



UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

ACTIVIDAD 02: Análisis de servicios de seguridad  
(X.800 y RFC 4949)

Carrera: ITI

Asignatura: CNO V Seguridad Informática

Pablo de Jesús Salazar Hernández - 171580

Mtro. Servando López Contreras

27/01/2026

## Introducción

La seguridad de la información es un pilar fundamental en el mundo digital actual. Para garantizarla, se han desarrollado estándares y marcos conceptuales que permiten definir, organizar y aplicar medidas de protección de manera coherente y universal. Entre los más relevantes se encuentran la Recomendación X.800 de la UIT-T y el RFC 4949 de la IETF, ambos documentos que, aunque surgieron en contextos distintos, comparten el objetivo de establecer un lenguaje común y una estructura sólida para abordar la seguridad informática.

## 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  |
|--|--|
| <b>Servicios X.800 Comprometidos</b>         | Integridad, confidencialidad de los datos, disponibilidad  |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Multi-stage attack: Ataque multiple en distintos lugares<br>data breach: brecha de información y availability attack |
| <b>Tipos de amenaza</b>                      | Externa (Acceso inicial no autorizado)   |
| <b>Vector de ataque</b>                      | Ausencia de respaldos inmutables, sin detección temprana   |
| <b>Impacto técnico / operativo</b>           | Perdida total de información crucial, filtración de información sensible.  |
| <b>Medida de control recomendada</b>         | MFA robusto, sistema de alertas de acceso, respaldos disponibles.  |

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   |
|--|---|
| <b>Servicios X.800 Comprometidos</b>         | Control de acceso, confidencialidad de datos  |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Misconfiguration: falta de configuración correcta para su uso enfocado<br>Exposure: exposición de los datos sensibles públicamente faltando a la privacidad |

|                                      |   |
|--------------------------------------|---|
| <b>Tipos de amenaza</b>              | Interna (fallo en la configuración de almacenamiento de datos en sus servicios)     |
| <b>Vector de ataque</b>              | Sin intrusiones activas, solo malas configuraciones                                 |
| <b>Impacto técnico / operativo</b>   | Legal y reputacional  |
| <b>Medida de control recomendada</b> | Validación temprana de controles de acceso, disponibilidad de servicios confiables. |

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  |
|--|--|
| <b>Servicios X.800 Comprometidos</b>         | Integridad de datos, confidencialidad de los datos   |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Supply chain attack: Ataque a agentes asociados a un servicio usando la gente confiable como una cadena de conexión rígida.                                    |
| <b>Tipos de amenaza</b>                      | Externa (Distribución de FakeUpdates en diversas organizaciones)   |
| <b>Vector de ataque</b>                      | Compromiso de actualizaciones legítimas, impacto social de legitimidad   |
| <b>Impacto técnico / operativo</b>           | Legal y reputacional   |
| <b>Medida de control recomendada</b>         | Control de acceso de credenciales, MFA robusto, identificador de tareas, avisos previos de acceso, doble confirmación interna para la distribución de software |

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  |
|--|--|
| <b>Servicios X.800 Comprometidos</b>         | Autenticación, control de acceso   |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Credential compromise con authentication failure conceptual: Comprometer las credenciales válidas mediante sistemas operativos, fallando el sistema de autenticación por ser credenciales válidas. |
| <b>Tipos de amenaza</b>                      | Externa (Robo de credenciales válidas)   |
| <b>Vector de ataque</b>                      | Compromiso de credenciales válidas, falta de capacitación a personal sobre los posibles riesgos en correos electrónicos  |

|                                      |   |
|--------------------------------------|---|
| <b>Impacto técnico / operativo</b>   | Perdida de control total para acceder, pérdida de información sensible. |
| <b>Medida de control recomendada</b> | MFA Robusto, monitoreo de comportamiento avanzado                       |

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   |
|--|---|
| <b>Servicios X.800 Comprometidos</b>         | Disponibilidad, integridad de datos.  |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Data destruction: cifrado o eliminación de datos importantes.<br>availability attack: ataque o cifrado de respaldos |
| <b>Tipos de amenaza</b>                      | Externa (Intrusión a bases de datos)  |
| <b>Vector de ataque</b>                      | Filtración en acceso a bases de datos, falta de confirmación de control de acceso                                   |
| <b>Impacto técnico / operativo</b>           | Imposibilidad de recuperar información perdida de información sensible.   |
| <b>Medida de control recomendada</b>         | MFA Robusto, monitoreo de comportamiento avanzado   |

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   |
|--|---|
| <b>Servicios X.800 comprometidos.</b>        | Confidencialidad, control de acceso   |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Insider threat: peligro interno, personal con accesos a información sensible. |
| <b>Tipo de amenaza.</b>                      | Interno   |
| <b>Vector de ataque.</b>                     | Privilegios de acceso, datos vulnerados                                       |
| <b>Impacto técnico / operativo.</b>          | Bases de datos extraídas y vulneradas, acceso a terceros.                     |
| <b>Medida de control recomendada.</b>        | Monitoreo constante, políticas de privilegio                                  |

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  |
|--|--|
| <b>Servicios X.800 comprometidos.</b>        | Integridad de los datos, no repudio.   |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Evidentiary integrity: integridad de los archivos alterados o cifrados<br>Audit Trail: Imposibilidad de poder demostrar que ocurrió ni quien fue el responsable. |
| <b>Tipo de amenaza.</b>                      | Externo  |
| <b>Vector de ataque.</b>                     | Registros de sistema cifrados o alterados  |
| <b>Impacto técnico / operativo.</b>          | Probatorio y legal, técnico  |
| <b>Medida de control recomendada.</b>        | Monitoreo constante, políticas de privilegio   |

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   |
|--|---|
| <b>Servicios X.800 comprometidos.</b>        | Integridad de los datos, no repudio.  |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Evidentiary integrity: integridad de los servicios usados a nivel global<br>operational failure: falla operacional de los servicios |
| <b>Tipo de amenaza.</b>                      | Externo   |
| <b>Vector de ataque.</b>                     | Registros de sistema cifrados o alterados   |
| <b>Impacto técnico / operativo.</b>          | Probatorio y legal, técnico   |
| <b>Medida de control recomendada.</b>        | Monitoreo constante, políticas de privilegio  |

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   |
|--|---|
| <b>Servicios X.800 comprometidos.</b>        | Autenticación, confidencialidad                             |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Masquerade, phishing  |
| <b>Tipo de amenaza.</b>                      | Externo   |
| <b>Vector de ataque.</b>                     | Suplantado de identidades legítimas e información sensible. |
| <b>Impacto técnico / operativo.</b>          | Brecha de información de usuarios.                          |
| <b>Medida de control recomendada.</b>        | 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 destructive attack, donde el objetivo no es solo el lucro, sino el daño irreversible. La detección tardía impidió cualquier contención efectiva.

| Elemento                                     | Respuesta                                    |
|--|--|
| <b>Servicios X.800 comprometidos.</b>        | Confidencialidad, Integridad, disponibilidad |
| <b>Definición(es) aplicable(s) RFC 4949.</b> | Destructive attack                           |
| <b>Tipo de amenaza.</b>                      | Interno                                      |
| <b>Vector de ataque.</b>                     | Información sensible                         |
| <b>Impacto técnico / operativo.</b>          | Sistemas de bases de datos                   |
| <b>Medida de control recomendada.</b>        | Medidas de detección tempranas.              |