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

CNO V: Seguridad Informática

Alonso Castillo Omar Karim 179033
Mtro. Servando López Contreras

27 de enero del 2026

Tabla de contenido

Introducción

La seguridad informática constituye un pilar esencial en la protección de los sistemas y la información frente a amenazas cada vez más sofisticadas. En este ejercicio se propone analizar escenarios de incidentes de seguridad aplicando los seis servicios de seguridad definidos en la recomendación ITU-T X.800 —autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad—, así como emplear de manera rigurosa la terminología estandarizada del RFC 4949.

El propósito central es fortalecer la capacidad del estudiante para identificar, explicar y documentar vulneraciones de seguridad en contextos reales, integrando tanto el enfoque conceptual de los servicios de seguridad como el marco terminológico técnico que facilita la comunicación profesional.

Informe

Escenario 01.

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 RFC 4949, 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.

Escenario 02.

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.

Escenario 03.

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.

Escenario 04.

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.

Escenario 05.

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.

Escenario 06.

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.

Escenario 07.

Tras un ataque, los registros del sistema quedaron cifrados o alterados, impidiendo reconstruir la secuencia de eventos. Esto compromete la integridad de los datos y el no repudio, ya que no es posible demostrar qué ocurrió ni quién fue responsable. Desde el RFC 4949, se trata de una violación de evidentiary integrity y del audit trail. El impacto no solo es técnico, sino también probatorio y legal.

Escenario 08.

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

Escenario 09.

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 masquera de y phishing, subrayando el componente de ingeniería social. La ausencia de mecanismos de autenticación del dominio y de concientización facilitó el éxito del ataque.

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

Análisis

Cada escenario de incidente de seguridad debe ser examinado de manera sistemática mediante el **llenado completo de la ficha de análisis**. El objetivo es que el análisis sea coherente, estandarizado y útil para documentar vulneraciones de seguridad en contextos reales, fortaleciendo así la capacidad de comunicación y el rigor técnico en la práctica profesional.

Escenario 01: Ataque LockBit (Ransomware y Exfiltración)

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad, Integridad, Disponibilidad.
Definición(es) aplicable(s) RFC 4949	**Multi-stage attack:** Serie de pasos del atacante para lograr un objetivo final. **Data breach:** Acceso o divulgación no autorizada de datos sensibles. **Availability attack:** Intento de impedir el acceso legítimo a servicios o datos.
Tipo de amenaza	Externa (Acceso inicial no autorizado seguido de ejecución maliciosa).
Vector de ataque	Exfiltración de datos y cifrado masivo de servidores.
Impacto técnico / operativo	Pérdida total de control operativo; exposición pública de información sensible.
Medida de control recomendada	Respaldos inmutables, detección temprana de anomalías, segmentación de red.

Escenario 02: Exposición en la Nube

Elemento	Respuesta
Servicios X.800 comprometidos	Control de acceso, Confidencialidad.
Definición(es) aplicable(s) RFC 4949	**Misconfiguration:** Error en la configuración de un sistema que debilita la seguridad. **Exposure:** Liberación accidental de datos sensibles en un entorno inseguro. **Malware:** Software malicioso (en este caso, se aclara que la falla no lo involucró).
Tipo de amenaza	Pasiva / Accidental (Originada por error de configuración).
Vector de ataque	Servicios de almacenamiento configurados como públicos.
Impacto técnico / operativo	Fuga masiva de bases de datos; impacto legal y reputacional severo.
Medida de control recomendada	Auditorías CSPM (Cloud Security Posture Management), políticas de acceso restringido.

Escenario 03: Compromiso de Cadena de Suministro

Elemento	Respuesta
Servicios X.800 comprometidos	Integridad, Confidencialidad.
Definición(es) aplicable(s) RFC 4949	**Supply chain attack:** Ataque que compromete los componentes o el software antes de llegar al usuario final. **Integrity:** Atributo que garantiza que el software no ha sido alterado de forma no autorizada.
Tipo de amenaza	Externa (Indirecta a través de un proveedor de confianza).
Vector de ataque	Inyección de código malicioso en actualizaciones de software legítimas.
Impacto técnico / operativo	Compromiso sistémico de múltiples organizaciones; ruptura de la cadena de confianza.
Medida de control recomendada	Análisis de integridad (hashes), monitoreo de comportamiento de software, sandboxing.

Escenario 04: Compromiso de Credenciales (Phishing)

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación, Control de acceso.
Definición(es) aplicable(s) RFC 4949	**Credential compromise:** Adquisición ilícita de nombres de usuario y contraseñas. **Authentication failure:** Situación donde el proceso de verificación no detecta a un impostor.
Tipo de amenaza	Externa (Uso de ingeniería social).
Vector de ataque	Campañas de phishing para el robo de identidades válidas.
Impacto técnico / operativo	Acceso persistente no detectado; movimiento lateral dentro de la red.
Medida de control recomendada	Implementación de MFA (Multi-Factor Authentication), monitoreo de comportamiento (UEBA).

Escenario 05: Destrucción de Respaldos (Ransomware)

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad, Integridad.
Definición(es) aplicable(s) RFC 4949	**Data destruction:** Acción intencional de borrar o corromper datos para que sean inutilizables. **Availability attack:** Ataque diseñado para interrumpir la operatividad.
Tipo de amenaza	Externa (Maliciosa con objetivo destructivo).
Vector de ataque	Cifrado y eliminación deliberada de respaldos y sistemas productivos.
Impacto técnico / operativo	Incapacidad total de recuperación; interrupción crítica del negocio.
Medida de control recomendada	Respaldos offline (Air-gapped) o bóvedas de datos inmutables.

Escenario 06: Amenaza Interna (Insider Threat)

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad, Control de acceso.
Definición(es) aplicable(s) RFC 4949	**Insider threat:** Persona con acceso legítimo que realiza actividades no autorizadas. **Privilege:** Derechos otorgados a un usuario para realizar acciones en el sistema.
Tipo de amenaza	Interna (Empleado con acceso legítimo).
Vector de ataque	Exceso de privilegios y extracción no autorizada de datos.
Impacto técnico / operativo	Exfiltración de propiedad intelectual y pérdida de activos informacionales.
Medida de control recomendada	Principio de mínimo privilegio (PoLP), sistemas de DLP (Data Loss Prevention).

Escenario 07: Alteración de Evidencia (Logs)

Elemento	Respuesta
Servicios X.800 comprometidos	Integridad, No repudio.
Definición(es) aplicable(s) RFC 4949	**Evidentiary integrity:** Certeza de que la información probatoria no ha sido alterada. **Audit trail:** Registro cronológico que permite reconstruir eventos.
Tipo de amenaza	Externa/Interna (Acción de post-explotación).
Vector de ataque	Cifrado o modificación de registros de auditoría del sistema.
Impacto técnico / operativo	Imposibilidad de reconstrucción forense; pérdida de capacidad probatoria legal.
Medida de control recomendada	Centralización de logs en servidores remotos inmutables (WORM).

Escenario 08: Falla Operativa Global

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad.
Definición(es) aplicable(s) RFC 4949	**Operational failure:** Caída del sistema debido a causas internas no maliciosas. **System availability:** Estado en que un sistema es accesible y utilizable.
Tipo de amenaza	Interna (Accidental/Error humano).
Vector de ataque	Despliegue de actualización crítica mal ejecutada.
Impacto técnico / operativo	Caída masiva de servicios críticos; impacto financiero y reputacional global.
Medida de control recomendada	Pruebas de regresión, planes de rollback y despliegues escalonados.

Escenario 09: Masquerade y Phishing

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación, Confidencialidad.
Definición(es) aplicable(s) RFC 4949	**Masquerade:** Intento de una entidad de hacerse pasar por otra. **Phishing:** Técnica de engaño para recolectar información de usuarios.
Tipo de amenaza	Externa (Ingeniería social).
Vector de ataque	Replicación de sitios web y correos electrónicos oficiales.
Impacto técnico / operativo	Captura masiva de datos sensibles de ciudadanos; fraude de identidad.
Medida de control recomendada	Implementación de DMARC/SPF, educación en ciberseguridad para el usuario.

Escenario 10: Ataque Destructivo Total

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad, Integridad, Disponibilidad.
Definición(es) aplicable(s) RFC 4949	**Destructive attack:** Ataque enfocado en causar daño irreversible al sistema. **Exfiltration:** Movimiento no autorizado de datos hacia el exterior.
Tipo de amenaza	Externa (Ataque malicioso avanzado).
Vector de ataque	Exfiltración de datos seguida de borrado masivo de sistemas.
Impacto técnico / operativo	Compromiso total de la triada de seguridad; daño irreversible a la infraestructura.
Medida de control recomendada	Sistemas de respuesta ante incidentes automatizados, segmentación crítica.

Conclusión

El análisis de estos incidentes demuestra que la seguridad efectiva depende de la aplicación conjunta de los servicios del estándar ITU-T X.800 y el lenguaje técnico del RFC 4949. Mientras el primero permite identificar qué objetivo de seguridad se ha roto, como la confidencialidad o la disponibilidad, el segundo aporta la precisión necesaria para describir si el evento fue una falla operativa, un ataque de ingeniería social o una vulnerabilidad en la cadena de suministro. Esta combinación es vital para entender que un sistema puede ser técnicamente funcional pero conceptualmente vulnerable, especialmente ante el robo de credenciales legítimas o errores de configuración en la nube.

La recurrencia de ataques destructivos y amenazas internas subraya que la protección de datos debe ir más allá de simples barreras externas. La integridad de los registros de auditoría y la inmutabilidad de los respaldos son elementos críticos para garantizar el no repudio y la recuperación ante desastres. En última instancia, documentar estos escenarios bajo estándares internacionales permite a las organizaciones fortalecer sus controles de acceso, aplicar el principio de mínimo privilegio y desarrollar una capacidad de respuesta ante incidentes mucho más robusta y profesional.

Referencias bibliográficas

International Telecommunication Union, Telecommunication Standardization Sector. (1991). *Recommendation ITU-T X.800: Security architecture for open systems interconnection for CCITT applications*. ITU. https://www.itu.int/rec/T-REC-X.800 199103-I/es

Shirey, R. (2007). *RFC 4949: Internet security glossary, version 2* (RFC 4949). RFC Editor. https://www.rfc-editor.org/rfc/rfc4949