

# Actividad 02

---

CNOV SEGURIDAD INFORMATICA

Brian Salvador Espinoza Aguilar  
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

## Contenido

Introducción .....	2
Contexto del X.800 y RFC 4949 .....	2
Contenido.....	2
Conclusiones .....	5
Referencias.....	6

## Introducción

En este documento se verán escenarios en los que se presentan vulnerabilidades o situaciones, en las cuales se podrán identificar los puntos importantes de dichos escenarios, como cuales servicios de x.800 fueron comprometidos y también con la ayuda del RFC 4949 identificar el tipo de vulneración que paso, de estos archivos también importante mencionarlos porque nos ayudarán a obtener definiciones que nos serán útiles para saber que está pasando.

## Contexto del X.800 y RFC 4949

Para comenzar es importante saber de para que nos sirven y de que tratan estos dos conceptos el primero, la x.800 define seis servicios de seguridad fundamentales, aplicables a cualquier sistema de comunicación los cuales se definen como:

1. Autentificación: Verifica la identidad de las entidades que se comunican.
2. Control de acceso: Garantiza que solo usuarios autorizados puedan acceder a recursos.
3. Confidencialidad de los datos: Protege la información de accesos no autorizados durante la transmisión.
4. Integridad de los datos: Asegura que los datos no sean alterados durante la transmisión.
5. No repudio: Evita que una entidad niegue haber participado en una transacción.
6. Disponibilidad: Garantiza que los sistemas y servicios estén operativos cuando se necesiten.

Por otro lado, el RFC 4949 es uno de los documentos más importantes en materia de criminología y fundamentos conceptuales de seguridad informática. Es emitido por la IETF y sirve como un glosario oficial de los términos utilizados en el ámbito de la seguridad en las redes, criptografía y protocolos de internet.

El nombre completo es “RFC 4949: Internet Security Glossary, Version 2”, se le atribuye a Russell L. (Russ) Shirey, del U.S. Department of Defense (DoD) y fue publicado en Agosto de 2007, finalmente fue emitido por IETF (Internet Engineering Task Force) — organismo responsable de los estándares técnicos de Internet.

## Contenido

Escenarios para analizar	
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.**

<b>Servicio X.800 Comprometidos</b>	Integridad de los datos, Disponibilidad, control de acceso
<b>Definiciones aplicables RFC 4949.</b>	Multi-stage attack: ataque compuesto por fases. Data breach: divulgacion de datos no autorizada
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Compromiso de credenciales y pérdida del control del sistema al poder ejecutar un ransomware
<b>Impacto técnico / operativo</b>	Filtración de datos sensibles
<b>Medida de control / recomendada</b>	Copias de seguridad aisladas y verificación doble al entrar al sistema

**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.**

<b>Servicio X.800 Comprometidos</b>	Autentificación, Control de acceso Integridad de los datos
<b>Definiciones aplicables RFC 4949.</b>	Misconfiguration: Estado de un sistema accesible que crea vulnerabilidades Unauthorized Disclosure: Divulgacion no autorizada.
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Los atacantes buscan activamente estos errores con escáneres automatizados.
<b>Impacto técnico / operativo</b>	Perdida completa de confidencialidad
<b>Medida de control / recomendada</b>	Configuración de privilegios de privilegios de la nube y herramientas de seguridad en la nube.

**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.**

<b>Servicio X.800 Comprometidos</b>	Integridad de los datos, autentificación
<b>Definiciones aplicables RFC 4949.</b>	Supply Chain Attack: ataque que explota una relación de confianza
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Actualización de software comprometido, abuso de la cadena de suministro.
<b>Impacto técnico / operativo</b>	Violación masiva de integridad del sistema
<b>Medida de control / recomendada</b>	Verificar firmas digitales, retraso controlado de actualizaciones críticas.

**Escenario 04. Mediante campañas de phishing, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. Aunque la autenticación funcionó**

<b>técnicamente, el servicio de autenticación fue comprometido al basarse en credenciales robadas, afectando también el control de acceso.</b>	
<b>Servicio X.800 Comprometidos</b>	Autentificación, control de acceso
<b>Definiciones aplicables RFC 4949.</b>	Control compromise: credencial ha sido obtenida por una entidad no autorizada
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Phishing, los atacantes evitaron controles de autentificación.
<b>Impacto técnico / operativo</b>	Acceso no autorizado a sistema de datos
<b>Medida de control / recomendada</b>	Múltiple factor de autentificación, monitoreo de comportamiento de usuarios.
<b>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.</b>	
<b>Servicio X.800 Comprometidos</b>	Disponibilidad, Integridad de los datos
<b>Definiciones aplicables RFC 4949.</b>	Data destruction: datos inaccesibles, availability attack: ataque de denegación de servicios.
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Credenciales robadas, uso de ransomware para localizar y destruir.
<b>Impacto técnico / operativo</b>	Eliminación total del plan de recuperación
<b>Medida de control / recomendada</b>	Backups inmutables
<b>Escenario 06. Un empleado con acceso legítimo extrae bases de datos completas y las vende 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.</b>	
<b>Servicio X.800 Comprometidos</b>	Confidencialidad de datos, control de acceso
<b>Definiciones aplicables RFC 4949.</b>	Insider threat: Amenaza proveniente de personas dentro de la organización
<b>Tipo de amenaza</b>	Interna
<b>Vector de ataque</b>	Uso indebido de credenciales y permisos legítimos
<b>Impacto técnico / operativo</b>	Perdida masiva de confidencialidad
<b>Medida de control / recomendada</b>	Revisar y ajustar permisos regularmente
<b>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.</b>	
<b>Servicio X.800 Comprometidos</b>	Integridad de los datos, no repudio
<b>Definiciones aplicables RFC 4949.</b>	Audit Trail: Registro cronológico de actividades, evidentiary Integrity: Propiedad que asegura que la evidencia digital no ha sido alterada.
<b>Tipo de amenaza</b>	Externa

<b>Vector de ataque</b>	Usan acceso administrativo para modificar/eliminar logs
<b>Impacto técnico / operativo</b>	Imposibilidad de realizar un análisis forense efectivo
<b>Medida de control / recomendada</b>	Almacenamiento inmutable de logs
<b>Escenario 08.</b> 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	
<b>Servicio X.800 Comprometidos</b>	Disponibilidad, Integridad de los datos
<b>Definiciones aplicables RFC 4949.</b>	Operational Failure: fallo que resulta de errores de procedimientos operativos
<b>Tipo de amenaza</b>	Interna
<b>Vector de ataque</b>	Implementación de cambios sin pruebas adecuadas
<b>Impacto técnico / operativo</b>	Perdidas financieras masivas, Interrupción global de servicios
<b>Medida de control / recomendada</b>	Monitoreo proactivo
<b>Escenario 09.</b> 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.	
<b>Servicio X.800 Comprometidos</b>	Autenticación, confidencialidad de los datos
<b>Definiciones aplicables RFC 4949.</b>	masquerade: Ataque donde una entidad finge ser una entidad diferente
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Creación de sitios y correos falsos que imitan entidades legítimas
<b>Impacto técnico / operativo</b>	Robo de credenciales
<b>Medida de control / recomendada</b>	Atentificación del dominio
<b>Escenario 10.</b> 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	
<b>Servicio X.800 Comprometidos</b>	Confidencialidad de datos, integridad de datos, disponibilidad
<b>Definiciones aplicables RFC 4949.</b>	destructive Attack: "Ataque diseñado para causar daño físico o lógico permanente"
<b>Tipo de amenaza</b>	Externa
<b>Vector de ataque</b>	Código malicioso específico para borrar/sobrescribir datos
<b>Impacto técnico / operativo</b>	Pérdida total de datos

**Medida de control / recomendada**

Detección temprana y respuesta inmediata

## Conclusiones

Como conclusión puedo obtener que existen muchas variables y vulnerabilidades que se pueden explotar y con esto puedo identificar muchas de ellas para poder tener más conocimiento al respecto e intentar evitar esos fallos en la seguridad en el futuro.

## Referencias

- 1) [RFC 4949 - Glosario de Seguridad en Internet, Versión 2](#)