Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Controles para la Seguridad de las Comunicaciones

Presentación del tema

Los controles para la seguridad de las comunicaciones comprenden el conjunto de mecanismos técnicos, administrativos y organizacionales destinados a proteger la transmisión de información entre sistemas, redes, dispositivos y usuarios. En las Tecnologías de la Información (IT), las comunicaciones son el tejido conectivo que vincula componentes del sistema: si los datos en reposo pueden protegerse con cifrado de almacenamiento, los datos en tránsito requieren mecanismos específicos que aseguren su confidencialidad, integridad y disponibilidad durante la transmisión.

Para los estudiantes de la Licenciatura en Administración, comprender la seguridad de las comunicaciones implica reconocer que la información no solo es vulnerable cuando está almacenada, sino también cuando circula por redes internas y externas. Un ataque de interceptación puede comprometer transacciones financieras, credenciales de acceso, datos personales o comunicaciones estratégicas sin que los participantes lo adviertan.

Amenazas específicas a las comunicaciones

Las comunicaciones enfrentan amenazas particulares. Los ataques de intermediario (Man-in-the-Middle, MitM) interceptan la comunicación entre dos partes sin que ninguna lo detecte. Los ataques de escucha pasiva (Eavesdropping) capturan datos transmitidos en redes sin cifrar. La denegación de servicio (DoS/DDoS) interrumpe la disponibilidad de los canales de comunicación. La suplantación de identidad (Spoofing) falsifica la identidad del remitente o del destino. Las inyecciones de tráfico malicioso alteran los datos durante la transmisión.

Estas amenazas impactan directamente sobre la triada CIA: comprometen la confidencialidad al exponer datos en tránsito, la integridad al alterar la información y la disponibilidad al bloquear canales.

Controles técnicos de las comunicaciones

Cifrado en tránsito. Los protocolos SSL/TLS (Secure Sockets Layer / Transport Layer Security) cifran la información transmitida por redes, garantizando que aunque sea interceptada resulte ilegible. HTTPS es la implementación más conocida en entornos web.

Redes privadas virtuales (VPN). Establecen túneles cifrados sobre redes públicas, permitiendo el acceso remoto seguro y la conexión entre sucursales. Son especialmente relevantes en entornos de teletrabajo.

Segmentación y microsegmentación de red. Las VLAN (Virtual Local Area Network) dividen la red en segmentos lógicos, limitando la propagación de ataques. La microsegmentación, propia del modelo Zero Trust, aísla flujos de comunicación entre sistemas.

Firewalls y sistemas de detección de intrusiones. Los firewalls controlan el tráfico entrante y saliente según reglas de seguridad. Los IDS (Intrusion Detection Systems) y los IPS (Intrusion Prevention Systems) detectan y bloquean patrones de tráfico malicioso.

Protocolos seguros de comunicación. SSH (Secure Shell) reemplaza protocolos inseguros como Telnet para la administración remota de servidores. SFTP y FTPS protegen la transferencia de archivos. S/MIME y PGP cifran comunicaciones por correo electrónico.

Controles administrativos y de gobernanza

Los controles administrativos complementan los técnicos mediante políticas de uso aceptable de redes, procedimientos para el manejo de información confidencial en comunicaciones, acuerdos de no divulgación (NDA) con proveedores y empleados, y revisiones periódicas de la arquitectura de red. La gestión de cambios en infraestructura de comunicaciones debe seguir procesos formales para evitar configuraciones inseguras.

El monitoreo continuo de las comunicaciones mediante SIEM permite detectar comportamientos anómalos, volúmenes inusuales de tráfico y conexiones a destinos no autorizados. La trazabilidad de las comunicaciones críticas es un requisito de gobernanza en organizaciones reguladas.

Conceptos clave

- Las comunicaciones como vector de ataque específico que requiere controles propios.
- Cifrado en tránsito mediante SSL/TLS como mecanismo esencial de protección.
- VPN para comunicaciones remotas seguras.
- Firewalls, IDS e IPS como controles activos del tráfico de red.
- Segmentación y microsegmentación para limitar la propagación de ataques.
- Ataques MitM y Eavesdropping como amenazas específicas de las comunicaciones.

Preguntas de repaso del tema

1. ¿Por qué las comunicaciones representan un vector de ataque específico diferente al almacenamiento?
2. ¿Qué es un ataque Man-in-the-Middle y cómo puede prevenirse?
3. ¿Por qué el cifrado SSL/TLS es esencial en las comunicaciones organizacionales?
4. ¿Qué diferencia existe entre un IDS y un IPS?
5. ¿Cómo contribuye la segmentación de red a la reducción del riesgo de comunicaciones?
6. ¿Qué función cumple una VPN en entornos de teletrabajo?

7. ¿Por qué los protocolos de administración remota no cifrados como Telnet representan un riesgo?
8. ¿Cómo se integra el monitoreo de comunicaciones con la gobernanza de TI?
9. ¿Qué controles administrativos complementan los controles técnicos en comunicaciones?
10. ¿Por qué la seguridad de las comunicaciones impacta en la triada CIA?