercio electrónico
- ¿Cómo podrías priorizar la implementación de estos conceptos en una organización con recursos limitados

### Conclusión del Laboratorio

- Resuma cómo la confidencialidad, integridad y disponibilidad trabajan juntas para proteger la información y los sistemas.
- Destaca la importancia de implementar medidas que aseguren los tres aspectos para una ciberseguridad efectiva.

# DESARROLLO DE LA ACTIVIDAD # 2

## Laboratorio: Confidencialidad, Integridad y Disponibilidad (Modelo CID)

### Definición de Términos Claves

1. **Confidencialidad**

La confidencialidad garantiza que la información solo sea accesible por las personas autorizadas, impidiendo el acceso no autorizado a datos sensibles.

**Ejemplo: Empresa del Sector Salud**

Una Empresa del sector salud protege los registros médicos de sus pacientes restringiendo el acceso solo a profesionales autorizados mediante sistemas de autenticación biométrica y permisos basados en roles.

**Aplicación práctica – Cifrado:**

Se utiliza cifrado de extremo a extremo para proteger los datos de los pacientes. De este modo, incluso si se intercepta la información durante una transmisión o si ocurre una brecha de seguridad, los datos no podrán ser leídos sin la clave correcta.

**Integridad**

La **integridad** asegura que los datos se mantengan **exactos, completos y sin modificaciones no autorizadas** durante su almacenamiento, procesamiento o transmisión.

**Ejemplo en software:**

Una empresa de software garantiza la **integridad** de sus productos distribuyendo archivos con **sumas de verificación (hashes)** como SHA-256. El cliente puede verificar que el archivo descargado es idéntico al original y que no ha sido corrompido o alterado por terceros.

**Aplicación práctica – Hashing:**

Al generar un hash único para cada archivo, cualquier alteración accidental o maliciosa del archivo durante la descarga será detectada inmediatamente, evitando instalaciones comprometidas.

**Disponibilidad**

La **disponibilidad** asegura que los datos y sistemas estén **accesibles cuando se necesitan**, incluso en caso de fallas o ataques.

**Ejemplo en banco:**

Un banco que ofrece servicios en línea implementa **servidores redundantes**, **sistemas de respaldo automático** y **equilibradores de carga** para garantizar que sus clientes puedan acceder a sus cuentas en cualquier momento, sin interrupciones.

**Aplicación práctica – Alta disponibilidad:**

Gracias a infraestructuras distribuidas, si un servidor falla, otro toma su lugar sin interrumpir el servicio. Esto protege tanto la reputación como la continuidad operativa del banco.

## Aplicar los conceptos de Confidencialidad, Integridad y Disponibilidad a escenarios prácticos

### 1. Confidencialidad

**Definición:** Garantizar que solo las personas autorizadas tengan acceso a la información.

- **Escenario práctico:**

Una **clínica médica virtual** implementa un sistema de autenticación de dos factores para que solo los médicos autorizados puedan acceder al historial clínico de los pacientes.

**Medidas técnicas:**

- Cifrado de datos en tránsito y en reposo.
- Accesos controlados por roles.
- Políticas de contraseñas fuertes.

## 2. Integridad

**Definición:** Asegurar que los datos no sean modificados de forma no autorizada o accidental.

- **Escenario práctico:**

Una empresa de software educativo envía actualizaciones de su sistema a estudiantes y docentes. Para asegurarse de que no se alteren los archivos, se incluyen hashes que los usuarios pueden verificar.

**Medidas técnicas:**

- Hashes como SHA-256 para validar archivos.
- Control de versiones.
- Registro de auditoría (logs).

## 3. Disponibilidad

**Definición:** Asegurar que los sistemas y datos estén accesibles cuando se necesiten.

**Escenario práctico:**

Una institución educativa virtual asegura que su plataforma de matrícula esté siempre en línea durante los periodos de inscripción. Para ello, utiliza servidores en la nube con redundancia y realiza respaldos automáticos diarios.

**Medidas técnicas:**

- Sistemas de respaldo.
- Redundancia de servidores (alta disponibilidad).
- Protección contra ataques DDoS.

**Relación entre los tres conceptos**

- Un fallo en la **confidencialidad** (ej. fuga de datos) puede poner en riesgo la **integridad** (modificación maliciosa).

- Una pérdida de **disponibilidad** (caída del sistema) impide validar la **integridad** de los datos.
- Un sistema seguro necesita equilibrio entre los tres pilares para ser confiable y robusto.

**Comparación y Reflexión**

| Concepto | Objetivo | Riesgo si falla | Tecnologías asociadas |
|---|---|---|---|
| **Confidencialidad** | Prevenir acceso no autorizado | Fugas de información, violación de privacidad | Cifrado, autenticación, firewalls |
| **Integridad** | Garantizar datos correctos | Manipulación de datos, errores operativos | Hashing, firmas digitales |
| **Disponibilidad** | Asegurar acceso continuo a servicios | Caídas de servicio, pérdida de productividad | Redundancia, backups, cloud infra |

**Interdependencia:**

Estos tres conceptos se **complementan** entre sí. Por ejemplo:

- Si la **confidencialidad** se ve comprometida (ej. datos expuestos), un atacante podría alterar información crítica, afectando también la **integridad**.
- Si los sistemas no están disponibles (fallo en la **disponibilidad**), los usuarios no pueden verificar ni corregir los datos, afectando la **integridad**.
- Un fallo en la **integridad** (datos corruptos) podría dañar permanentemente información confidencial.

## Conclusión del Laboratorio

La **confidencialidad, integridad y disponibilidad** forman la base del modelo de seguridad de la información. Trabajan en conjunto para proteger datos sensibles y sistemas de manera integral:

- **Confidencialidad** evita el acceso no autorizado.
- **Integridad** asegura que los datos no sean manipulados.
- **Disponibilidad** garantiza el acceso constante y seguro.

Sin medidas que aborden los tres aspectos, un sistema de información será vulnerable. Por tanto, implementar estrategias balanceadas, incluso con recursos limitados, es vital para mantener una **ciberseguridad efectiva**.

## Referencias y Recursos


- Cisco Networking Academy – *Cybersecurity Essentials* https://skillsforall.com/course/cybersecurity-essentials
- GitHub – *Repositorio para prácticas de ciberseguridad* https://github.com