27 DE ENERO DE 2026

ANÁLISIS DE SERVICIOS DE SEGURIDAD (X.800 Y RFC 4949)

CAROL ELIZABETH CORTES BELTRAN
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Contenido

Introducción

En el ámbito de la seguridad informática, la capacidad de analizar incidentes de manera estructurada y con terminología precisa es una competencia fundamental para cualquier profesional. Este análisis se sustenta en dos pilares normativos esenciales: la **Recomendación ITU-T X.800**, que establece una arquitectura de seguridad y define seis servicios fundamentales para proteger las comunicaciones, y el **RFC 4949** de la IETF, que sirve como el glosario de referencia para la terminología técnica en seguridad de redes. La integración de ambos marcos proporciona una metodología robusta para descomponer eventos complejos, identificar fallas de seguridad y comunicar hallazgos de manera estandarizada.

La presente actividad tiene como objetivo aplicar estos marcos al análisis de diez escenarios de incidentes realistas y representativos de las principales amenazas contemporáneas. Estos escenarios abarcan un espectro amplio de tácticas, técnicas y procedimientos utilizados por actores maliciosos, y serán examinados a través de la lente de los servicios X.800 y la terminología del RFC 4949. Los casos incluyen desde ataques de ransomware avanzado y compromiso de la cadena de suministro, hasta amenazas internas, exposición de datos por mala configuración y ataques destructivos con exfiltración. Cada escenario presenta desafíos específicos que ponen a prueba diferentes combinaciones de los servicios de seguridad, como la Autenticación, el Control de Acceso, la Confidencialidad, la Integridad, el No Repudio y la Disponibilidad.

A través del análisis minucioso de estos casos, el estudiante no solo identificará los servicios de seguridad vulnerados, sino que también aprenderá a emplear la terminología correcta —como *multi-stage attack*, *data breach*, *misconfiguration* o *destructive attack*— para describir los mecanismos y el impacto de cada incidente. Este ejercicio pretende cerrar la brecha entre la teoría de los estándares y la práctica del análisis forense y de incidentes, preparando al futuro profesional para documentar, argumentar y proponer medidas de mitigación con un lenguaje técnico sólido y universalmente reconocido en la industria de la ciberseguridad.

Escenario01. Incidente LockBit

En múltiples incidentes atribuidos al grupo **LockBit**, organizaciones públicas y privadas han sufrido el cifrado masivo de servidores tras un acceso inicial no autorizado.
Antes de ejecutar el ransomware, los atacantes **exfiltraron información sensible** y posteriormente amenazaron con su publicación, evidenciando un compromiso simultáneo de la **confidencialidad, la integridad y la disponibilidad**.
Desde el enfoque del **RFC4949**, el incidente se clasifica como un **multi-stage attack** con **data breach** y **availability attack**, donde la indisponibilidad del sistema es solo una fase final del daño.
La ausencia de **respaldos inmutables** y de **detección temprana** permitió que el impacto fuera total.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad de datos, autenticación, control de accesos y disponibilidad.
Definición(es) aplicable(s) RFC 4949.	Multi-stage attack (ataque en etapas, Data Breach (brecha de datos) y availability attack.
Tipo de amenaza.	Interna
Vector de ataque.	Acceso inicial no autorizado
Impacto técnico / operativos.	Interrupción total de operaciones, pérdida de control de datos sensibles y posible extorsión financiera
Medida de control recomendada.	Detección de anomalías, control de acceso autenticación y verificación de permisos

Escenario 02 Análisis de Exposición de Datos

En diversos casos documentados, bases de datos completas quedaron accesibles públicamente debido a errores de configuración en servicios de

almacenamiento en la nube. No existió una explotación técnica sofisticada, sino una falla en el control de acceso, lo que derivó directamente en la pérdida de

confidencialidad de los datos. El RFC 4949 describe este tipo de incidentes como misconfiguration y exposure, subrayando que la amenaza no siempre

implica malware o intrusión activa. El impacto suele ser legal y reputacional, aun cuando no se pueda demostrar acceso malicioso.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad de datos, control de acceso
Definición(es) aplicable(s) RFC 4949.	Misconfiguration (errores de configuración), exposure (bases de datos disponibles al público)
Tipo de amenaza.	Interna
Vector de ataque.	Servicios de almacenamiento
Impacto técnico / operativo.	Legal
Medida de control recomendada.	Integridad de datos, control de acceso, autentificación

Escenario 03 Análisis de Compromiso

Un proveedor legítimo de software fue comprometido y distribuyó una actualización que incluía código malicioso, afectando a cientos de organizaciones que

confiaban en él. Este escenario refleja una violación grave de la integridad de los sistemas y, en muchos casos, de la confidencialidad, al permitir accesos no

autorizados posteriores. El RFC 4949 lo identifica como supply chain attack, destacando el abuso de relaciones de confianza. El daño es particularmente crítico

porque rompe el supuesto de legitimidad del software firmado.

Elemento	Respuesta
Servicios X.800 comprometidos.	Integridad, confidencialidad

Definición(es) aplicable(s) RFC 4949.	Supply chain Attack : Infiltración en un sistema, servicio o software aprovechando la confianza en un proveedor o proceso intermedio.
Tipo de amenaza.	Amenaza con troyano.
Vector de ataque.	Proveedor legítimo de software comprometido
Impacto técnico / operativo.	Rompe supuesto de legitimidad de software firmado
Medida de control recomendada.	Detección de intrusiones y anomalías

Escenario 04 Robo de Credenciales usando Phishing

Mediante campañas de phishing, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. Aunque la

autenticación funcionó técnicamente, el servicio de autenticación fue comprometido al basarse en credenciales robadas, afectando también el control de

acceso. Según el RFC 4949, se trata de un credential compromise con authentication failure conceptual, no técnica. La falta de MFA y de monitoreo de

comportamiento facilitó la persistencia del atacante.

Elemento	Respuesta
Servicios X.800 comprometidos.	Autenticación, control de acceso
Definición(es) aplicable(s) RFC 4949.	Phishing es un ataque de ingeniería social para obtener información sensible mediante engaño. Credential compromiso: Situación en la que credenciales válidas son robadas o utilizadas por un atacante. Authentication
Tipo de amenaza.	Amenaza persistente (suplantación de identidad durante meses)
Vector de ataque.	Ingeniería social/ campañas de phishing
Impacto técnico / operativo.	Persistencia del atacante dentro de la red y posible acceso no autorizado a datos internos.
Medida de control recomendada.	Implementación de doble autenticación

Escenario 05 Ataques de Ransomware

En ataques de ransomware avanzados, los atacantes eliminaron o cifraron los respaldos antes de afectar los sistemas productivos. Este hecho compromete

directamente la disponibilidad y la integridad de la información, al impedir la recuperación. El RFC 4949 clasifica este comportamiento como data destruction

y availability attack, evidenciando intención deliberada de maximizar el daño. La inexistencia de respaldos offline o inmutables convierte el incidente en

catastrófico.

Elemento	Respuesta
Servicios X.800 comprometidos.	Disponibilidad e integridad de datos
Definición(es) aplicable(s) RFC 4949.	Data destruction y availability attack.
Tipo de amenaza.	Externa
Vector de ataque.	Escalado de privilegios para alcanzar sistemas de almacenamiento y gestión de copias.
Impacto técnico / operativo.	Imposibilidad de recuperación ante desastres y pérdida permanente de datos críticos.
Medida de control recomendada.	Implementación de copias de seguridad offline e inmutables

Escenario 06 Abuso de Privilegios y Amenaza Interna

Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas. El servicio afectado fue

principalmente la confidencialidad, junto con fallas en el control de acceso por exceso de privilegios. El RFC 4949 define este escenario como insider threat,

destacando que el riesgo interno puede ser tan grave como el externo. La carencia de monitoreo y de políticas de mínimo privilegio fue determinante.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad y control de acceso
Definición(es) aplicable(s) RFC 4949.	Insider threat
Tipo de amenaza.	Amenaza interna
Vector de ataque.	Abuso de privilegios por empleado con acceso legítimo.

Impacto técnico / operativo.	Exfiltración de propiedad intelectual y pérdida de ventaja competitiva
Medida de control recomendada.	Implementación de políticas de mínimo privilegio, así como monitoreo de comportamiento de usuarios.

Escenario 07 Alteración de Registros y Pérdidas

Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas. El servicio afectado fue

principalmente la confidencialidad, junto con fallas en el control de acceso por exceso de privilegios. El RFC 4949 define este escenario como insider threat,

destacando que el riesgo interno puede ser tan grave como el externo. La carencia de monitoreo y de políticas de mínimo privilegio fue determinante.

Elemento	Respuesta
Servicios X.800 comprometidos.	Integridad y no repudio
Definición(es) aplicable(s) RFC 4949.	Audit trail compromiso Alteración o eliminación de registros de auditoría para ocultar actividades..
Tipo de amenaza.	Externa
Vector de ataque.	Scripts de post explotación, para borrar o modificar datos y registros de eventos.
Impacto técnico / operativo.	Pérdida de visibilidad sobre el incidente, incapacidad para realizar una reconstrucción forense, nulidad de pruebas para procesos legales y compromiso del cumplimiento normativo.
Medida de control recomendada.	Centralización de logs con almacenamiento de solo escritura.

Escenario 08 Falla Global por Actualización

Una actualización mal ejecutada provocó la caída simultánea de múltiples servicios críticos a nivel global. Aunque no existió un atacante, el servicio de

disponibilidad fue gravemente afectado. El RFC 4949 contempla estos eventos como operational failure, recordando que la seguridad también se ve afectada

por errores internos. La falta de pruebas previas y planes de reversión amplificó el impacto.

Elemento	Respuesta
Servicios X.800 comprometidos.	Disponibilidad

Definición(es) aplicable(s) RFC 4949.	Operational failure Falla en la operación normal de un sistema que afecta su funcionamiento esperado. Service disruption Interrupción parcial o total de un servicio informático.
Tipo de amenaza.	Accidental
Vector de ataque.	externa
Impacto técnico / operativo.	Caída masiva de servicios, perdida de ingresos y posible afectación de la continuidad del negocio.
Medida de control recomendada.	Un entorno dedicado a pruebas y planes de emergencia

Escenario 09 : Suplantación de Sitios Oficiales

Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible. Este escenario afecta la autenticación, al suplantar

identidades legítimas, y la confidencialidad de los datos recolectados. El RFC 4949 lo clasifica como masquerade y phishing, subrayando el componente de

ingeniería social. La ausencia de mecanismos de autenticación del dominio y de concientización facilitó el éxito del ataque.

Elemento	Respuesta
Servicios X.800 comprometidos.	Autenticación, confidencialidad de datos.
Definición(es) aplicable(s) RFC 4949.	Masquerade y phishing
Tipo de amenaza.	Externa
Vector de ataque.	Ausencia de mecanismos de autenticación de dominio y falta de concientización.
Impacto técnico / operativo.	Compromiso de datos personales y posible robo de identidad.
Medida de control recomendada.	Mecanismos de autenticación y campañas de concientización a gran escala.

Escenario 10

En algunos incidentes, tras exfiltrar información, los atacantes ejecutaron acciones destructivas para borrar sistemas completos y eliminar rastros. Se produce

un compromiso total de la confidencialidad, la integridad y la disponibilidad, configurando uno de los peores escenarios posibles. El RFC 4949 describe este

patrón como destructive attack, donde el objetivo no es solo el lucro, sino el daño irreversible. La detección tardía impidió cualquier contención efectiva.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad, disponibilidad e integridad de datos
Definición(es) aplicable(s) RFC 4949.	Destructive attack
Tipo de amenaza.	Activa (malware tipo wiper)
Vector de ataque.	Ejecución de comandos destructivos para borrar sistemas y eliminar rastros
Impacto técnico / operativo.	Destrucción irreversible de la infraestructura digital
Medida de control recomendada.	Destrucción irreversible de la infraestructura tecnológica.

Conclusión

El análisis de los escenarios propuestos evidencia la **complementariedad y utilidad práctica** de los marcos **ITU-T X.800** y **RFC 4949**. La X.800 proporcionó la estructura conceptual para identificar de manera sistemática qué servicios de seguridad (como la Integridad en un ataque *man-in-the-middle* o la Disponibilidad en un DDoS) fueron vulnerados en cada caso. Simultáneamente, el RFC 4949 permitió describir con precisión técnica los vectores de ataque (ej. *supply chain attack*, *credential compromise*, *destructive attack*), evitando ambigüedades y facilitando una comunicación clara entre profesionales.

Referencias

International Telecommunication Union. (1991). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800). Shirey, R. (2007). RFC 4949: Internet Security Glossary, Version 2. IETF.