UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ACT02: ANÁLISIS DE SERVICIOS DE SEGURIDAD (X.800 Y RFC 4949)

CARRERA: ITI

ASIGNATURA: CON V SEGURIDAD INFORMÁTICA

CAVAZOS ZACARÍAS RODOLFO – 178823

MTRO. SERVANDO LÓPEZ CONTRERAS

27 DE ENERO DE 2026

Índice

Introducción

A lo largo de la historia encontramos casos sobre ataques maliciosos, robo de información, suplantación de la misma, y entre muchos casos más similares. Esto no se excluye en el mundo digital.

Para prevenir y reforzar la seguridad de las interconexiones y toda red que pueda existir, se crearon 2 documentos primordiales a la orden del público general para establecer estándares de protección y prevención ante las fechorías mencionadas anteriormente. Estos son el **ITU-T X.800 "Security Architecture for Open Systems Interconnection (OSI) for CCITT Applications",** y el **RFC 4949 (Request For Comments).**

El documento ITU-T X.800 fue diseñado y publicado como marco conceptual unificado, para el entendimiento, planificación e implementación de seguridad en redes. Complementando al modelo OSI permite la generación de capas transversales de seguridad, de manera que provee principios, servicios y mecanismos de defensa. Funge como base para normas posteriores (como ISO/IEC 7498-2 y las familias ISO 27000), protege datos, asegura autenticidad, garantiza disponibilidad y se establece en sus 6 servicios fundamentales de seguridad: **autenticación, control de acceso, confidencialidad de datos, integración de datos, no repudio y disponibilidad.** Además, tiene mecanismos específicos (directos hacia un servicio) y comunes (forma transversal) que implementan los servicios anteriores.

Por su parte, el documento **RFC 4949 (Request For Comments)**, glosario oficial emitido por la **IETF (Internet Engineering Task Force)** sirve y guía con sus definiciones a aquellos integrados en el ámbito de la seguridad de redes, criptografía y protocolos de Internet. Su función es prácticamente la de recopilar todos los **conceptos y definiciones** necesarias para determinar casos específicos en la rama a trabajar.

Casos presentados

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.	Autenticación, Confidencialidad de datos., Integridad de datos, Disponibilidad
Definición(es) aplicable(s) RFC 4949.	Multi-stage attack: Acceso no autorizado. Data breach: Exfiltración de información. Availabilty attack: Bloqueo de acceso a sistemas críticos.
Tipo de amenaza.	Externa
Vector de ataque.	Información sensible
Impacto técnico / operativo.	Indisponibilidad del sistema
Medida de control recomendada.	Un sistema robusto, validaciones y bloqueo ante ingresos desconocidos de datos.

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.	Control de acceso, Confidencialidad de los datos
Definición(es) aplicable(s) RFC 4949.	Misconfiguration: Parámetros de acceso mal definidos. Exposure: Datos accedibles de manera pública.
Tipo de amenaza.	Interna
Vector de ataque.	Almacenamiento en la nube

Impacto técnico / operativo.	Falla en el acceso a los datos (usuarios no autorizados)
Medida de control recomendada.	Mejores de medida de control de acceso, corrección de errores en la configuración de servicio.

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 un *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 de los sistemas, Confidencialidad.
Definición(es) aplicable(s) RFC 4949.	Supply chain attack: Proveedor legítimo comprometido., distribución de código malicioso como legítimo.
Tipo de amenaza.	Interna
Vector de ataque.	Compromiso de credenciales, filtración de información personal.
Impacto técnico / operativo.	Daño en credenciales de software
Medida de control recomendada.	Reposición de credenciales, recuperación de software corrompido.

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, control de acceso
Definición(es) aplicable(s) RFC 4949.	Credential compromise: Credenciales auténticas comprometidas. Authentication failure (conceptual):Autenticación inadecuada.
Tipo de amenaza.	Externa

Vector de ataque.	Credenciales de usuarios corporativos
Impacto técnico / operativo.	Bases de datos de usuarios corporativos y datos de la empresa.
Medida de control recomendada.	MFA, monitoreo constante de uso de credenciales.

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 una 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: Eliminación o cifrado de respaldos. Availability attack: Bloqueo de posible recuperación.
Tipo de amenaza.	Externa
Vector de ataque.	Respaldos de sistemas productivos
Impacto técnico / operativo.	Destrucción de datos, exposición de datos
Medida de control recomendada.	Respaldos offline o inmutables

Escenario 6

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 una intención deliberada de maximizar el daño. La inexistencia de respaldos *offline* o inmutables convierte el incidente en catastrófico.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad, control de acceso
Definición(es) aplicable(s) RFC 4949.	Insider threat: Atacante interno operando con credenciales legítimas.
Tipo de amenaza.	Interno
Vector de ataque.	Privilegios de acceso, datos vulnerados
Impacto técnico / operativo.	Bases de datos extraidas y vulneradas, acceso a terceros.

Medida de control recomendada.	Monitoreo constante, políticas de privilegio

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 la *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 los datos, no repudio.
Definición(es) aplicable(s) RFC 4949.	Evidentiary integrity: Evidencia sin valor técnico y legal. Audit trail: Imposibilito la reconstrucción secuencial de eventos.
Tipo de amenaza.	Externo
Vector de ataque.	Registros de sistema cifrados o alterados
Impacto técnico / operativo.	Probatorio y legal, técnico
Medida de control recomendada.	Monitoreo constante, políticas de privilegio

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 de planes de reversión amplificó el impacto.

Elemento	Respuesta
Servicios X.800 comprometidos.	Disponibilidad
Definición(es) aplicable(s) RFC 4949.	Operational failure: Actualización mal ejecutada.
Tipo de amenaza.	Interno
Vector de ataque.	Servicios críticos
Impacto técnico / operativo.	Probatorio y legal, técnico
Medida de control recomendada.	Pruebas previas, planes de revisión

Escenario 9

Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible Este escenario afecta la a**utenticación** 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
Definición(es) aplicable(s) RFC 4949.	Masquerade: Suplantación de identidades oficiales Phishing: Correos y sitios falsificados.
Tipo de amenaza.	Externo
Vector de ataque.	Suplantado de identidades legítimas e información sensible.
Impacto técnico / operativo.	Brecha de información de usuarios.
Medida de control recomendada.	Mecanismos de autenticación del dominio y 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 un *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
Definición(es) aplicable(s) RFC 4949.	Destructive attack: Ataque radical, eliminación completa de datos, sistemas y rastros.
Tipo de amenaza.	Interno
Vector de ataque.	Información sensible
Impacto técnico / operativo.	Sistemas de bases de datos
Medida de control recomendada.	Medidas de detección tempranas.

Conclusión

En un entorno digital caracterizado por amenazas constantes y escenarios de riesgo cada vez más complejos, los documentos **ITU-T X.800** y **RFC 4949** representan referencias esenciales para el análisis y la gestión de la seguridad de la información. Ambos proporcionan un marco conceptual y terminológico que permite comprender, estructurar y evaluar los incidentes de seguridad de manera sistemática.

El modelo **X.800** aporta una visión integral de la seguridad al definir servicios y mecanismos que complementan al modelo OSI, facilitando la identificación de los principios afectados y la implementación de controles adecuados. Por su parte, el **RFC 4949** estandariza el lenguaje técnico necesario para clasificar incidentes y comunicar sus impactos de forma precisa, tanto a nivel técnico como organizacional.

En conjunto, estos documentos permiten no solo analizar los incidentes desde una perspectiva técnica, sino también fortalecer la prevención, la toma de decisiones y la gestión del riesgo, consolidándose como fundamentos vigentes e indispensables en el ámbito de la ciberseguridad.

Referencias Bibliográficas

- International Telecommunication Union. (1991). *X.800: Security architecture for open systems interconnection for CCITT applications*. https://www.itu.int/rec/t-rec-x.800-199103-i/es
- Shirey, R. W. (2007). *Internet security glossary, version 2* (RFC 4949). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4949