Módulo 4: Servicios y Seguridad en las Redes

Lección 4: Importancia del Cifrado en Redes de Comunicación

Objetivos de la Lección

- Explicar qué es el cifrado y por qué es esencial en las redes de comunicación de computadoras.
- Distinguir entre el cifrado de datos en tránsito y el cifrado de datos en reposo (almacenamiento).
- Aplicar conceptos de cifrado para proteger la confidencialidad e integridad de la información en redes locales y externas.

Introducción de la Lección

Cada día, millones de datos viajan por las redes: correos electrónicos, contraseñas, números de tarjetas, documentos confidenciales. En este entorno digital, garantizar que la información no pueda ser leída o alterada por personas no autorizadas es fundamental. Aquí entra en juego el **cifrado (o encriptación)**, una de las herramientas más poderosas para mantener segura la comunicación y el almacenamiento de datos en las redes de computadoras.

En esta lección explicaremos cómo funciona el cifrado, sus tipos más comunes, y cómo se aplica tanto al transmitir información como al almacenarla. Entender estos mecanismos permite proteger la privacidad, mantener la integridad de los datos y evitar accesos no autorizados, especialmente en redes públicas o entornos empresariales.

Cifrado en Redes de Comunicación

El cifrado transforma datos legibles en un formato codificado (texto cifrado) que solo puede ser entendido si se posee la clave adecuada para descifrarlo. Esto asegura que, aunque los datos sean interceptados, no puedan ser comprendidos ni manipulados.

1. Cifrado de Datos en Tránsito

- **Definición:** Protección de los datos mientras se transmiten de un punto a otro a través de la red.
- **Ejemplos:** Navegación HTTPS, uso de VPN, correos cifrados, VoIP cifrada.
- **Herramientas comunes:** SSL/TLS, IPsec, SSH.
- **Ventaja principal:** Evita que terceros (ataques de tipo “man-in-the-middle”) puedan leer o alterar los datos durante su envío.

2. Cifrado de Punto a Punto (End-to-End Encryption)

- **Aplicación:** Usado en aplicaciones de mensajería y videollamadas como WhatsApp o Signal.
- **Beneficio:** Solo el emisor y el receptor tienen acceso a la información, ni siquiera el proveedor del servicio puede verla.

Cifrado de Datos en Reposo (Almacenados)

Además del cifrado durante la transmisión, los datos también deben estar protegidos mientras se almacenan en servidores, discos duros, o dispositivos móviles.

1. Cifrado de Archivos y Discos

- **Ejemplo:** BitLocker (Windows), FileVault (macOS), cifrado en Android/iOS.

- **Aplicación:** Protege los datos incluso si el dispositivo es robado o comprometido físicamente.

2. Bases de Datos Cifradas

- **Uso común:** En servicios bancarios, salud, y comercio electrónico.
- **Ventaja:** Protege la integridad y privacidad de la información confidencial almacenada.

3. Cifrado en la Nube

- **Importancia:** Asegura que la información guardada en servicios como Google Drive, Dropbox o AWS esté protegida.
- **Cifrado del lado del cliente:** Los datos se cifran antes de enviarse a la nube, aumentando el control del usuario sobre la seguridad.

Tipos de Cifrado Comúnmente Usados

Tipo de Cifrado	Descripción	Uso
Simétrico (ej. AES)	Usa una sola clave para cifrar y descifrar.	Rápido, usado en comunicaciones internas y discos duros.
Asimétrico (ej. RSA)	Usa un par de claves: una pública y una privada.	Intercambio de claves, firma digital, SSL/TLS.
Hashing (ej. SHA-256)	No es reversible, usado para verificar integridad.	Contraseñas, integridad de archivos.

Importancia del Cifrado en la Seguridad de Redes

1. **Confidencialidad:** Solo los usuarios autorizados pueden leer los datos.
2. **Integridad:** Asegura que los datos no sean modificados sin autorización.
3. **Autenticación:** Mediante certificados digitales, permite confirmar la identidad de los usuarios o dispositivos.
4. **Cumplimiento Legal:** Muchas normativas (como GDPR, HIPAA) exigen cifrado para proteger datos personales o sensibles.

Relación con Otros Conceptos de Seguridad

- **VPN y Cifrado:** Una VPN cifra toda la conexión del usuario con la red, protegiendo incluso en redes públicas.
- **Firewalls y Cifrado:** Aunque los firewalls controlan el acceso, el cifrado garantiza que la información esté protegida incluso si un atacante logra entrar.
- **IDS/HIDS:** Detectan actividad sospechosa, pero el cifrado evita que la información comprometida sea útil para el atacante.

Resumen de la Lección

El cifrado es un pilar fundamental en la seguridad de redes de comunicación. Protege tanto los datos que viajan por la red como los que permanecen almacenados, asegurando confidencialidad, integridad y cumplimiento con normativas de protección de datos. Conocer sus tipos, aplicaciones y beneficios permite diseñar redes más seguras, resilientes y confiables.

Actividad de la Lección

Esta actividad te permitirá comprender y aplicar los conceptos de cifrado en redes, tanto en la comunicación como en el almacenamiento de datos.

Instrucciones:

1. **Análisis de Caso:**
    - Imagina que eres el encargado de proteger los datos de una empresa que trabaja con clientes a través de internet.
    - Explica cómo aplicarías el cifrado en:
        - Las comunicaciones con los clientes.
        - El almacenamiento de la información en servidores internos o en la nube.
2. **Comparación de Tipos de Cifrado:**
    - Realiza una tabla comparativa entre cifrado simétrico, asimétrico y hashing.
    - Incluye ejemplos reales de herramientas o protocolos que usen cada tipo.
3. **Diseño de Red Segura con Cifrado:**
    - Dibuja un esquema simple de red que incluya componentes como firewall, VPN, y bases de datos cifradas.
    - Explica cómo cada componente ayuda a proteger los datos.
4. **Entrega de la Actividad:**
    - Presenta un informe en formato PDF que incluya tus respuestas, la tabla comparativa y el diagrama propuesto.
    - Entrega el documento en el espacio asignado por el profesor.