UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CNO V SEGURIDAD INFORMATICA

ACTIVIDAD 02 ANÁLISIS DE SERVICIOS DE SEGURIDAD (X.800 Y RFC 4949)

Moreno Solís Gisela Geraldine 176522

Mtro. Servando López Contreras

Introducción

Por otro lado, el marco ITU-T X.800 establece “que” servicios de seguridad se deben garantizar (Autenticación, Control de Acceso, Confidencialidad de datos, Integridad de datos, Disponibilidad y No repudio), mientras que el RFC proporciona el vocabulario estándar para describir “cómo” y “por que” fallaron (tipos de ataques y vulnerabilidades). La unión de ambos permite pasar de una descripción anecdótica a un informe técnico profesional.

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), Integridad (datos cifrados/modificados), Disponibilidad (servidores inaccesibles).
DEFINICIÓN(ES) RFC 4949	Availability Attack
TIPO DE AMENAZA	Externa (Maliciosa deliberada).
VECTOR DE ATAQUE	Intrusión inicial no autorizada seguida de Lateral Movement.
IMPACTO TÉCNICO / OPERATIVO	Parada total de operaciones, daño reputacional por fuga de información sensible.
MEDIDA DE CONTROL RECOMENDADA	Respaldos inmutables (offline), segmentación de red y herramientas DLP (Data Loss Prevention).

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** (datos públicos), **Control de acceso** (permisos abiertos a "Everyone").
Definición(es) RFC 4949	Exposure.
Tipo de amenaza	Interna (Involuntaria / Error humano).
Vector de ataque	Error de configuración en permisos de almacenamiento (ej. S3 bucket abierto).
Impacto técnico / operativo	Violación de normativas de privacidad (GDPR/LFPDPPP), sanciones legales.
Medida de control recomendada	Implementación de CSPM (Cloud Security Posture Management) y auditoría continua de permisos.

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** (software alterado), **Autenticación** (se confió en la firma del proveedor comprometido).
Definición(es) RFC 4949	Supply Chain Attack, Trojan Horse, Malicious Logic.
Tipo de amenaza	Externa (estructural/sistémica).
Vector de ataque	Compromiso de la infraestructura de desarrollo del proveedor (CI/CD).
Impacto técnico / operativo	Compromiso masivo de clientes confiados; acceso persistente (backdoor).
Medida de control recomendada	Verificación de firmas, sandboxing de actualizaciones antes de despliegue en producción.

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** (vulnerada por robo), **Control de acceso** (acceso ilegítimo autorizado por el sistema).
Definición(es) RFC 4949	Credential Compromise, Advanced Persistent Threat (APT).
Tipo de amenaza	Externa (Ingeniería Social).
Vector de ataque	Phishing dirigido (Spear Phishing).
Impacto técnico / operativo	Espionaje corporativo prolongado, exfiltración silenciosa.
Medida de control recomendada	MFA (Autenticación Multifactor) obligatorio y monitoreo de comportamiento (UEBA).

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** (imposibilidad de recuperar), **Integridad** (destrucción de activos).
Definición(es) RFC 4949	*Data Destruction*, *Sabotage*, *Availability Attack*.
Tipo de amenaza	Externa (Maliciosa destructiva).
Vector de ataque	Escalación de privilegios para alcanzar repositorios de respaldo.
Impacto técnico / operativo	Pérdida total de datos, posible quiebra operativa de la organización.
Medida de control recomendada	Regla 3-2-1 de respaldos, almacenamiento en cinta o *air-gapped* (desconectado).

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 (exceso de privilegios otorgados).
Definición(es) RFC 4949	*Insider Threat*, *Theft* (robo), *Unauthorized Disclosure*.
Tipo de amenaza	Interna (Maliciosa).

Vector de ataque	Abuso de confianza y privilegios legítimos.
Impacto técnico / operativo	Fuga de propiedad intelectual, pérdida de ventaja competitiva.
Medida de control recomendada	Principio de Mínimo Privilegio (PoLP) y monitoreo de actividad de usuarios internos.

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	No Repudio (no se puede probar quién lo hizo), Integridad (de la evidencia).
Definición(es) RFC 4949	*Deception*, *Audit Trail modification*, *Accountability failure*.
Tipo de amenaza	Externa o Interna (Anti-forense).
Vector de ataque	Manipulación directa de archivos de sistema (*log tampering*).
Impacto técnico / operativo	Imposibilidad legal de imputar responsabilidad o entender el alcance del ataque.
Medida de control recomendada	Envío de logs en tiempo real a un servidor remoto (SIEM) con escritura *WORM* (Write Once Read Many).

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 Sugerida**
Servicios X.800 comprometidos	**Disponibilidad** (interrupción del servicio).
Definición(es) RFC 4949	*Operational Failure*, *Human Error*, *System Crash*.
Tipo de amenaza	Interna (No maliciosa / Accidental).

Vector de ataque	N/A (Fallo en procesos de QA/Control de calidad).
Impacto técnico / operativo	Interrupción masiva de negocio, pérdidas financieras por tiempo de inactividad.
Medida de control recomendada	Pruebas exhaustivas en entorno *staging* y despliegue escalonado (*Canary deployment*).

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 de origen de datos** (suplantada), **Confidencialidad** (datos entregados al atacante).
Definición(es) RFC 4949	*Spoofing*, *Phishing*, *Social Engineering*.
Tipo de amenaza	Externa (Fraude).
Vector de ataque	Correos masivos y dominios *typosquatting* (similares al real).
Impacto técnico / operativo	Robo de identidad de usuarios, pérdida de confianza en la institución.
Medida de control recomendada	Implementación de DMARC/SPF/DKIM en correos y monitoreo de marca (*Brand Protection*).

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, Disponibilidad (Compromiso total).
Definición(es) RFC 4949	*Destructive Attack*, *Wiper Malware*, *Sabotage*.

Tipo de amenaza	Externa (Ciberwarfare o Hacktivismo destructivo).
Vector de ataque	Ejecución de malware tipo *Wiper* tras obtener control total.
Impacto técnico / operativo	Destrucción irreversible de infraestructura lógica y datos.
Medida de control recomendada	Segmentación estricta de red y planes de Recuperación ante Desastres (DRP) probados.

Conclusión

Al analizar estos diez escenarios, me queda claro que el estándar X.800 y el RFC 4949 se complementan: uno nos dice qué debemos proteger (como la autenticación y el acceso) y el otro nos ayuda a ponerle el nombre correcto a las amenazas cuando esas protecciones fallan.
Lo que más me llamó la atención es que, en la mayoría de estos casos, el problema no fue que los hackers usaran una tecnología imposible de detener, sino que aprovecharon errores humanos y descuidos básicos, como contraseñas robadas (phishing) o configuraciones equivocadas en la nube.
Pensando en el entorno de Latinoamérica, creo que la lección más importante es que no siempre se necesita el software más caro para estar seguros. Muchas veces, basta con aplicar bien los fundamentos, como activar la autenticación de dos pasos (MFA) y revisar bien los permisos antes de salir a producción. Si cuidamos esos detalles básicos, podemos evitar la mayoría de los incidentes graves que vimos en la actividad.

Referencias Bibliográficas

1. Shirey, R. (2007). *RFC 4949: Internet Security Glossary, Version 2*. Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc4949
2. López Contreras, S. (2025). *Apuntes de clase: Fundamentos del Hacking Ético - Parcial I*. [Material de clase].
3. **International Telecommunication Union (ITU).** (1991). *Recommendation X.800: Security architecture for Open Systems Interconnection for CCITT applications*. ITU-T. https://www.itu.int/rec/T-REC-X.800