27 DE ENERO DE 2026

ANÁLISIS DE SERVICIOS DE SEGURIDAD

ACTIVIDAD 2

BRUNO AXEL PUENTE LUNA 177876
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Contents

Introducción

El RFC 4949 es un **glosario** emitido por IETF (Internet Engineering Task Force), funcionando como estándar global para la jerga en Ciberseguridad; Define los riesgos como una expectativa de pérdida expresada como la probabilidad de que una amenaza concreta aproveche una vulnerabilidad concreta con un resultado perjudicial particular; Da múltiples definiciones para las palabras mas comunes en el ámbito, y de manera inversa, entrega palabras para usarse en el ámbito sirviendo de referencia exhaustiva que ayuda a la comunidad de Internet a mejorar la claridad de la documentación y el debate.

ITU-T X.800: "Security Architecture for Open Systems Interconnection (OSI) for CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) Applications", es un **marco conceptual** para implementar, planificar y entender la seguridad en redes de comunicación y sistemas interconectados. Describe el modelo de referencia básico para la interconexión de sistemas abiertos (ISA). Dicha Recomendación establece un marco para coordinar el desarrollo de recomendaciones existentes y futuras para la interconexión de sistemas. Suele complementar diferentes modelos como el modelo OSI, sirviendo de base para otras normas como ISO/IEC 7498, la familia ISO 27000 etc.

Estos elementos son de mucha ayuda al momento de relatar incidentes de seguridad, puesto que con el RFC 4949 podemos estandarizar nuestro documento para que sea legible a todo quien lo lea y tenga conocimientos de ciberseguridad, y el marco ITU-T X.800 para proteger los datos, asegurar la autenticidad de la comunicación, garantizar disponibilidad y ofrecer una estructura de referencia para implementar seguridad, con esto, nuestros reportes serán lo mas concisos para nuestros compañeros del campo, aplicando buenas practicas de ciberseguridad y defendiendo infraestructuras vulnerables contra ataques internos y externos.

En este reporte se revisarán diez casos de uso sobre análisis de servicios de seguridad, identificando de manera superficial los servicios X.800 comprometidos, para después aplicar las definiciones en el RFC 4949, y medir el tipo de amenaza; analizar el vector de ataque; revisar el impacto técnico y operativo; recomendando medidas de control para el caso.

Desarrollo

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
Servicio X.800 comprometidos.	Autenticación, Control de accesos, Confidencialidad de datos.
Definición(es) aplicable(s) RFC 4949	Authentication: Proceso de verificación de una afirmación de que una entidad o un recurso del sistema tiene un determinado valor de atributo. Authorization: Una autorización que se concede a una entidad del sistema para acceder a un recurso del sistema. Credential compromise: Incidente de seguridad en el que las credenciales quedan expuestas a un posible acceso no autorizado. Data confidentiality: La propiedad de que los datos no se revelan a las entidades del sistema a menos que hayan sido autorizadas para conocerlos. One-way encryption: Transformación irreversible de texto sin cifrar a texto cifrado, de tal manera que el texto sin cifrar no pueda recuperarse a partir del texto cifrado mediante procedimientos que no sean exhaustivos, incluso si se conoce la clave criptográfica.
Tipo de Amenaza	Externa (acceso no autorizado)
Vector de ataque	Data Breach, Credenciales comprometidas y encriptación de datos.
Impacto técnico / operativo	Perdida de datos, Compromiso con los usuarios, daños a la infraestructura.
Medida de control recomendada	Creación de respaldos, revisión de privilegios, detección de accesos remotos no autorizados, autenticaciones robustas, capacitaciones en uso de credenciales.

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
Servicio X.800 comprometidos.	Confidencialidad de datos
Definición(es) aplicable(s) RFC 4949	Confidentiality: propiedad de que la información no sea revelada a entidades no autorizadas. Exposure: condición en la que información queda accesible a entidades no autorizadas. Misconfiguration: configuración incorrecta que introduce una vulnerabilidad sin requerir explotación técnica avanzada. Unauthorized access: acceso a un recurso sin autorización.
Tipo de Amenaza	Externa, pasiva (exposición accidental sin intrusión activa).
Vector de ataque	Configuración incorrecta de mecanismos de control de acceso en servicios de almacenamiento, permitiendo acceso público.
Impacto técnico / operativo	Divulgación de información sensible, pérdida de confidencialidad, posibles sanciones legales y daño reputacional, aun sin evidencia de acceso malicioso.
Medida de control recomendada	Validación estricta de configuraciones de acceso, aplicación del principio de mínimo privilegio, auditorías periódicas de exposición y monitoreo de accesos no autorizados.

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
Servicio X.800 comprometidos.	Integridad de datos
Definición(es) aplicable(s) RFC 4949	Integrity: propiedad de que los datos y sistemas no sean modificados de manera no autorizada. Supply chain attack: ataque en el que un adversario compromete un elemento confiable de la cadena de suministro para distribuir código malicioso. Malicious code: software diseñado para infiltrarse o dañar un sistema sin el consentimiento del propietario. Trust: expectativa de que una entidad o componente se comporte de manera predecible y legítima.
Tipo de Amenaza	Externa, activa (abuso de una relación de confianza legítima).
Vector de ataque	Compromiso del proveedor de software y distribución de actualizaciones firmadas que contienen código malicioso.
Impacto técnico / operativo	Violación de la integridad del software, pérdida de confianza en actualizaciones legítimas, accesos no autorizados posteriores y posible exposición de información sensible.
Medida de control recomendada	Verificación independiente de integridad de actualizaciones, controles estrictos sobre la cadena de suministro, monitoreo de comportamiento del software y validación continua de confianza en proveedores.

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
Servicio X.800 comprometidos.	Autenticación, Control de acceso
Definición(es) aplicable(s) RFC 4949	Authentication: proceso de verificación de la identidad declarada de una entidad. Credential compromise: divulgación o robo de credenciales que permite a un atacante hacerse pasar por una entidad legítima. Authentication failure: falla del servicio de autenticación al aceptar credenciales comprometidas, aun cuando el mecanismo funcione correctamente. Authorization: concesión de privilegios de acceso a recursos.
Tipo de Amenaza	Externa, activa (suplantación de identidad mediante credenciales robadas).
Vector de ataque	Phishing para obtención de credenciales válidas y uso prolongado de accesos legítimos sin detección.
Impacto técnico / operativo	Acceso persistente no autorizado, uso indebido de privilegios legítimos, pérdida de control sobre sistemas y posible exposición de información.
Medida de control recomendada	Autenticación multifactor, monitoreo de comportamiento anómalo, detección de uso indebido de credenciales y revisión periódica de privilegios.

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
Servicio X.800 comprometidos.	Disponibilidad, Integridad de datos
Definición(es) aplicable(s) RFC 4949	Availability: propiedad de que los sistemas y la información estén accesibles y utilizables cuando se requieran. Availability attack: acción deliberada destinada a degradar o impedir el acceso a servicios o datos. Data destruction: eliminación o inutilización intencional de datos. Integrity: propiedad de que la información no sea modificada o destruida de manera no autorizada.
Tipo de Amenaza	Externa, activa (ataque deliberado para maximizar impacto).
Vector de ataque	Eliminación o cifrado de respaldos como fase previa al cifrado de sistemas productivos.
Impacto técnico / operativo	Pérdida total de capacidad de recuperación, interrupción prolongada de operaciones, daño severo a la continuidad del negocio.
Medida de control recomendada	Respaldos offline o inmutables, separación de privilegios sobre sistemas de backup, monitoreo de operaciones destructivas y pruebas periódicas de recuperación.

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
Servicio X.800 comprometidos.	Confidencialidad de datos, Control de acceso
Definición(es) aplicable(s) RFC 4949	Confidentiality: propiedad de que la información no sea divulgada a entidades no autorizadas. Insider threat: amenaza originada por una entidad interna con acceso autorizado que utiliza ese acceso de forma indebida. Authorization: concesión de derechos y privilegios de acceso a recursos. Excessive privilege: asignación de privilegios superiores a los necesarios para cumplir una función.
Tipo de Amenaza	Interna, activa (abuso deliberado de privilegios legítimos).
Vector de ataque	Uso indebido de accesos legítimos para extracción y exfiltración de bases de datos completas.
Impacto técnico / operativo	Divulgación masiva de información sensible, pérdida de confianza, impacto legal y reputacional significativo.
Medida de control recomendada	Aplicación estricta del principio de mínimo privilegio, monitoreo de actividades de usuarios privilegiados, segregación de funciones y auditorías de acceso.

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
Servicio X.800 comprometidos.	Integridad de datos, No repudio
Definición(es) aplicable(s) RFC 4949	Integrity: propiedad de que los datos no sean alterados de manera no autorizada. Non-repudiation: garantía de que una entidad no pueda negar la autoría de una acción realizada. Evidentiary integrity: propiedad que asegura que la evidencia digital mantiene su valor probatorio. Audit trail: registro cronológico de eventos que permite rastrear acciones y responsabilidades.
Tipo de Amenaza	Externa, activa (alteración deliberada de registros).
Vector de ataque	Cifrado o modificación de registros del sistema para impedir reconstrucción de eventos
Impacto técnico / operativo	Imposibilidad de análisis forense, pérdida de evidencia confiable, afectación legal y probatoria, debilitamiento de procesos de responsabilidad.
Medida de control recomendada	Protección de registros mediante controles de integridad, almacenamiento inmutable, separación de privilegios y aseguramiento del audit trail.

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
Servicio X.800 comprometidos.	Disponibilidad
Definición(es) aplicable(s) RFC 4949	Availability: propiedad de que sistemas y servicios estén accesibles y operativos cuando se requieren. Operational failure: falla originada por errores internos de operación, configuración o mantenimiento, sin intervención de un atacante.
Tipo de Amenaza	Interna, no maliciosa (falla operacional).
Vector de ataque	Actualización defectuosa ejecutada sin pruebas previas ni mecanismos de reversión.
Impacto técnico / operativo	Interrupción simultánea de servicios críticos, degradación severa de la continuidad operativa a escala global.
Medida de control recomendada	Pruebas controladas de actualizaciones, planes de reversión, gestión de cambios y mecanismos de redundancia operativa.

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
Servicio X.800 comprometidos.	Autenticación, Confidencialidad de datos
Definición(es) aplicable(s) RFC 4949	Authentication: proceso de verificación de la identidad declarada de una entidad. Masquerade: ataque en el que una entidad se hace pasar por otra legítima. Phishing: técnica de ingeniería social utilizada para obtener información sensible mediante engaño. Confidentiality: propiedad de que la información no sea divulgada a entidades no autorizadas.
Tipo de Amenaza	Externa, activa (ingeniería social y suplantación de identidad).
Vector de ataque	Sitios web y correos electrónicos falsificados que imitan entidades legítimas para recolectar información sensible.
Impacto técnico / operativo	Obtención no autorizada de credenciales y datos personales, pérdida de confianza institucional y posibles consecuencias legales.
Medida de control recomendada	Mecanismos de autenticación de dominio, fortalecimiento de autenticación de identidad y programas de concientización de usuarios.

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
Servicio X.800 comprometidos.	Confidencialidad de datos, Integridad de datos, Disponibilidad
Definición(es) aplicable(s) RFC 4949	Confidentiality: propiedad de que la información no sea divulgada a entidades no autorizadas. Integrity: propiedad de que los datos y sistemas no sean alterados o destruidos de manera no autorizada. Availability: propiedad de que sistemas y datos estén accesibles cuando se requieren. Destructive attack: ataque cuyo objetivo principal es causar daño irreversible mediante destrucción de datos o sistemas.
Tipo de Amenaza	Externa, activa (destrucción deliberada de sistemas e información).
Vector de ataque	Exfiltración de información seguida de eliminación o destrucción de sistemas para borrar rastros y maximizar daño.
Impacto técnico / operativo	Pérdida irreversible de información, colapso operativo, imposibilidad de recuperación y afectación crítica a la continuidad del negocio.
Medida de control recomendada	Detección temprana de actividades anómalas, segmentación de sistemas críticos, controles de integridad y disponibilidad, y mecanismos de recuperación resiliente.