UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

# ACT. 2 ANÁLISIS DE SERVICIOS DE SEGURIDAD

CNO V: Seguridad Informática

UPSLP

181760 – Josué Emiliano Rosales Ramírez

# 1 CONTENIDO

# 2 INTRODUCCIÓN

En este trabajo, se estará revisando distintos escenarios de ataques relacionadas con la ciberseguridad, con el fin de utilizar los marcos X.800 y el RFC 4949 para analizar correctamente las áreas comprometidas, tipos de amenazas y mecanismos sugeridos. Esta actividad ayudará para que el alumno pueda adentrarse ante este importante conocimiento de la seguridad cibernética.

## 2.1 GLORARIO

### 2.1.1 X.800

Conocido realmente como *ITU-T X.800: "Security Architecture for Open Systems Interconnection (OSI) for CCITT Applications* es una "RECOMENDACIÓN" que proporciona un panorama muy claro para entender, planificar e identificar la seguridad en las redes y sistemas interconectados.

### 2.1.2 RFC-4949

Es un glosario oficial de los términos utilizados en la seguridad cibernéti ca.

# 3 ESCENARIOS

## 3.1 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 X.800 comprometidos.** | Control de acceso, Confidencialidad de datos, disponibilidad |
| **Definición(es) aplicable(s) RFC 4949.** | access control center (Es en donde se controlan los accesos a permisos, credenciales, privilegios de un sistema ), data confidentiality (Informacion que no esta para el publico ni siquiera para un sector de los internos, solo se accede y se publica con acceso autorizado.)<br>Data breach (fuga de información sensible) |
| **Tipo de amenaza.** | Extorsion |
| **Vector de ataque.** | Credenciales de acceso no autorizadas, |
| **Impacto técnico / operativo** | Exposición de datos sensibles |
| **Medida de control recomendada.** | Control de acceso y cifrado de información |

## 3.2 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 X.800 comprometidos.** | Control de acceso, confidenciabilidad de datos |
| **Definición(es) aplicable(s) RFC 4949.** | Exposure (Cuando datos son lanzados al público sin una autorización previa), misconfiguration (Errores en la instalación correcta de sistemas de redes). |
| **Tipo de amenaza.** | Exposición de datos |
| **Vector de ataque.** | Mala configuración del sistema y de permisos |
| **Impacto técnico / operativo** | Reputación |
| **Medida de control recomendada.** | Mejorar el control de accesos |

## 3.3 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 X.800 comprometidos.** | Autenticación, integridad y confidencialidad de datos |
| **Definición(es) aplicable(s) RFC 4949.** | Trust chain (camino certificado y ancla de confianza) |
| **Tipo de amenaza.** | Integridad de los sistemas de los clientes |
| **Vector de ataque.** | Proveedor de software |
| **Impacto técnico / operativo** | Reputación, pausa de servicio de los clientes. |
| **Medida de control recomendada.** | Siempre validar la entrada de software, |

## 3.4 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.** | Control de acceso, autenticación |
| **Definición(es) aplicable(s) RFC 4949.** | Credential compromise (credenciales que fueron expuestas ante potenciales accesos no autorizados) |
| **Tipo de amenaza.** | Saltarse los parámetros de seguridad |
| **Vector de ataque.** | Phishing |
| **Impacto técnico / operativo** | Limpieza de usuarios no autorizados, análisis de que fue lo que hicieron los atacantes en el tiempo que no levantaron alertas |
| **Medida de control recomendada.** | MFA y constantes monitoreos de accesos |

## 3.5 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 de datos |
| **Definición(es) aplicable(s) RFC 4949.** | Data destruction (borrado de información sensible), availability attack (ataque directo a la disponibilidad del sistema o de recursos de sistemas que lo hacen inutilizable) |
| **Tipo de amenaza.** | Intención deliberada de maximización de daño |
| **Vector de ataque.** | Credenciales robadas o phishing |
| **Impacto técnico / operativo** | Pérdida total de datos |
| **Medida de control recomendada.** | MFA, respaldos offline |

## 3.6 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 de datos |
| **Definición(es) aplicable(s) RFC 4949.** | Insider threat (un usuario que tiene acceso al sistema y está dentro del perímetro de seguridad, volviéndolo una amenaza si se lo propone o hasta en casos de negligencia), |
| **Tipo de amenaza.** | Interno y externo por la información vendida |
| **Vector de ataque.** | Empleado con accesos |
| **Impacto técnico / operativo** | Reputación, investigación del usuario en cuestión, investigación de que información ha sido vendida |
| **Medida de control recomendada.** | Control de privilegios al mínimo por roles y módulos establecidos. |

## 3.7 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.** | No repudio, integridad de los datos |
| **Definición(es) aplicable(s) RFC 4949.** | Evidentiary integrity (Es el que la evidencia no ha sido manipulada o alterada), Audit Trail (Es el orden cronológico de los hechos que se reconstruye para examinar la secuencia actividades que rodean una actividad o evento) |
| **Tipo de amenaza.** | Persistencia al desconocer el origen de los hechos y no saber quien es el atacante |
| **Vector de ataque.** | Scripts para borrar o cifrar la evidencia, accesos privilegiados al sistema. |
| **Impacto técnico / operativo** | La integridad de registros baja, legal |
| **Medida de control recomendada.** | Controlar accesos, logs protegidos |

# 4 CONCLUSIÓN

Al término del análisis de los escenarios, se puede ver que hay muchos problemas y riesgos muy graves que pueden llegar a ocurrir por errores en el control de accesos y el como se manejan la protección de los logs o respaldos del sistema. Por un lado desafortunado hay muchas brechas o vectores por el que una amenaza podría entrar, pero también hay muchas maneras de mitigarlas y es por eso que se puede concluir que conocer estos marcos X.800 y el RFC 4949, no son conocimiento vano, sino que son conceptos y normas **claves** que encaminan hacia como cuidar y proteger los sistemas de redes contra los ataques que podrían tirar gran parte de una corporación, pues hoy en día hay muchas vulnerabilidades y todo por un desconocimiento o por un sentido de altivez, pero como se pudo ver en los escenarios, nadie está exento, ni siquiera se puede asegurar que la amenaza no podría entrar por algún proveedor de software de confianza o venir de un empleado interno (ya sea con la intención de hacer daño o por negligencia).

En fin, a pesar de que se puede mejorar el análisis hecho en este trabajo, es un motor para que uno como individuo se de cuenta que aun hay mucho por saber e informarse, pues esta actividad abrió el panorama sobre los riesgos que hay, pero también sobre las medidas que se pueden tomar como recomendación del X.800 y como clasificar las amenazas por el glosario RFC-4949 para así encontrar el origen y mitigar el daño, nuestra seguridad en la red depende de eso.

# 5 BIBLIOGRAFÍA


Russell L. (Russ) Shirey, d. U. (2007). *RFC 4949: Internet Security Glossary,.* Obtenido de https://datatracker.ietf.org/doc/html/rfc4949

UIT. (2026). *Connecting the world and beyond*. Obtenido de https://www.itu.int/en/Pages/default.aspx