ACTIVIDAD 02

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

Juan Diego Aguilar Espinoza
CON V SEGURIDAD INFORMATIOCA
Mtro. Servando López Contreras

El RFC 4949 es básicamente un diccionario de seguridad informática que define los términos mas importantes acerca de la ciberseguridad, define que es una amenaza o una vulnerabilidad.

El ITU-TX.800 explica qué servicios de seguridad se deben ofrecer para proteger un sistema siendo los principales Autenticación, Control de Acceso, Confidencialidad de Datos, Integridad de Datos, No Repudio.

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, Integridad, Disponibilidad
Definición(es) aplicable(s) RFC 4949.	Data breach, Availability attack y Multi-stage attack.
Tipo de amenaza.	Externa (grupo criminal)
Vector de ataque.	Acceso inicial no autorizado, exfiltración de datos y despliegue de ransomware.
Impacto técnico / operativo.	Sistemas caídos y filtración de datos sensibles.
Medida de control recomendada.	Backups inmutables, EDR/SIEM y segmentación.

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, Control de acceso.
Definición(es) aplicable(s) RFC 4949.	Misconfiguration, Exposure y Access control.
Tipo de amenaza.	Externa pasiva (exposición sin intrusión directa).
Vector de ataque.	Servicios de almacenamiento en la nube configurados como públicos sin autenticación.

Impacto técnico / operativo.	Fuga de datos sensibles y sanciones legales/multas..
Medida de control recomendada.	Auditorías de nube (CSPM), mínimo privilegio y cifrado.

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, Confidencialidad, Control de acceso.
Definición(es) aplicable(s) RFC 4949.	Supply chain attack, Integrity y Trust relationship abuse.
Tipo de amenaza.	Externa (con explotación indirecta de confianza).
Vector de ataque.	Software legítimo que fue infectado antes de ser distribuido.
Impacto técnico / operativo.	Acceso masivo de atacantes y pérdida de confianza en proveedores.
Medida de control recomendada.	Verificación de firmas, Zero Trust y monitoreo de comportamiento.

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, Control de acceso.
Definición(es) aplicable(s) RFC 4949.	Credential compromise, Authentication failure y Phishing.
Tipo de amenaza.	Externa (ingeniería social).
Vector de ataque.	Correos falsos que roban contraseñas reales para entrar al sistema.
Impacto técnico / operativo.	Intrusos con accesos válidos y riesgo de que se muevan por toda la red.

Medida de control recomendada.	MFA (Multifactor) obligatorio, capacitación y monitoreo de accesos.

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, Integridad.
Definición(es) aplicable(s) RFC 4949.	Data destruction, Availability attack e Integrity violation.
Tipo de amenaza.	Externa (actor malicioso con intención deliberada de daño).
Vector de ataque.	Acceso previo al entorno de respaldos y cifrado o eliminación de copias de seguridad antes del ataque principal.
Impacto técnico / operativo.	Pérdida permanente de datos e imposibilidad de recuperar la operación.
Medida de control recomendada.	Respaldos offline/inmutables y separación de llaves de acceso al backup.

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, Control de acceso.
Definición(es) aplicable(s) RFC 4949.	Insider threat, Confidentiality breach y Excessive privilege.
Tipo de amenaza.	Interna (empleado con acceso legítimo).
Vector de ataque.	Uso indebido de privilegios válidos para extraer bases de datos completas sin controles efectivos.
Impacto técnico / operativo.	Fuga de información sensible y pérdida de confianza institucional.
Medida de control recomendada.	Mínimo privilegio, división de tareas y monitoreo de comportamiento (UEBA).

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	Disponibilidad.
Definición(es) aplicables (RFC 4949)	Operational failure y Availability loss.
Tipo de amenaza	No maliciosa (error interno/operacional).
Vector de ataque	Actualización mal ejecutada sin pruebas previas ni mecanismos de reversión.
Impacto técnico / operativo	Caída global de servicios críticos y parálisis operativa.
Medida de control recomendada	Gestión de cambios, entornos de prueba y despliegues progresivos.

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.
Definición(es) aplicable(s) RFC 4949	Operational failure y Availability attack (no malicioso).
Tipo de amenaza	Interna (Accidental / Error de configuración).
Vector de ataque	Actualización de software fallida en pre-producción.
Impacto técnico / operativo	Caída masiva de servicios y pérdida de continuidad del negocio.
Medida de control recomendada	Ambientes de Staging, gestión de cambios y planes 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	Confidencialidad y Autenticación.
Definición(es) aplicable(s) RFC 4949	Masquerade (suplantar identidad) y Phishing (engaño).
Tipo de amenaza	Externa (Cibercrimen / Ingeniería Social).
Vector de ataque	Sitios web falsos (spoofing) y correos fraudulentos.
Impacto técnico / operativo	Robo masivo de datos y pérdida de confianza institucional.
Medida de control recomendada	DMARC/SPF (seguridad de correo), certificados SSL y capacitación.

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, Integridad y Disponibilidad.
Definición(es) aplicable(s) RFC 4949	Destructive attack (daño irreversible) y Data breach (robo previo).
Tipo de amenaza	Externa (Actores de amenazas avanzadas / Sabotaje).
Vector de ataque	Intrusión, escalada de poder y uso de Wipers (borradores).
Impacto técnico / operativo	Destrucción de infraestructura y borrado de evidencia forense.
Medida de control recomendada	Backups offline, detección EDR y Plan de Recuperación (DRP).

Conclusión

El análisis de los escenarios demuestra que la seguridad informática actual no puede realizarse de forma improvisada, si no que se necesitan normas especificas para ser efectiva por eso la relación entre RFC 4949 y el ITU-T X.800 nos permite identificar correctamente las vulnerabilidades y sus medidas de control.

Referencias bibliográficas

Shirey, R. W. (n.d.). RFC 4949: Internet Security Glossary, Version 2. Retrieved from https://datatracker.ietf.org/doc/html/rfc4949

Tsbmail. (n.d.). Retrieved from https://www.itu.int/rec/T-REC-X.800-199103-I/en