UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

27-1-2026

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

Hernández Fernández Diego Osvaldo

182217

Diego Osvaldo Hernández Fernández

Contenido

Introducción y Contexto Técnico

La seguridad de la información se rige por estándares que unifican criterios técnicos y operativos. La Recomendación X.800 establece la arquitectura de seguridad para sistemas abiertos, clasificando los Servicios de Seguridad (Autenticación, Control de Acceso, Confidencialidad, Integridad y No Repudio) y los mecanismos para ejecutarlos. Por su parte, el RFC 4949 actúa como el glosario terminológico fundamental de la IETF, proporcionando definiciones precisas para la gestión de amenazas y vulnerabilidades, permitiendo que el análisis de incidentes tenga validez técnica y legal.

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.

Elemento	Respuesta
Servicios X.800 comprometidos	El robo de datos rompe la confidencialidad, el cifrado altera la integridad y el bloqueo del sistema anula la disponibilidad.
Definición(es) aplicable(s) RFC 4949	**Multi-stage attack:** Serie de pasos progresivos para lograr un objetivo. **Data Breach:** Liberación no autorizada de datos sensibles. **Availability Attack:** Acción que impide que los usuarios accedan a los servicios.
Tipo de amenaza	Externa.
Vector de ataque	Acceso inicial no autorizado seguido de Exfiltración de datos y Cifrado masivo.
Impacto técnico / operativo	Pérdida de control operativa, exposición pública de secretos corporativos y extorsión financiera.
Medida de control recomendada	Respaldos inmutables**,** segmentación de red y políticas de cifrado de datos sensibles.

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.

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad y Control de acceso.
Definición(es) aplicable(s) RFC 4949	**Misconfiguration:** Configuración incorrecta de componentes de seguridad. **Exposure:** Situación donde datos sensibles son visibles a personas no autorizadas. **Data Leak:** Divulgación accidental de información protegida.
Tipo de amenaza	Interna.
Vector de ataque	Configuración incorrecta de permisos**.**
Impacto técnico / operativo	Pérdida de confidencialidad ya que hubo una **f**uga de datos masiva que podría llevar a sanciones legales severas y daño irreparable a la reputación de la empresa.
Medida de control recomendada	Auditorías de configuración, implementación del Principio de Menor Privilegio, y cifrado de datos en reposo.

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.

Elemento	Respuesta
Servicios X.800 comprometidos	La integridad se vulnera al modificar el software original y la confidencialidad se ve afectada por el acceso no autorizado posterior.
Definición(es) aplicable(s) RFC 4949	**Supply Chain Attack:** Ataque que compromete a un proveedor para llegar a sus clientes. **Malicious Code:** Software diseñado con propósitos hostiles (backdoor).

	Trust Relationship: Confianza en que un tercero mantiene estándares de seguridad.
Tipo de amenaza	Externa.
Vector de ataque	Inyección de código malicioso en actualizaciones oficiales y abuso de firmas digitales confiables.
Impacto técnico / operativo	Se permitió la ejecución de código malicioso con privilegios elevados en cientos de organizaciones simultáneamente.
Medida de control recomendada	Sandboxing de actualizaciones, monitoreo de comportamiento post-parche y auditorías a proveedores.

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.

Elemento	**Respuesta**
Servicios X.800 comprometidos	Autenticación y Control de acceso.
Definición(es) aplicable(s) RFC 4949	**Credential compromise:** Obtención ilegal de datos de acceso. **Authentication failure (Conceptual):** El proceso técnico de validar la clave funciona, pero falla el propósito de identificar al usuario real. **Phishing:** Engaño para obtener información sensible.
Tipo de amenaza	Externa.
Vector de ataque	Phishing y abuso de credenciales legítimas para acceso inicial
Impacto técnico / operativo	Acceso no autorizado de larga duración (esto implica que los ciberdelincuentes podrían permanecer meses sin ser detectado permite el robo de datos, espionaje y posible movimiento lateral)
Medida de control recomendada	Auditorías u programas de concientización sobre Phishing y análisis de comportamiento de usuarios y entidades

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.

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad e Integridad ya que la disponibilidad se anula al cifrar los datos, y la integridad se pierde totalmente al alterar los archivos de respaldo.
Definición(es) aplicable(s) RFC 4949	**Data destruction:** Alteración o borrado deliberado de datos. **Availability attack:** Acción que impide el uso legítimo de los recursos del sistema. **Ransomware:** Malware que bloquea el acceso a datos y exige un rescate.
Tipo de amenaza	Externa.
Vector de ataque	Movimiento lateral con escalada de privilegios para comprometer los servidores de respaldo.
Impacto técnico / operativo	Pérdida permanente de datos si no existen copias externas, parálisis total de la operación y daño financiero masivo.
Medida de control recomendada	Respaldos inmutables dando como ejemplo la regla de los 5 (consiste en tener 5 respaldos físicos y otros 5 respaldos en la nube)

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.

Elemento	Respuesta
Servicios X.800 comprometidos	Confidencialidad y Control de acceso, empezando por la confidencialidad que es el objetivo principal del robo, mientras que el control de acceso falla al permitir privilegios excesivos al empleado.

Definición(es) aplicable(s) RFC 4949	**Insider Threat:** Individuo con acceso legítimo que abusa de sus privilegios para causar daño. **Data Leak / Exfiltration:** Transferencia no autorizada de datos hacia el exterior. **Least Privilege (Violation):** Incumplimiento del principio de otorgar solo los permisos necesarios para la función laboral.
Tipo de amenaza	Interna.
Vector de ataque	Abuso de privilegios legítimos ya que se hizo extracción de datos mediante medios físicos (USB), nubes personales o correos electrónicos.
Impacto técnico / operativo	Fuga de datos sensibles de clientes, posibles demandas legales y crisis de confianza interna.
Medida de control recomendada	Aplicar el principio de mínimo privilegio**,** monitoreo de actividad inusual y auditorías de acceso periódicas.

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.

Elemento	Respuesta
Servicios X.800 comprometidos	Integridad y no repudio ya que al alterar los registros, no se puede garantizar que la información sea veraz ni vincular las acciones a un usuario específico.
Definición(es) aplicable(s) RFC 4949	**Audit Trail:** Conjunto de registros que permiten reconstruir eventos. **Evidentiary Integrity:** Cualidad de la evidencia que no ha sido alterada desde su recolección. **Non-repudiation:** Servicio que evita que una entidad niegue haber realizado una acción.
Tipo de amenaza	**Externa.**
Vector de ataque	Inyección de comandos o escalada de privilegios para obtener permisos de escritura/borrado en los archivos de registro del sistema (logs).

Impacto técnico / operativo	Imposibilidad de realizar un análisis de causa raíz, pérdida de validez legal de las pruebas y vulnerabilidad ante futuros ataques similares.
Medida de control recomendada	Centralización de Logs en un servidor externo de solo lectura, uso de Hashing para verificar integridad (verificar si es el archivo es el original o se realizó alguna modificación)

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.

Elemento	Respuesta
Servicios X.800 comprometidos	Disponibilidad, debido a que el sistema deja de ser accesible para los usuarios autorizados, interrumpiendo la continuidad del servicio.
Definición(es) aplicable(s) RFC 4949	**Operational Failure:** Incumplimiento de la función del sistema debido a causas internas no maliciosas. **Availability:** Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. **Denial of Service (Inadvertent):** Interrupción del servicio causada accidentalmente.
Tipo de amenaza	Interna.
Vector de ataque	Despliegue de software defectuoso ya que existió una falta de control de calidad y omisión de pruebas en entorno.
Impacto técnico / operativo	Caída sistémica, pérdida de ingresos, afectación a la infraestructura crítica y crisis de reputación global.
Medida de control recomendada	Pruebas exhaustivas en entornos aislados y políticas de Gestión de Cambios.

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 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	Se vulnera la autenticidad del origen ya que el usuario cree que habla con la entidad oficial y se pierde la confidencialidad de los datos entregados.
Definición(es) aplicable(s) RFC 4949	**Masquerade:** Tipo de amenaza donde una entidad no autorizada pretende ser una entidad autorizada. **Phishing:** Intento de adquirir información sensible mediante el engaño en comunicaciones electrónicas. **Spoofing:** Técnica para falsificar datos (como el remitente de un correo o una URL) para parecer legítimo.
Tipo de amenaza	Externa.
Vector de ataque	Clonación de sitios web y envío de correos fraudulentos con remitentes falsificados.
Impacto técnico / operativo	Robo masivo de identidad ya que existe un **c**ompromiso de cuentas personales y bancarias, pérdida de confianza ciudadana en las plataformas oficiales y daños financieros.
Medida de control recomendada	Protocolos para autenticación de correos, certificados SSL/TLS validados, y programas constantes de concientización para usuarios finales.

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	Se roban los datos (Confidencialidad), se alteran registros (Integridad) y se destruye el sistema (Disponibilidad).
Definición(es) aplicable(s) RFC 4949	**Destructive Attack:** Ataque cuyo objetivo principal es causar daño físico o lógico permanente. **Data Exfiltration:** Extracción no autorizada de información. **Wiper:** Malware diseñado específicamente para borrar o destruir el contenido de una unidad de almacenamiento.

Tipo de amenaza	Externa.
Vector de ataque	Exfiltración de datos seguida de la ejecución de scripts de borrado masivo con privilegios de administrador.
Impacto técnico / operativo	Destrucción irreversible de la infraestructura, imposibilidad de recuperación forense y cierre prolongado de operaciones.
Medida de control recomendada	Detección temprana (IDS/IPS), segmentación de red para evitar movimientos laterales.

Conclusión

El análisis de estos escenarios demuestra que la seguridad efectiva no depende de herramientas aisladas, sino de un marco normativo sólido como el **X.800** y el **RFC 4949**. Estos estándares permiten transformar incidentes complejos en diagnósticos técnicos precisos, facilitando la toma de decisiones basada en la tríada de **Confidencialidad, Integridad y Disponibilidad**.

Referencias

- Unión Internacional de Telecomunicaciones. (1991). *Recomendación UIT-T X.800: Arquitectura de seguridad para la Interconexión de Sistemas Abiertos para aplicaciones de las CCITT*. https://www.itu.int/rec/t-rec-x.800-199103-i/es
- Shirey, R. (2007). *Internet Security Glossary, Version 2* (RFC No. 4949). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4949