

Universidad Politécnica de San Luis Potosí

Materia:
Seguridad Informática

Octavo Semestre

Profesor:
Servando López Contreras

Alumna:
América Fabiola Guerra Ramírez - 179884

Tarea: Análisis de servicios de seguridad
(X.800 y RFC 4949)

Fecha de entrega: 27 de enero de 2026

Introducción

La seguridad informática es esencial para proteger la información frente a incidentes cada vez más frecuentes y complejos. En esta tarea se analizarán distintos escenarios de seguridad aplicando los servicios definidos en el ITU-T X.800 y utilizando la terminología estandarizada del RFC 4949. El objetivo es identificar las vulneraciones presentes, comprender la relación entre los servicios de seguridad comprometidos y describir técnicamente las amenazas y ataques, fortaleciendo así el análisis y la documentación de incidentes en contextos reales.

Escenario	Servicios X.800 comprometidos	Definición(es) aplicable(s) RFC 4949.	Tipo de amenaza	Vector de ataque.	Impacto técnico / operativo	Medida de control recomendada.
1	Confidencialidad, Integridad y Disponibilidad.	Multi-stage attack, Data Breach, Availability Attack.	Externa	Inyección de Ransomware tras acceso inicial no autorizado.	Interrupción de servicios críticos y exposición de datos sensibles.	Respaldos inmutables y segmentación de red.
2	Confidencialidad y Control de Acceso.	Misconfiguration, Exposure, Data Leak.	Interna	Error humano en configuración de permisos en la nube.	Exposición pública de bases de datos y sanciones legales.	CSPM (Cloud Security Posture Management) y auditorías.
3	Integridad y Autenticación.	Supply Chain Attack, Malicious Code, Trust Relationship.	Externa	Compromiso de actualización de software de un tercero.	Ruptura de la cadena de confianza y compromiso masivo.	Análisis de composición de software (SCA) y firmas digitales.
4	Autenticación y Control de Acceso.	Credential Compromise, Masquerade, Phishing.	Externa	Ingeniería social para robo de credenciales legítimas.	Persistencia del atacante y acceso lateral inadvertido.	MFA (Autenticación Multi-Factor) y monitoreo UEBA.
5	Disponibilidad e Integridad.	Data Destruction, Availability Attack, Backup Integrity.	Externa	Cifrado y eliminación activa de copias de seguridad.	Incapacidad total de recuperación ante desastres.	Respaldos "Air-gapped" y políticas de Object Lock.
6	Confidencialidad y Control de Acceso.	Insider Threat, Privilege Abuse, Data Theft.	Interna	Abuso de privilegios por empleado con acceso legítimo.	Robo de propiedad intelectual y fuga de información.	Principio de mínimo privilegio (PoLP) y herramientas DLP.

7	Integridad y No Repudio.	Audit Trail, Evidentiary Integrity, Tampering.	Externa	Alteración o borrado de registros (logs) del sistema.	Imposibilidad de reconstrucción forense y nulidad legal.	Logs centralizados en SIEM y almacenamiento WORM.
8	Disponibilidad.	Operational Failure, System Outage, Human Error.	Internia	Aplicación de actualización fallida sin pruebas previas.	Caída global de servicios y pérdida de ingresos.	Gestión de cambios (Change Management) y entornos Staging.
9	Autenticación y Confidencialidad.	Phishing, Spoofing, Social Engineering.	Externa	Suplantación de identidad mediante sitios web clonados.	Robo de datos personales y daño a la reputación oficial.	Protocolos DMARC/SPF y concientización de usuarios.
10	Confidencialidad, Integridad y Disponibilidad.	Destructive Attack, Intrusion, Data Wiping.	Externa	Exfiltración seguida de borrado masivo de sistemas.	Destrucción irreversible de la infraestructura tecnológica.	Plan de Respuesta a Incidentes (IRP) y detección IDS activa.

Análisis de Impacto y Medidas de Control

En estos 10 escenarios, queda claro que la seguridad no es solo que "no se caiga la página", sino proteger todo el flujo de información.

Ataques de Ransomware y Destrucción (Escenarios 01, 05 y 10): Cuando grupos como LockBit entran, no solo cifran archivos; hacen un desastre en etapas. Primero roban datos y luego bloquean todo. El impacto es que la empresa se detiene por completo y puede hasta quebrar si no tiene cómo recuperar sus datos. La mejor defensa aquí no es solo un antivirus, sino tener respaldos.

El Factor Humano y las Identidades (Escenarios 04 y 09): Aquí el atacante solo necesitó convencer a alguien de dar su contraseña mediante phishing. Esto es peligroso porque el atacante pudo obtener acceso con llaves legítimas. Para evitar esto, lo más sencillo y efectivo es obligar a usar autenticación de dos factores (2FA), sobre todo, para que no caiga en trampas.

Errores Internos y Configuración (Escenarios 02 y 08): Aprendimos que no siempre hay un "malo" afuera; a veces nosotros mismos dejamos la base de datos abierta por un error de configuración. El impacto es legal y reputacional, porque la gente pierde la confianza. La solución es usar herramientas que revisen automáticamente la configuración en la nube y nunca hacer cambios sin probarlos antes en un entorno seguro.

Traiciones y Proveedores (Escenarios 03 y 06): Es el peor de los casos: cuando un empleado roba información o un software en el que confiamos viene con muchas consecuencias. Aquí

el impacto es la pérdida de información importante de la empresa. La medida clave es el Mínimo Privilegio: que nadie tenga acceso a más de lo que estrictamente necesita para trabajar.

Borrando Huellas (Escenario 07): Si un atacante borra los registros de actividad, será muy difícil encontrarlo. No podemos saber quién entró ni qué se llevó, lo que arruina cualquier investigación legal. Para evitar esto, los registros deben mandarse a un servidor externo donde solo se puedan escribir y nunca borrar.

Conclusión

El análisis de incidentes de seguridad informática mediante los servicios definidos en el ITU-T X.800 y la terminología del RFC 4949 permite comprender de forma estructurada cómo se producen y afectan las vulneraciones de seguridad en escenarios reales. La aplicación conjunta de ambos marcos facilita una descripción técnica precisa, mejora la comunicación profesional y fortalece la capacidad para identificar, explicar y documentar adecuadamente los incidentes, contribuyendo a una visión integral de la seguridad de la información.

Referencias

- ITU: CONNECTING THE WORLD AND BEYOND. (S. F.). ITU.
<HTTPS://WWW.ITU.INT/ES/PAGES/DEFAULT.ASPX#/ES>
- RFC 4949: INTERNET SECURITY GLOSSARY, VERSION 2. (S. F.). IETF DATatracker.
<HTTPS://DATATRACKER.IETF.ORG/DOC/HTML/RFC4949>