27-1-2026

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

Jasso Dávila Pedro Damian 176658

Pedro Damian Jasso Davila
Mtro. Servando López Contreras
CNO V: SEGURIDAD INFORMÁTICA

Introducción

La seguridad informática se basa en modelos y marcos conceptuales que permiten analizar de forma estructurada los incidentes que afectan a los sistemas de información. Uno de los modelos fundamentales es el definido por la Recomendación ITU-T X.800, que establece los seis servicios de seguridad: autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad. Estos servicios permiten identificar qué propiedades de la información han sido comprometidas durante un incidente.

Por otro lado, el RFC 4949 – Internet Security Glossary proporciona un vocabulario estandarizado de términos de ciberseguridad, permitiendo describir de manera precisa amenazas, vulnerabilidades, ataques e impactos. Mientras X.800 define qué aspecto de la seguridad se ve afectado, el RFC 4949 ayuda a explicar cómo y por qué ocurrió el incidente.

El análisis conjunto de ambos marcos es esencial en la seguridad informática actual, ya que facilita la comunicación profesional, la documentación técnica de incidentes y la toma de decisiones para implementar controles de protección. En esta actividad se analizan distintos escenarios reales de ciberataques y fallas operativas, identificando los servicios de seguridad comprometidos y aplicando la terminología técnica del RFC 4949.

Términos clave del RFC 4949 utilizados:

- **Attack:** Acción intencional para evadir servicios de seguridad y violar la política de seguridad de un sistema.
- **Threat:** Circunstancia o evento con potencial de causar daño explotando una vulnerabilidad.
- **Vulnerability:** Debilidad que puede ser explotada para comprometer la seguridad.
- **Data Breach:** Exposición o divulgación no autorizada de información sensible.
- **Availability Attack:** Ataque que busca impedir el acceso legítimo a sistemas o datos.
- **Masquerade:** Suplantación de identidad para obtener acceso no autorizado.
- **Phishing:** Técnica de ingeniería social para engañar a usuarios y obtener información confidencial.
- **Insider Threat:** Riesgo proveniente de una persona con acceso legítimo que hace uso indebido de sus privilegios.
- **Operational Failure:** Falla interna no maliciosa que afecta la disponibilidad de los servicios.

Caso 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	Confidencialidad de datos, Integridad de datos, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	Multi-stage attack, Data breach, Availability attack.
Tipo de amenaza.	Externa (grupo criminal).
Vector de ataque.	Acceso inicial no autorizado + exfiltración + cifrado de sistemas.
Impacto técnico / operativo.	Pérdida total de acceso a sistemas, filtración de datos sensibles
Medida de control recomendada.	Backups inmutables, EDR, segmentación de red, detección temprana

Caso 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	Control de acceso, Confidencialidad de datos.
Definición(es) aplicable(s) RFC 4949.	Misconfiguration, Exposure, Unauthorized Access.
Tipo de amenaza.	Externa oportunista.
Vector de ataque.	Acceso público a servicios mal configurados en la nube.
Impacto técnico / operativo.	Fuga de datos, sanciones legales y daño reputacional.
Medida de control recomendada.	Revisiones de configuración, auditorías de seguridad, control de acceso adecuado.

Caso 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	Integridad, Confidencialidad, Autenticación
Definición(es) aplicable(s) RFC 4949.	Supply chain attack, Code compromise.
Tipo de amenaza.	Externa a través de proveedor confiable.
Vector de ataque.	Actualización de software legítimo con código malicioso.
Impacto técnico / operativo.	Compromiso masivo de organizaciones, pérdida de confianza.
Medida de control recomendada.	Validación de integridad, monitoreo de comportamiento, control de aplicaciones.

Caso 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	Autenticación, Control de acceso, Confidencialidad.
Definición(es) aplicable(s) RFC 4949.	Phishing, Credential compromise, Authentication failure.
Tipo de amenaza.	Externa (ingeniería social).
Vector de ataque.	Correos y sitios falsos para robar credenciales.
Impacto técnico / operativo.	Acceso prolongado a sistemas internos.
Medida de control recomendada.	MFA, monitoreo de anomalías, capacitación a usuarios.

Caso 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	Disponibilidad, Integridad.
Definición(es) aplicable(s) RFC 4949.	Data destruction, Availability attack.
Tipo de amenaza.	Externa maliciosa
Vector de ataque.	Eliminación o cifrado de backups antes del ataque principal.
Impacto técnico / operativo.	Imposibilidad de recuperación de sistemas
Medida de control recomendada.	Backups offline/inmutables, separación de privilegios.

Caso 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	Confidencialidad, Control de acceso.
Definición(es) aplicable(s) RFC 4949.	Insider threat, Data exfiltration.
Tipo de amenaza.	Interna
Vector de ataque.	Extracción de bases de datos por usuario autorizado.
Impacto técnico / operativo.	Violación de datos, problemas legales.
Medida de control recomendada.	Principio de mínimo privilegio, DLP, monitoreo de actividad.

Caso 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	Integridad, No repudio.

Definición(es) aplicable(s) RFC 4949.	Audit trail compromise, Evidentiary integrity.
Tipo de amenaza.	Externa maliciosa.
Vector de ataque.	Alteración o cifrado de registros del sistema.
Impacto técnico / operativo.	Imposibilidad de análisis forense.
Medida de control recomendada.	Logs remotos, almacenamiento inmutable, SIEM.

Caso 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	Disponibilidad
Definición(es) aplicable(s) RFC 4949.	Operational failure.
Tipo de amenaza.	Interna no maliciosa.
Vector de ataque.	Actualización defectuosa sin pruebas previas.
Impacto técnico / operativo.	Caída global de servicios.
Medida de control recomendada.	Entornos de prueba, planes de rollback, gestión de cambios.

Caso 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	Autenticación, Confidencialidad.
Definición(es) aplicable(s) RFC 4949.	Masquerade, Phishing.
Tipo de amenaza.	Externa (ingeniería social).
Vector de ataque.	Sitios y correos falsificados.

Impacto técnico / operativo.	Robo de datos personales.
Medida de control recomendada.	SPF, DKIM, DMARC, campañas de concientización.

Caso 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	Confidencialidad, Integridad, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	Destructive attack, Data breach.
Tipo de amenaza.	Externa avanzada.
Vector de ataque.	Exfiltración seguida de destrucción de sistemas.
Impacto técnico / operativo.	Pérdida total de información y operaciones.
Medida de control recomendada.	Segmentación, monitoreo continuo, backups seguros, respuesta a incidentes.

Conclusión

El análisis de los escenarios demuestra que los incidentes de seguridad rara vez afectan un solo aspecto de la protección de la información. La aplicación del modelo ITU-T X.800 permitió identificar que servicios de seguridad fueron comprometidos en cada caso, mostrando que la confidencialidad, integridad y disponibilidad suelen verse afectadas de manera simultánea.

También, el uso de la terminología del RFC 4949 facilitó describir de forma técnica los tipos de amenazas, vulnerabilidades y ataques involucrados. La combinación de ambos proporciona una visión integral que fortalece la comprensión de los incidentes y apoya la definición de medidas de control adecuadas.

Referencias

ITU-T. (1991). *Recommendation X.800: Security Architecture for Open Systems Interconnection*. International Telecommunication Union.

Shirey, R. (2007). *RFC 4949: Internet Security Glossary, Version 2*. Internet Engineering Task Force (IETF).