UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Universidad Politécnica de San Luis Potosí
Ing. Tecnologías de la Información
Primavera 2026

Actividad 02 .- Análisis de servicios de seguridad (X.800 y RFC 4949)

Jorge Emmanuel López Monsiváis 179842
Mto: Servando López Contreras

Fecha de Entrega: 27/01/2026

Introducción

El RFC 4949, titulado “Internet Security Glossary”, es un documento publicado por la IETF que proporciona un glosario estandarizado de términos relacionados con la seguridad de la información y las redes. Su objetivo principal es unificar el significado de conceptos clave como autenticación, confidencialidad, integridad, disponibilidad, control de acceso y criptografía, entre muchos otros. Este RFC sirve como referencia común para investigadores, profesionales y estudiantes, ayudando a evitar ambigüedades y a mejorar la comunicación en el ámbito de la seguridad informática.

Por su parte, la recomendación UIT-T X.800, conocida como “Arquitectura de seguridad para la interconexión de sistemas abiertos (OSI)”, define un marco conceptual para la seguridad de redes. En este estándar se establecen los servicios de seguridad (como confidencialidad, integridad, autenticación y no repudio), así como los mecanismos de seguridad que permiten implementarlos. El modelo X.800 es fundamental porque ofrece una visión estructurada de cómo proteger la información en sistemas de comunicación, y ha influido en muchos modelos y normas de seguridad posteriores.

En conjunto, el RFC 4949 y el UIT-T X.800 son pilares teóricos de la seguridad de la información: el primero aporta claridad terminológica, mientras que el segundo proporciona una arquitectura conceptual para diseñar y analizar sistemas seguros.

Se plantean diferentes escenarios en donde habrá que identificar algunos elementos.

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.	• Confidencilidad**:** Por la exfiltración de datos sensibles. • Integridad**:** Por el cifrado de archivos (modificación no autorizada). • Disponibilidad**:** Por el bloqueo de acceso a servidores y sistemas. • Control de acceso: Por el acceso inicial no atuorizado a la red.
Definición(es) aplicable(s) RFC 4949.	• Multi-stage attack: Serie de acciones de ataque que se dirigen a un objetivo común. • Data Breach: Un incidente de seguridad en el que los datos son accedidos sin autorización. • Availability Attack: Una acción que impide el acceso a los servicios del sistema. • Exfiltration: Transferencia no autorizada de datos desde dentro de un sistema.
Tipo de amenaza.	Externa (Cuando alguien accede desde el exterior, no hay infiltrados)
Vector de ataque.	Acceso inicial no autorizado, exfiltración de datos y ejecución final del ransomwatre.
Impacto técnico / operativo.	Pérdida total de la CIA de los datos, interrupción de la continuidad del negocio, exposición de datos sensibles y posible daño reputacional/extorsión.

Medida de control recomendada	Implementación de respaldos inmutables, sistemas de detección y respuesta para detección temprana, segmnetación de red y política de Zero Trust.

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**:** Los datos fueron legibles para entidades no autorizadas. • Control de Acceso: Fallo en los mecanismos para limitar el acceso a usuarios legítimos.
Definición(es) aplicable(s) RFC 4949.	• Misconfiguration**:** Error en la configuración de parámetros de seguridad que crea una vulnerabilidad. • Exposure**:** Incidente donde datos sensibles se vuelven disponibles a personas no autorizadas. • Data Leak: Salida no intencionada de datos fuera del control administrativo.
Tipo de amenaza.	Interna (No se pudiera clasificar como infiltrado, pero la mala configuración del servicio de almacenamiento)
Vector de ataque.	De acuerdo con la descripción del problema, se puede concluir que no hubo una explotación real, en este caso el acceso directo fue la via HTTP/S.
Impacto técnico / operativo.	Compromiso de la privacidad de la información, posibles multas por

	incumplimiento de leyes de protección de datos y daño a la imagen corporativa.
Medida de control recomendada	Auditorías o capacitación de configuración automatizada y monitoreo de logs de acceso.

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.	• Integirdad**:** El software original fue modificado con código malicioso. • Autenticación**:** Se abusa de la identidad del proveedor para distribuir el malware. • Confidencialidad**:** El accceso posterior permite el robo de información.
Definición(es) aplicable(s) RFC 4949.	• **Supply Chain Attack:** Ataque que apunta a los elementos menos seguros de una red de suministro. • **Software Integrity:** La garantía de que el código no ha sido alterado de manera no autorizada. • **Trojan Horse:** Código malicioso contenido dentro de un programa aparentemente inofenivo.
Tipo de amenaza.	Externa (La infección fue distribuída)
Vector de ataque.	Inyección de código malicioso en el repositorio de desarrollo.
Impacto técnico / operativo.	Pérdida de confianza en la infraestructura de clave pública (PKI) y firmas digitales, acceso masivo a redes de clientes y compromiso sistémico a gran escala.

Medida de control recomendada	Análisis de composición de software, uso de hashes y monitoreo de comportamiento de red.

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**:** El servicio es engañado al presentar credenciales legítimas por un usuario ilegítimo. • Control de Acceso: Una vez superada la autenticación, el atacante ejerce privilegios no autorizados.
Definición(es) aplicable(s) RFC 4949.	• Credential Compromise: El acto de obtener datos de autenticación de manera ilícita. • Phishing**:** Técnica de ingeniería social para engañar a los usuarios y obtener información sensible. • Authentication Failure: Cuando el sistema valida la credencial pero la identidad real del sujeto no corresponde al dueño legítimo.
Tipo de amenaza.	Externa (Uso de credenciales tuvo acceso a cerdenciales válidas)
Vector de ataque.	Aplicación de la ingeniería spcial seguida de un inicio de sesión.
Impacto técnico / operativo.	Suplantación de identidad, acceso a la información y persistencia prolongada dentro de la red sin ser detectado.
Medida de control recomendada	Aplicar autenticación de múltiples factores, analzar el comportamiento de

	los usuarios y campañas de concientización.

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**:** Se impide la recuperación de los servicios y datos. • Integridad**:** Los archivos de respaldo son alterados o eliminados. • Control de Acceso: El atacante logra elevar privilegios para alcanzar los repositorios de backup.
Definición(es) aplicable(s) RFC 4949.	• Data Destruction**:** Alteración o eliminación deliberada de datos para que no puedan ser utilizados o recuperados. • Availability Attack: Ataque diseñado para impedir que un sistema realice su función crítica. • Recovery Point Objective Failure**:** Incapacidad de restaurar el sistema a un estado anterior debido a la pérdida de datos.
Tipo de amenaza.	Externa (El ransomware fue inyectado)
Vector de ataque.	Escalada de privilegios y movimiento hacia los servidores de respaldo.
Impacto técnico / operativo.	Incapacidad de recuperación ante desastres, pérdida permanente de activos de información y parálisis total de las operaciones del negocio por tiempo indefinido.
Medida de control recomendada	Implementación de respaldos inmutables, y backups online

	implementando también privilegios de acceso a ellos.

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**:** Los datos fueron revelados a entidades no autorizadas. • Control de Acceso**:** Abuso de privilegios otorgados para fines distintos a los laborales.
Definición(es) aplicable(s) RFC 4949.	• Insider Threat**:** Una entidad autorizada que utiliza el acceso, de forma consciente o inconsciente, para dañar al sistema. • Abuse of Privilege**:** Uso de privilegios para realizar funciones no autorizadas. • Data Theft**:** Extracción física o digital de datos para beneficio propio o de terceros.
Tipo de amenaza.	Interna (El empleado aprovecho sus privilegios de usuario para poder extraer la información y hacer mal uso de ella.)
Vector de ataque.	Uso indebido de privilegios legítimos
Impacto técnico / operativo.	Pérdida de propiedad intelectual, ventaja competitiva y datos de clientes; posibles sanciones legales y quiebra de la confianza interna.
Medida de control recomendada	Implementación de sistemas de prevención de fuga de datos y monitorieo de actividad de los usuarios.

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**:** Los registros (logs) fueron modificados o eliminados. • No Repudio**:** Se pierde la capacidad de probar la autoría de las acciones realizadas. • Autenticación**:** Al perder la trazabilidad, no se puede validar quién accedió realmente.
Definición(es) aplicable(s) RFC 4949.	• Audit Trail**:** Conjunto de registros que proporcionan evidencia documental de la secuencia de actividades. • Evidentiary Integrity: La seguridad de que la prueba digital no ha sido alterada desde su creación. • Accountability**:** Propiedad que asegura que las acciones de una entidad puedan ser rastreadas de forma única hacia esa entidad.
Tipo de amenaza.	Externa (Se considera externa dado a la manera en la que se oculta la información para evitar la respuesta legal)
Vector de ataque.	Manipulación directa de archivos de registro del sistema operativo, limpieza de logs de aplicaciones tras obtener privilegios de administrador.
Impacto técnico / operativo.	No se puede realizar un análisis de causa raíz y se pierde la validez de las pruebas legales en juicio.
Medida de control recomendada	Implementacion de control de logs en tiempo real a un servidor remoto y el uso de firmas digitales.

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**:** El servicio dejó de ser accesible para los usuarios autorizados debido a la caída de los sistemas.
Definición(es) aplicable(s) RFC 4949.	• Operational Failure: Un evento donde un sistema no puede realizar su función debido a errores internos, no necesariamente ataques. • Service Disruption: Interrupción temporal o permanente de un servicio del sistema. • Reliability**:** La propiedad de que un sistema se comporte de acuerdo con sus especificaciones de manera consistente.
Tipo de amenaza.	Interna (El ataque resultó de un error en los procesos de gestión de cambios, no hubo intención maliciosa)
Vector de ataque.	No se puede definir el vector de ataque, dadoque se trató de un error de procesos.
Impacto técnico / operativo.	Denegación del servicio a escala masiva, pérdida de ingresos y caos operativo.
Medida de control recomendada	Implementación de pruebas de regresión y un plan de reversión.

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.	• Autenticación: Se compromete la veracidad de la identidad del origen (suplantación del sitio oficial). • Confidencialidad: Los datos sensibles de los ciudadanos son expuestos a terceros no autorizados.
Definición(es) aplicable(s) RFC 4949.	• Masquerade**:** Una entidad que finge ser otra para obtener acceso no autorizado o privilegios. • Phishing**:** Técnica de engaño para adquirir información sensible mediante la falsificación de una comunicación electrónica. • Social Engineering**:** Manipulación psicológica de personas para que realicen acciones o divulguen información confidencial.
Tipo de amenaza.	Externa (Se usa el phishing para obtener la información de las personas)
Vector de ataque.	Spoofing de correo y URL, se crearon sitios web espejo y se envían correos masivos.
Impacto técnico / operativo.	Robo masivo de identidades, compromiso de cientas bancarias y pérdida de la confianza publica.
Medida de control recomendada	Implementación de autenticación de correo, uso de certificados SSL/TLS y programas de concientización ciudadana.

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**:** Por la exfiltración previa de datos. • Integridad**:** Por la alteración y destrucción de archivos del sistema. • Disponibilidad**:** Por la eliminación total de la capacidad operativa del hardware/software.
Definición(es) aplicable(s) RFC 4949.	• Destructive Attack**:** Un ataque cuyo propósito principal es causar un daño permanente o costoso a los recursos del sistema. • Data Wipe**:** Eliminación irreversible de datos que impide su recuperación forense. • Anti-Forensics**:** Acciones para omitir, alterar o destruir evidencia que podría ser usada en una investigación.
Tipo de amenaza.	Externa (Ataque malintencionado de alta intensidad orientado a la parálisis total)
Vector de ataque.	Compromiso de cientas administrativas, seguido de la exfiltración de datos silenciosa y finalmente la ejecución del malware de destrucción de volúmenes.
Impacto técnico / operativo.	Destrucción de archivos digitales, imposibilidad de recuperación mediante métodos estándar y necesidad de reconstrucción total de la infraestructura.
Medida de control recomendada	Segmentacion de red estricta, sistemas de detección de anomalías y respaldos inaccesibles desde la red principal.

Conclusión

El análisis sistemático de estos diez escenarios demuestra que la seguridad informática, bajo los marcos del RFC 4949 y el ITU-T X.800, no es un estado estático sino un equilibrio dinámico donde la tríada de confidencialidad, integridad y disponibilidad es vulnerable tanto a ataques externos sofisticados como a errores humanos internos. El aprendizaje fundamental es que las organizaciones deben trascender la seguridad perimetral tradicional para adoptar un enfoque de defensa en profundidad, entendiendo que el compromiso de la autenticación y el abuso de confianza son los vectores más críticos en la actualidad.

En última instancia, la resiliencia no solo depende de prevenir intrusiones, sino de la capacidad de mantener audit trails íntegros y respaldos inmutables que permitan la recuperación ante ataques destructivos o fallos operativos, transformando la seguridad en un proceso de mejora continua basado en la detección temprana y el control estricto de privilegios.

Referencias

Shirey, R. (2007). *Internet Security Glossary, Version 2* (RFC 4949). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4949

Unión Internacional de Telecomunicaciones. (1991). *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones de las CCITT* (Recomendación ITU-T X.800). https://www.itu.int/rec/T-REC-X.800-199103-I/es