ACTIVIDAD 02

Seguridad Informatica

27 DE ENERO DE 2026

CASTILLO OLVERA CARLOS RENÉ

182033

En la actualidad, los incidentes de seguridad informática son cada vez más frecuente. Muchas veces, una mala configuración, un error humano o el abuso de una relación de confianza pueden generar consecuencias tan graves como un ataque. Por eso, resulta importante contar con modelos que permitan analizar de manera clara qué falló y el ¿por qué?.

En este trabajo se analizan distintos escenarios de incidentes de seguridad utilizando los servicios de seguridad definidos en la recomendación ITU-T X.800 y la terminología del RFC 4949. El modelo X.800 ayuda a identificar qué aspectos de la seguridad fueron comprometidos, como la confidencialidad, la integridad o la disponibilidad, mientras que el RFC 4949 aporta un lenguaje común para describir amenazas, ataques y fallas de forma precisa.

A través del estudio de casos como ransomware, errores de configuración, amenazas internas y ataques a “empresas”, se busca demostrar que ambos marcos se complementan y facilitan una mejor comprensión de los incidentes. Esto permite analizar situaciones reales de manera más ordenada y coherente, fortaleciendo la capacidad de documentar y explicar vulneraciones de seguridad.

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 X800 Comprometidos	Control de Acceso, Autenticacion.
Definiciones Aplicables del RFC 4949	Multi-stage Attack: ataque ejecutado en fases sucesivas con distintos objetivos. Data Breach: compromiso y exposición de información sensible. Availability Attack: ataque orientado a impedir el acceso legítimo a sistemas y datos.
Tipo de amenaza	Externa .
Vector de ataque	Acceso inicial no autorizado, filtración de datos.
Impacto técnico / operativo	Acceso no autorizado, Robo de identidad
Medida de control recomendada	Firma digital (para autenticación y no repudio), Control de acceso.

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 X800 Comprometidos	Confidencialidad de datos, Control de acceso.
Definiciones Aplicables del RFC 4949	Misconfiguration: configuración incorrecta de sistemas o servicios. Exposure: puesta a disposición no intencional de información sensible.
Tipo de amenaza	Interna.
Vector de ataque	Configuración pública o permisos excesivos en servicios de almacenamiento en la nube.
Impacto técnico / operativo	Accesos no autorizados, Información desprotegida.
Medida de control recomendada	Gestión de seguridad (políticas, auditorías, monitoreo), Etiquetado de seguridad.

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 X800 Comprometidos	Control de acceso, Integridad de datos.
Definiciones Aplicables del RFC 4949	Supply Chain Attack: ataque que compromete un componente legítimo para afectar a múltiples víctimas.
Tipo de amenaza	Interna
Vector de ataque	Compromiso del proveedor y distribución de actualización con programa malicioso
Impacto técnico / operativo	Actualizaciones alteradas, control de acceso no autorizado.
Medida de control recomendada	Control de acceso, Ruteo seguro.

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, Control de acceso, Confidencialidad.
Definición(es) aplicable(s) RFC 4949.	Credential Compromise: exposición o robo de credenciales válidas. Authentication Failure: falla del servicio de autenticación al aceptar identidades no legítimas.
Tipo de amenaza.	Externa (atacante no autorizado utilizando credenciales válidas).
Vector de ataque.	Campañas de phishing para obtención de credenciales, seguidas de accesos persistentes.
Impacto técnico / operativo.	Acceso no detectado, manipulación de sistemas y aumento del riesgo de ataques.
Medida de control recomendada.	Implementación de MFA, monitoreo de comportamiento de los usuarios.

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, Integridad.
Definición(es) aplicable(s) RFC 4949.	Availability Attack: ataque destinado a impedir el acceso legítimo a sistemas o datos. Data Destruction: eliminación o corrupción deliberada de información.
Tipo de amenaza.	Externa (ataque deliberado por grupos de ransomware).
Vector de ataque.	Compromiso inicial seguido de eliminación o cifrado de respaldos y posterior cifrado de sistemas productivos.
Impacto técnico / operativo.	Imposibilidad de recuperación, pérdidas económicas.
Medida de control recomendada.	Control de privilegios sobre sistemas.

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.
Definición(es) aplicable(s) RFC 4949.	Insider Threat: amenaza originada por personal con acceso autorizado.
Tipo de amenaza.	Interna.
Vector de ataque.	Acceso autorizado a bases de datos y extracción deliberada de información.
Impacto técnico / operativo.	Pérdida de información sensible, perdida de confianza.
Medida de control recomendada.	Control de acceso, Cifrado (para confidencialidad).

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.	Integridad, No repudio.
Definición(es) aplicable(s) RFC 4949.	Evidentiary Integrity: preservación de la validez de la evidencia digital. Audit Trail: registros cronológicos que permiten reconstruir eventos.
Tipo de amenaza.	Externa.
Vector de ataque.	Cifrado o modificación de registros del sistema y de auditoría.
Impacto técnico / operativo.	Imposibilidad de reconstruir eventos.
Impacto probatorio / legal.	Invalidez de evidencia digital.
Medida de control recomendada.	ontroles de integridad.

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
Servicios X.800 comprometidos.	Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	Operational Failure: falla causada por errores humanos o técnicos no maliciosos.
Tipo de amenaza.	Interna.
Vector de ataque.	Actualización mal ejecutada.
Impacto técnico / operativo.	Caída de servicios críticos, interrupción de operaciones.
Medida de control recomendada.	Gestión de eventos y alarmas, Ruteo seguro.

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, Confidencialidad.
Definición(es) aplicable(s) RFC 4949.	Masquerade: suplantación de identidad de una entidad legítima. Phishing: obtención fraudulenta de información mediante engaño.
Tipo de amenaza.	Externa.
Vector de ataque.	Replicar los sitios web oficiales y envío de correos de ffraude.
Impacto técnico / operativo.	Exposición de datos sensibles.
Medida de control recomendada.	Monitoreo de dominios falsos.

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.
Definición(es) aplicable(s) RFC 4949.	Destructive Attack: ataque orientado a causar daño irreversible. Data
Tipo de amenaza.	Externa.
Vector de ataque.	Exfiltración seguida de borrado y destrucción de sistemas.
Impacto técnico / operativo.	Pérdida total de información, interrupción definitiva de servicios.
Medida de control recomendada.	Detección temprana, monitoreo continuo.

El análisis de los escenarios demuestra que los incidentes de seguridad rara vez afectan un solo aspecto del sistema. En la mayoría de los casos, varios servicios de seguridad del modelo X.800 se ven comprometidos al mismo tiempo, lo que amplifica el impacto del incidente y dificulta su contención y recuperación.

El uso del RFC 4949 permitió describir cada escenario con mayor claridad, diferenciando entre ataques externos, amenazas internas y fallas operativas sin intención maliciosa. Esto evidencia que la seguridad no depende únicamente de la presencia de atacantes, sino también de decisiones internas, configuraciones incorrectas y falta de controles adecuados.

En conclusión, el uso combinado de X.800 y RFC 4949 resulta muy útil para analizar incidentes de seguridad de forma práctica y comprensible. Mientras X.800 permite identificar qué servicio de seguridad fue afectado, el RFC 4949 ayuda a explicar cómo ocurrió el incidente, facilitando un análisis más completo y alineado con situaciones reales.

FUENTES

- ITU-T. (1991). Recomendación X.800: Arquitectura de seguridad para la interconexión de sistemas abiertos. Unión Internacional de Telecomunicaciones. https://www.itu.int/rec/t-rec-x.800-199103-i/es

- IETF. (2007). RFC 4949 – Internet Security Glossary, Version 2. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc4949