UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 02

Análisis de servicios de seguridad

ITU-T X.800 y RFC 4949

Alumno:
Erik De La Rosa Rodríguez
Matrícula: 177700

Asignatura:
CNG V: Seguridad informatica

Docente:
Mtro. Servando López Contreras

San Luis Potosí, S.L.P.
28 de enero de 2026

1. Introducción y contexto del ITU-T X.800 y el RFC 4949

La seguridad informática moderna requiere marcos conceptuales claros que permitan analizar, comunicar y documentar incidentes de manera estructurada. En este contexto, la recomendación ITU-T X.800 y el RFC 4949 representan dos referencias fundamentales que, aunque tienen propósitos distintos, se complementan de forma directa en el análisis de la seguridad de los sistemas de información.

El estándar ITU-T X.800, publicado por la Unión Internacional de Telecomunicaciones, surge como una extensión del modelo OSI con el objetivo de integrar la seguridad como un componente transversal en las comunicaciones entre sistemas. Su principal aportación es la definición de seis servicios de seguridad: autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad. Estos servicios permiten identificar qué propiedad de seguridad ha sido comprometida en un incidente, independientemente de la tecnología o plataforma involucrada.

Por otro lado, el RFC 4949, emitido por la Internet Engineering Task Force (IETF), no define mecanismos técnicos ni controles específicos, sino que funciona como un glosario oficial de seguridad informática. Este documento establece una terminología estandarizada para describir amenazas, vulnerabilidades, ataques e impactos, lo que resulta esencial para la comunicación técnica precisa entre profesionales del área.

La relación entre ambos marcos es complementaria: mientras que el ITU-T X.800 permite analizar *qué servicio de seguridad fue afectado*, el RFC 4949 facilita describir *cómo ocurrió el incidente* y *qué tipo de amenaza o ataque estuvo involucrado*. En conjunto, ambos estándares proporcionan una base sólida para el análisis técnico, la documentación profesional y la toma de decisiones en materia de seguridad informática actual, especialmente en escenarios reales donde convergen factores técnicos, humanos y organizacionales.

2. Análisis de escenarios de seguridad

Escenario 01: Ransomware con exfiltración de datos

Servicios X.800 comprometidos: Confidencialidad, Integridad, Disponibilidad.

Definiciones RFC 4949 aplicables: Multi-stage attack, Data breach, Availability attack.

Tipo de amenaza: Externa.

Vector de ataque: Acceso inicial no autorizado seguido de ejecución de ransomware y exfiltración de información.

Impacto técnico y operativo: Pérdida total de acceso a sistemas críticos, exposición de información sensible y afectación a la continuidad operativa.

Medidas de control recomendadas: Respaldos inmutables, detección temprana, segmentación de red y respuesta a incidentes.

Escenario 02: Bases de datos expuestas por mala configuración

Servicios X.800 comprometidos: Confidencialidad, Control de acceso.

Definiciones RFC 4949 aplicables: Misconfiguration, Exposure.

Tipo de amenaza: Interna por error de configuración.

Vector de ataque: Acceso público no intencionado a servicios en la nube.

Impacto técnico y operativo: Exposición de datos con consecuencias legales y reputacionales.

Medidas de control recomendadas: Revisión de configuraciones, principio de mínimo privilegio y auditorías periódicas.

Escenario 03: Ataque a la cadena de suministro

Servicios X.800 comprometidos: Integridad, Confidencialidad.

Definiciones RFC 4949 aplicables: Supply chain attack.

Tipo de amenaza: Externa.

Vector de ataque: Distribución de actualizaciones con código malicioso.

Impacto técnico y operativo: Compromiso masivo de sistemas confiables.

Medidas de control recomendadas: Validación de firmas, monitoreo de comportamiento y evaluación de proveedores.

Escenario 04: Phishing con robo de credenciales

Servicios X.800 comprometidos: Autenticación, Control de acceso.

Definiciones RFC 4949 aplicables: Credential compromise, Authentication failure.

Tipo de amenaza: Externa mediante ingeniería social.

Vector de ataque: Phishing.

Impacto técnico y operativo: Acceso persistente no autorizado.

Medidas de control recomendadas: MFA, concientización y monitoreo de comportamiento.

Escenario 05: Eliminación de respaldos

Servicios X.800 comprometidos: Disponibilidad, Integridad.

Definiciones RFC 4949 aplicables: Data destruction, Availability attack.

Tipo de amenaza: Externa.

Vector de ataque: Compromiso previo y eliminación de respaldos.

Impacto técnico y operativo: Imposibilidad de recuperación.

Medidas de control recomendadas: Backups offline e inmutables.

Escenario 06: Amenaza interna

Servicios X.800 comprometidos: Confidencialidad, Control de acceso.

Definiciones RFC 4949 aplicables: Insider threat.

Tipo de amenaza: Interna.

Vector de ataque: Abuso de privilegios legítimos.

Impacto técnico y operativo: Fuga de información sensible.

Medidas de control recomendadas: Mínimo privilegio y monitoreo de accesos.

Escenario 07: Alteración de registros

Servicios X.800 comprometidos: Integridad, No repudio.

Definiciones RFC 4949 aplicables: Evidentiary integrity, Audit trail compromise.

Impacto técnico y legal: Imposibilidad de reconstruir eventos.

Medidas de control recomendadas: Registros inmutables y monitoreo centralizado.

Escenario 08: Fallo operativo

Servicios X.800 comprometidos: Disponibilidad.
Definiciones RFC 4949 aplicables: Operational failure.
Impacto técnico y operativo: Interrupción global de servicios.
Medidas de control recomendadas: Pruebas previas y planes de reversión.

Escenario 09: Suplantación de identidad

Servicios X.800 comprometidos: Autenticación, Confidencialidad.
Definiciones RFC 4949 aplicables: Masquerade, Phishing.
Impacto técnico y operativo: Robo de información de usuarios.
Medidas de control recomendadas: SPF, DKIM, DMARC y concientización.

Escenario 10: Ataque destructivo

Servicios X.800 comprometidos: Confidencialidad, Integridad, Disponibilidad.
Definiciones RFC 4949 aplicables: Destructive attack.
Impacto técnico y operativo: Daño irreversible.
Medidas de control recomendadas: Detección temprana y respuesta inmediata.

3. Conclusiones

El análisis de los escenarios demuestra que los servicios de seguridad definidos en el ITU-T X.800 siguen siendo vigentes para identificar qué propiedades fundamentales han sido comprometidas en incidentes reales. Asimismo, el RFC 4949 permite describir estos eventos con un lenguaje técnico preciso y estandarizado, evitando ambigüedades en la comunicación profesional.

La combinación de ambos marcos fortalece la capacidad del analista para documentar incidentes, proponer controles adecuados y comprender que la seguridad informática no depende únicamente de ataques externos sofisticados, sino también de errores humanos, fallas operativas y amenazas internas, aspectos especialmente relevantes en el contexto latinoamericano.

4. Referencias

- https://www.itu.int/rec/T-REC-X.800
- https://datatracker.ietf.org/doc/html/rfc4949