27 DE ENERO DE 2026

ANÁLISIS DE SERVICIOS DE SEGURIDAD

CIBERSEGURIDAD

173030 MAYELI SÁNCHEZ RAMÍREZ
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Introducción

La seguridad de la información en las redes de comunicación depende en gran medida de la infraestructura que las soporta, ya que routers, servidores, enlaces y dispositivos de red representan puntos críticos que pueden ser evaluados y explotados por un atacante. Por ello, el análisis de la seguridad no solo se centra en los datos, sino también en la postura real de seguridad de la red, identificando debilidades técnicas y operativas que afectan la comunicación y la continuidad de los servicios.

La recomendación ITU-T X.800 proporciona una arquitectura de seguridad que define los servicios y mecanismos necesarios para proteger los sistemas basados en el modelo OSI, estableciendo principios como autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad. Su enfoque es principalmente conceptual y estructural, orientado al diseño de controles de seguridad.

Por otro lado, el RFC 4949 funciona como el glosario oficial de seguridad en Internet, normalizando la terminología utilizada para describir amenazas, ataques, vulnerabilidades e impactos, lo que permite una comunicación técnica precisa y consistente.

En conjunto, X.800 y RFC 4949 se complementan para analizar escenarios reales de incidentes de seguridad, facilitando la identificación de servicios comprometidos, la correcta clasificación de amenazas y la propuesta de medidas de control coherentes y viables.

Escenario 1: 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 e integridad de datos y disponibilidad.
Definición(es) aplicable(s) RFC 4949.	• Multi-stage attack: ataque compuesto por múltiples fases encadenadas. • Data breach: divulgación no autorizada de información sensible. • Availability attack: ataque orientado a impedir el acceso a recursos.
Tipo de amenaza.	Externa (ataque mediante accesos no autorizados).
Vector de ataque.	Acceso inicial no autorizado seguido de exfiltración de datos y despliegue del ransomware.
Impacto técnico / operativo.	Disponibilidad nula en los servicios, no tener control acerca de la información y posible daño legal.

Medida de control recomendada.	Respaldos, segmentación de red y planes de respuesta a incidentes.

Escenario 2: 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.
Definición(es) aplicable(s) RFC 4949.	• Misconfiguration: configuración incorrecta de un sistema. • Exposure: exposición de información a partes no autorizadas.
Tipo de amenaza.	Interna (Errores de configuración y mala gestión de accesos).
Vector de ataque.	Servicios de almacenamiento que son accesibles desde internet por estar mal configurados.
Impacto técnico / operativo.	Filtración de datos.
Medida de control recomendada.	Una periódica revisión en la configuración y auditorias de seguridad n la nube.

Escenario 3: 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.	Confidencialidad e integridad de datos.
Definición(es) aplicable(s) RFC 4949.	• Supply chain attack: compromiso de un proveedor confiable para propagar código malicioso.
Tipo de amenaza.	Externa (se explota una relación de confianza desde o externo hacia lo interno).
Vector de ataque.	Actualizaciones de software en riesgo o comprometidas.
Impacto técnico / operativo.	Compromiso masivo de sistemas, propagación del ataque y pérdida de confianza del proveedor.
Medida de control recomendada.	Entornos de prueba, monitoreo de comportamiento después de cada actualización y control de integridad.

Escenario 4: 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: uso indebido de credenciales válidas. • Authentication failure: fallo conceptual del proceso de autenticación.
Tipo de amenaza.	Externa (ya que se realiza mediante campañas de ingeniería social).
Vector de ataque.	Sitios falsos de autenticación y/o correos fraudulentos.
Impacto técnico / operativo.	Filtración de información.
Medida de control recomendada.	Autenticación multifactor (varios pasos) y constante monitoreo.

Escenario 5: 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.	Integridad de datos y disponibilidad.
Definición(es) aplicable(s) RFC 4949.	• Data destruction: destrucción deliberada de información. • Availability attack: ataque contra la continuidad operativa.
Tipo de amenaza.	Externa (comprometen la red para después realizar movimientos internos para maximizar el impacto).
Vector de ataque.	Acceso previo con eliminación o cifrado de datos.
Impacto técnico / operativo.	Que sea imposible de recuperar.
Medida de control recomendada.	Separación de credenciales administrativas y respaldos inmutables.

Escenario 6: 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 de datos y control de acceso.
Definición(es) aplicable(s) RFC 4949.	• Insider threat: amenaza originada por personal con acceso legítimo.
Tipo de amenaza.	Interna (es causado por un empleado o usuario con acceso legítimo dentro de la organización).
Vector de ataque.	Uso indebido de privilegios no autorizados.
Impacto técnico / operativo.	Fuga de información y daño legal.
Medida de control recomendada.	Monitoreo de unidades internas.

Escenario 7: 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 de datos y No repudio.
Definición(es) aplicable(s) RFC 4949.	• Evidentiary integrity: integridad probatoria. • Audit trail: registro de eventos de seguridad.
Tipo de amenaza.	Interna (la amenaza es dentro del círculo, independientemente de cómo se haya originado el acceso).
Vector de ataque.	Modificación o cifrado de logs del sistema.
Impacto técnico / operativo.	Impacto forense e imposibilidad de autoría.
Medida de control recomendada.	Almacenamiento seguro de logs y registros inmutables.

Escenario 8: 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 causada por errores internos.
Tipo de amenaza.	Interna (producido por errores operativos y de gestión dentro).
Vector de ataque.	Actualización sin pruebas ni plan de reversión.
Impacto técnico / operativo.	Caída de servicios críticos y afectación global.
Medida de control recomendada.	Control de cambios y ambientes de prueba.

Escenario 9: 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: suplantación de identidad. • Phishing: engaño para obtener información sensible.
Tipo de amenaza.	Externa (mediante la suplantación de identidades el engaño a usuarios).
Vector de ataque.	Correos y sitios falsos que imitan entidades legítimas.
Impacto técnico / operativo.	Robo de información personal.
Medida de control recomendada.	Certificados digitales y campañas de concientización.

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 e Integridad de datos, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	• Destructive attack: ataque orientado a causar daño irreversible.
Tipo de amenaza.	Externa (se ejecutan acciones destructivas sobre lo interno).
Vector de ataque.	Exfiltración seguida de borrado y sabotaje de sistemas.
Impacto técnico / operativo.	Pérdida total de sistemas, información y capacidad operativa.
Medida de control recomendada.	Respaldos inmutables y respuesta inmediata a incidentes.

Conclusión

El análisis de los escenarios presentados demuestra que los incidentes de seguridad no se limitan únicamente a ataques externos sofisticados, sino que también pueden originarse dentro de la propia organización a partir de errores operativos, malas configuraciones o abuso de privilegios. El uso del marco ITU-T X.800 permitió identificar de forma estructurada los servicios de seguridad comprometidos en cada caso, mientras que el RFC 4949 facilitó una clasificación precisa y estandarizada de las amenazas, ataques e impactos asociados.

En el contexto latinoamericano, muchas organizaciones enfrentan limitaciones presupuestales, falta de personal especializado y una madurez desigual en materia de ciberseguridad, lo que incrementa

la probabilidad de incidentes internos y externos. Por ello, resulta fundamental priorizar medidas prácticas y viables como la correcta gestión de accesos, la implementación de autenticación multifactor, respaldos inmutables, monitoreo continuo y capacitación constante del personal.

Referencias

Material de clase. Tipos de pruebas de penetración: Pruebas de infraestructura de red. Presentación proporcionada por el docente Servando López Contreras.

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