ANALISIS DE SERVICIOS DE SEGURIDAD (X.800 , RFC4949)

CON V – SEGURIDAD INFORMATICA

27 DE ENERO DE 2026

PALOMO CERDA JOSE ARMANDO 175932
MSTRO. SERVANDO LOPEZ CUEVAS
Universidad Politécnica de San Luis Potosi

Contenido

ANALISIS DE SERVICIOS DE SEGURIDAD (X.800 , RFC4949)

Introducción

En el panorama actual de la ciberseguridad, la sofisticación de las amenazas exige que los profesionales de TI utilicen un lenguaje técnico estandarizado y marcos de referencia robustos para el análisis de incidentes. Esta actividad se centra en la aplicación de dos pilares fundamentales: el modelo **ITU-T X.800** y el **RFC 4949**.

El estándar **X.800**, desarrollado por la Unión Internacional de Telecomunicaciones, establece los servicios de seguridad necesarios para proteger las arquitecturas de red, definiendo conceptos críticos como la confidencialidad, la integridad y la disponibilidad. Por otro lado, el **RFC 4949** funciona como el glosario terminológico de Internet, proporcionando definiciones precisas que permiten a los analistas categorizar amenazas, ataques y vulnerabilidades de manera inequívoca.

A través del análisis de diez escenarios distintos —que van desde el ransomware avanzado y ataques a la cadena de suministro hasta errores de configuración en la nube y amenazas internas—, este trabajo busca demostrar cómo el uso correcto de esta terminología facilita la identificación de vectores de ataque y la implementación de controles de seguridad efectivos. Al contrastar la teoría con casos prácticos, se fortalece la capacidad de documentar vulnerabilidades y proponer medidas de mitigación que protejan los activos más valiosos de cualquier organización: su información y su continuidad operativa.

Escenarios

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.	**Confidencialidad:** Por la exfiltración de datos sensibles. **Integridad:** Por la alteración/cifrado de los archivos originales. **Disponibilidad:** Por el bloqueo de acceso a los servidores.
Definición(es) aplicable(s) RFC 4949.	**Data Breach:** Acceso y liberación de datos a entidades no autorizadas. **Availability Attack:** Acción que impide el uso legítimo de recursos. **Multi-stage Attack:** Ataque que ocurre en varias fases (acceso, exfiltración, cifrado). **Unauthorized Access:** Entrada no permitida al sistema.
Tipo de amenaza.	**Externa Activa:** Un agente externo realiza acciones para alterar el estado del sistema y robar datos.
Vector de ataque.	Explotación de vulnerabilidades o credenciales comprometidas para acceso inicial, seguido de movimiento lateral y exfiltración de datos.
Impacto técnico / operativo.	Parálisis total de la operación, pérdida de control sobre la privacidad de los datos y daño reputacional por posible publicación.
Medida de control recomendada.	Implementación de **respaldos inmutables** (offline), sistemas de detección **EDR/XDR** para frenar la exfiltración, y segmentación de red.

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:** El servicio principal afectado, ya que datos privados se volvieron públicos. **Control de Acceso:** La política de seguridad falló al permitir lectura a usuarios no autenticados.
Definición(es) aplicable(s) RFC 4949.	**Exposure:** Incidente donde datos sensibles se vuelven disponibles para entidades no autorizadas. **Misconfiguration:** Error en la configuración de seguridad que crea una vulnerabilidad. **Data Leak:** Salida no intencionada de información del perímetro de control.
Tipo de amenaza.	**Externa Pasiva:** No requiere una acción técnica contra el sistema; la información "fluye" hacia afuera por sí sola debido a la falla.
Vector de ataque.	Ausencia de mecanismos de autenticación en buckets de almacenamiento o bases de datos (Open S3 Buckets / Open Database).
Impacto técnico / operativo.	Sanciones legales (GDPR/LFPDPPP), pérdida de confianza de los clientes y exposición de propiedad intelectual.
Medida de control recomendada.	Implementación de **Políticas de Menor Privilegio**, auditorías automatizadas de configuración (CSPM) 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.	**Integridad:** El software legítimo fue alterado con código malicioso. **Autenticación:** Se abusó de la confianza en la firma digital del proveedor. **Confidencialidad:** Como consecuencia del acceso posterior no autorizado.
Definición(es) aplicable(s) RFC 4949.	**Supply Chain Attack:** Ataque que apunta a elementos menos seguros en la red de suministros. **Malware:** Código diseñado para ejecutar procesos no deseados. **Trust Abuse:** Violación de una relación de confianza establecida entre entidades.
Tipo de amenaza.	**Externa Activa:** Un tercero manipula el proceso de desarrollo o distribución para causar daño.
Vector de ataque.	Inyección de código malicioso en el repositorio de código fuente del proveedor o compromiso del servidor de actualizaciones.
Impacto técnico / operativo.	Compromiso masivo de clientes finales, pérdida de confianza en el ecosistema de software y despliegue automatizado de puertas traseras (*backdoors*).
Medida de control recomendada.	**Análisis de composición de software (SCA)**, verificación de *hashes* post-descarga, implementación de Zero Trust y sandboxing de actualizaciones.

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:** Se suplanta la identidad del usuario legítimo. **Control de Acceso:** El atacante evade las restricciones al usar una identidad válida. **Confidencialidad:** Acceso a información privada durante el periodo de persistencia.
Definición(es) aplicable(s) RFC 4949.	**Credential Compromise:** Obtención de datos de autenticación por un tercero. **Phishing:** Engaño para obtener información confidencial **Masquerade:** Una entidad se hace pasar por otra para obtener privilegios no autorizados.
Tipo de amenaza.	**Externa Activa:** El atacante interactúa con el usuario para robar datos y luego con el sistema para acceder.
Vector de ataque.	Ingeniería social (correo electrónico malicioso) para captura de credenciales y posterior inicio de sesión remoto.
Impacto técnico / operativo.	Persistencia de largo plazo (APT), robo de datos continuado y posible movimiento lateral hacia otros servidores.
Medida de control recomendada.	Implementación obligatoria de **MFA (Autenticación de Múltiples Factores)**, análisis de comportamiento (UEBA) y capacitación en concientización de seguridad.

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 elimina la capacidad de restaurar el servicio. **Integridad:** Los archivos de respaldo son alterados o eliminados permanentemente.
Definición(es) aplicable(s) RFC 4949.	**Data Destruction:** Alteración deliberada de datos para que no puedan ser recuperados. **Availability Attack:** Acción diseñada para prevenir que un sistema realice su función. **Ransomware:** Software malicioso que bloquea el acceso a datos hasta que se pague un rescate.
Tipo de amenaza.	**Externa Activa:** El atacante realiza acciones directas de borrado y cifrado dentro del sistema.
Vector de ataque.	Movimiento lateral hasta alcanzar los servidores de almacenamiento o consolas de administración de backups.
Impacto técnico / operativo.	Pérdida definitiva de datos, incapacidad de recuperación ante desastres y cierre total de operaciones por tiempo indefinido.
Medida de control recomendada.	Estrategia de respaldo **3-2-1** con **respaldos inmutables** (WORM) o **Air-gapped** (fuera de línea), y protección de credenciales de administrador de backups.

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:** Datos privados fueron expuestos y vendidos. **Control de Acceso:** Falló la restricción de qué datos podía ver o exportar el empleado.
Definición(es) aplicable(s) RFC 4949.	**Insider Threat:** Individuo con acceso autorizado que utiliza dicho acceso para dañar la organización. **Data Leakage:** Salida no autorizada de datos sensibles. **Privilege Abuse:** Uso de derechos de acceso para propósitos distintos a los asignados.
Tipo de amenaza.	**Interna Activa:** El daño proviene de alguien dentro del perímetro de seguridad que realiza acciones deliberadas.
Vector de ataque.	Abuso de privilegios administrativos o de usuario y exfiltración de datos mediante medios físicos (USB) o servicios en la nube.
Impacto técnico / operativo.	Pérdida de propiedad intelectual, ventaja competitiva comprometida y posibles multas regulatorias severas.
Medida de control recomendada.	Implementación del **Principio de Mínimo Privilegio (PoLP)**, sistemas de Prevención de Pérdida de Datos (**DLP**) y monitoreo de actividad de usuarios (UAM).

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. **Autenticación:** Al no haber registros, no se puede validar quién accedió.
Definición(es) aplicable(s) RFC 4949.	**Audit Trail:** Conjunto de registros que proporcionan evidencia de la secuencia de actividades. **Evidentiary Integrity:** Cualidad de los datos que los hace aceptables como prueba en un proceso legal. **Tampering:** Alteración deliberada de información o registros.
Tipo de amenaza.	**Externa Activa:** El atacante realiza cambios intencionales para encubrir su actividad.
Vector de ataque.	Acceso administrativo a los archivos de registro del sistema o uso de herramientas de limpieza de logs (Log wipers).
Impacto técnico / operativo.	Imposibilidad de realizar análisis forense, pérdida de validez legal de las pruebas y desconocimiento del alcance real de la intrusión.
Medida de control recomendada.	Implementación de **Servidores de Logs Centralizados** (SIEM) con escritura *Append-only* y envío de registros en tiempo real fuera del host local.

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 principal afectado debido a la interrupción del acceso a los recursos críticos.
Definición(es) aplicable(s) RFC 4949.	**Operational Failure:** Error interno que resulta en la pérdida de un servicio del sistema. **Denial of Service (DoS):** Aunque no fue intencional, el resultado es la negación del servicio a usuarios legítimos. **System Integrity:** Se ve afectada la cualidad del sistema de operar de manera correcta y predecible.
Tipo de amenaza.	**Interna Accidental:** El daño es causado por personal interno sin intención maliciosa, derivado de un error en los procedimientos.
Vector de ataque.	Error de configuración o bug en el código de la actualización distribuido sin validación previa.
Impacto técnico / operativo.	Caída masiva de servicios, pérdida económica por tiempo de inactividad (downtime) y daño reputacional ante clientes globales.
Medida de control recomendada.	Implementación de **Pruebas de Regresión** en ambientes de Staging, **Despliegues Progresivos** (Canary Deployments) y Planes de Rollback automáticos.

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 suplanta la identidad de una entidad legítima para engañar al usuario. **Confidencialidad:** Los datos sensibles de los ciudadanos son capturados por terceros.
Definición(es) aplicable(s) RFC 4949.	**Masquerade:** Una entidad se hace pasar por otra para obtener acceso o información. **Phishing:** Técnica de ingeniería social para adquirir información sensible de forma fraudulenta. **Deception:** Circunstancia donde un usuario es engañado para aceptar como verdadero algo falso.
Tipo de amenaza.	**Externa Activa:** El atacante crea activamente recursos falsos para interceptar comunicaciones y datos.
Vector de ataque.	Creación de dominios "typosquatting" (nombres similares), duplicación de diseño web (clonación) y envío de correos fraudulentos.
Impacto técnico / operativo.	Robo masivo de identidades, fraudes financieros a gran escala y pérdida total de confianza en los canales digitales oficiales.
Medida de control recomendada.	Implementación de protocolos **DMARC/SPF/DKIM**, uso de certificados SSL con validación extendida y campañas de **Security Awareness** para usuarios.

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:** Violada durante la fase previa de exfiltración. **Integridad:** Destrucción total de la estructura de archivos y sistemas operativos. **Disponibilidad:** Pérdida permanente de acceso a los servicios y datos.
Definición(es) aplicable(s) RFC 4949.	**Destructive Attack:** Ataque cuyo objetivo principal es dañar o destruir recursos. **Data Destruction:** Borrado deliberado de información sin posibilidad de recuperación. **Intrusion:** Acceso no autorizado que precede a la fase de destrucción.
Tipo de amenaza.	**Externa Activa:** Un adversario con alta motivación realiza acciones de sabotaje a gran escala.
Vector de ataque.	Infiltración inicial (phishing o vulnerabilidades) seguida de la ejecución de software tipo *wiper* que sobrescribe el Master Boot Record (MBR).
Impacto técnico / operativo.	Destrucción irreversible de la infraestructura IT, pérdida de continuidad de negocio a largo plazo y costos de reconstrucción masivos.
Medida de control recomendada.	**Segregación de redes** crítica, detección de anomalías en tiempo real (IDS/IPS), y una estrategia de **Disaster Recovery** basada en sitios alternos.

Conclusión

El análisis de los diez escenarios presentados en esta actividad permite concluir que la ciberseguridad no es un estado estático, sino un proceso dinámico que requiere una comprensión profunda de los servicios de seguridad definidos en el estándar X.800. A lo largo de los casos estudiados, se observa que la pérdida de la tríada Confidencialidad-Integridad-Disponibilidad (CIA) rara vez ocurre de forma aislada; por el contrario, los ataques modernos son multidimensionales y abusan de la confianza técnica y humana.

La aplicación de la terminología del RFC 4949 resulta indispensable para cualquier profesional del hacking ético. Como se demostró en los escenarios de "insider threats" y "misconfigurations", muchas de las vulnerabilidades más críticas no provienen de exploits sofisticados, sino de fallas conceptuales en el control de acceso y el manejo de privilegios. Esto subraya que la tecnología, por sí sola, es insuficiente si no va acompañada de políticas de monitoreo continuo y una cultura de prevención.

Finalmente, este ejercicio refuerza la importancia de la detección temprana y la respuesta ante incidentes. Mientras que las medidas preventivas como el MFA y los respaldos inmutables son barreras vitales, la capacidad de reconstruir una secuencia de eventos a través de un audit trail íntegro es lo que permite a las organizaciones aprender de los incidentes y fortalecer sus defensas. En última instancia, el dominio de estos marcos normativos es lo que distingue a un técnico de un analista de seguridad estratégico, capaz de proteger la infraestructura crítica en un entorno de amenazas en constante evolución.

Glosario (X.800 y RFC 4949)

Servicios de Seguridad (Modelo X.800)

Estos son los servicios que una red debe proveer para ser considerada segura:

Autenticación: Garantiza que la entidad (usuario o sistema) es quien dice ser.

Control de Acceso: Protección contra el uso no autorizado de recursos (quién puede entrar y a qué).

Confidencialidad: Asegura que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad: Garantiza que los datos no han sido alterados de manera no autorizada (ya sea por accidente o malicia).

No Repudio: Impide que alguien niegue haber realizado una acción (como enviar un correo o modificar un archivo).

Términos Fundamentales (RFC 4949)

Definiciones estándar para la comunicación técnica profesional:

Amenaza (Threat): Una circunstancia o evento con el potencial de causar daño a un sistema mediante su vulneración.

Ataque (Attack): Una acción deliberada que intenta evadir los servicios de seguridad y violar la política de seguridad de un sistema.

Audit Trail (Pista de Auditoría): Registros cronológicos de las actividades del sistema que permiten reconstruir y examinar una secuencia de eventos.

Credential Compromise: El acceso no autorizado a datos de autenticación (passwords, tokens).

Exposición (Exposure): Incidente donde datos sensibles son revelados a personas sin autorización, ya sea por error o por ataque.

Ingeniería Social: Técnicas para engañar a las personas y lograr que revelen información confidencial o realicen acciones que comprometan la seguridad.

Insider Threat: Un individuo con acceso legítimo que usa ese poder para causar daño a la organización.

Masquerade: Cuando una entidad se hace pasar por otra para obtener privilegios.

Phishing: Un método de engaño para obtener información sensible suplantando a una fuente confiable.

Ransomware: Tipo de malware que bloquea el acceso a los datos (normalmente cifrándolos) y exige un pago para liberarlos.

Vulnerabilidad: Una debilidad en un sistema que puede ser explotada por una amenaza para causar daño.

3. Tipos de Ataques según el RFC

Ataque Pasivo: Intenta aprender o utilizar información del sistema, pero no afecta los recursos del mismo (ej. espionaje de tráfico).

Ataque Activo: Intenta alterar los recursos del sistema o afectar su funcionamiento (ej. borrar archivos, cifrar servidores).

Bibliografía

Para el Estándar X.800:

International Telecommunication Union. (1991). Security architecture for Open Systems Interconnection for CCITT applications (Recommendation X.800). Recuperado de https://www.itu.int/rec/T-REC-X.800-199103-I/en

Para el RFC 4949:

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

Para conceptos de Hacking Ético

Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Syngress.