Actividad 2

Estefano Alessandro Rodríguez Morin
178584
CNO V: Seguridad Informática
27/01/2026

La seguridad informática moderna se fundamenta en marcos normativos que estandarizan la protección de la información. El modelo ITU-T X.800, conocido como la Arquitectura de Seguridad para el modelo OSI, define de manera sistemática los servicios de seguridad (como autenticación, confidencialidad e integridad) y los mecanismos necesarios para mitigar amenazas en las comunicaciones. Por su parte, el RFC 4949 funciona como un glosario fundamental que establece una terminología técnica precisa y consensuada. Juntos, estos marcos permiten que los profesionales de la ciberseguridad no solo implementen controles robustos, sino que también documenten y comuniquen incidentes de manera estandarizada y profesional.

En el contexto actual, donde los ciberataques han evolucionado hacia modelos complejos como el ransomware y las amenazas persistentes avanzadas (APT), la relación entre estos estándares es vital. Mientras que el X.800 proporciona la estructura conceptual para identificar qué pilar de la seguridad ha sido vulnerado, el RFC 4949 aporta el lenguaje técnico para describir con exactitud la naturaleza de la vulnerabilidad y el impacto del ataque. El análisis de escenarios prácticos mediante estos dos pilares garantiza una comprensión profunda de los incidentes, facilitando el diseño de estrategias de defensa más efectivas y alineadas con las mejores prácticas internacionales.

Escenario 1: Análisis de Incidente LockBit

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.

Elemento	Respuesta
Servicios X.800 comprometidos.	Control de acceso, Confidencialidad de Datos, Disponibilidad, Integridad
Definición(es) aplicable(s) RFC 4949.	**Multi-stage attack**:Serie de acciones que progresan desde el compromiso inicial hasta el objetivo final. **Data breach**: Entrada no autorizada que resulta en pérdida o filtración de datos. Availability attack: Impide el acceso legítimo a servicios o recursos del sistema
Tipo de amenaza.	Externa (Con inyección de ransomware)
Vector de ataque.	Accesos no autorizados, Extrafiltración de datos y Disperción de Ransomware
Impacto técnico / operativo.	Perdida de control del sistema,Divulgación de información confidencial y daño a la reputación
Medida de control recomendada.	Implementación de Backups offline, cifrado de datos en reposo

Escenario 2: Análisis de Exposición de Datos en la Nube

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.

Elemento	Respuesta
Servicios X.800 comprometidos.	Control de acceso, Integridad de Datos, Confidencialidad de Datos
Definición(es) aplicable(s) RFC 4949.	**Misconfiguration**:Error de configuración que crea una vulnerabilidad. **Exposure**: Datos de un sistema que son accesibles a entidades no autorizadas por falta de seguridad
Tipo de amenaza.	Interna (falla en la configuración de credenciales y acceso)
Vector de ataque.	Filtrado de información
Impacto técnico / operativo.	Imposibilidad de mantener un control de acceso hacia la base de datos
Medida de control recomendada.	Implementar herramientas de monitoreo (CSPM) para detectar configuraciones abiertas y aplicar el principio de **Privilegio Mínimo**.

Escenario 3: Análisis de Compromiso de Cadena de Suministro

Un proveedor legítimo de software fue comprometido y distribuyó una actualización que incluía código malicioso, afectando a cientos de organizaciones que confiaban en él.

Elemento	Respuesta
Servicios X.800 comprometidos.	Integridad de Datos, Confidencialidad, Control de acceso
Definición(es) aplicable(s) RFC 4949.	**Supply chain attack**: Ataque que consiste en manipulación de productos antes de llegar al usuario final.
Tipo de amenaza.	Externo (Ejecución de código malicioso)
Vector de ataque.	Inyección de código malicioso
Impacto técnico / operativo.	Ejecución de código malicioso y pérdida de confianza en la infraestructura de actualización del software.
Medida de control recomendada.	Seguir métodos de verificación para actualizaciones y/o instalaciones de fuentes externas

Escenario 4: Robo de Credenciales mediante Phishing

Mediante campañas de phishing, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. El servicio de autenticación fue comprometido al basarse en credenciales robadas.

Elemento	Respuesta
Servicios X.800 comprometidos.	Control de acceso, Autenticación, Confidencialidad de Datos
Definición(es) aplicable(s) RFC 4949.	**Credential compromise**: Datos de autenticación legítimos son conocidos por terceros no autorizados **Authentication failure**: Incapacidad del proceso de seguridad para asegurar que la persona que intenta acceder es quien dice ser
Tipo de amenaza.	Externa (Ingeniería Social)
Vector de ataque.	Robo de credenciales por medio de phishing
Impacto técnico / operativo.	Suplantación de identidad, Acceso persistente de terceros como usuarios legítimos
Medida de control recomendada.	Implementación de tokens físicos o aplicaciones de autenticación (MFA)

Escenario 5: Destrucción de Respaldos en Ataques de Ransomware

En ataques de ransomware avanzados, los atacantes eliminaron o cifraron los respaldos antes de afectar los sistemas productivos, impidiendo la recuperación.

Elemento	Respuesta
Servicios X.800 comprometidos.	Integridad de Datos, Disponibilidad
Definición(es) aplicable(s) RFC 4949.	**Data destruction**: Acción de borrar o alterar datos de manera que resulten irrecuperables **Availability attack**: Acto que impide a usuarios autorizados un acceso al sistema
Tipo de amenaza.	Externa (Por medio de inyección de ransomware)
Vector de ataque.	Encriptación y/o bloqueo de información
Impacto técnico / operativo.	Pérdida total de información, riesgo en la disponibilidad de la información y sistemas
Medida de control recomendada.	Respaldos Inmutables, Mantener copias de seguridad fuera de línea o en medios que no permitan la edición ni el borrado.

Escenario 6: Amenaza Interna y Abuso de Privilegios

Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas, aprovechando su exceso de privilegios.

Elemento	Respuesta
Servicios X.800 comprometidos.	Control de acceso, Confidencialidad
Definición(es) aplicable(s) RFC 4949.	**Insider threat**: Entidad con acceso autorizado que actúa de forma maliciosa.
Tipo de amenaza.	Interna
Vector de ataque.	Abuso de privilegios
Impacto técnico / operativo.	Filtrado de información sensible sobre la empresa
Medida de control recomendada.	Restringir accesos a lo estrictamente necesario y aplicar DLP (Data Loss Prevention) para monitorear exfiltración.

Escenario 7: Alteración de Registros y Pérdida de Trazabilidad

Tras un ataque, los registros del sistema quedaron cifrados o alterados, impidiendo reconstruir la secuencia de eventos.

Elemento	Respuesta
Servicios X.800 comprometidos.	Integridad de Datos, No repudio, Disponibilidad
Definición(es) aplicable(s) RFC 4949.	**Evidentiary integrity**: Atributo de los datos que garantiza que no han sido alterados **Audit trail**: Registro cronológico de un sistema que permite reconstrucción y examinación de una secuencia de eventos
Tipo de amenaza.	Externa
Vector de ataque.	Cifrado de datos y registros del sistema
Impacto técnico / operativo.	Nulidad de la evidencia para investigaciones internas
Medida de control recomendada.	Enviar registros en tiempo real a un servidor externo con almacenamiento inmutable que impida su modificación posterior.

Escenario 8: Falla Operativa Global por Actualización

Una actualización mal ejecutada provocó la caída simultánea de múltiples servicios críticos a nivel global. Aunque no existió un atacante, la disponibilidad fue gravemente afectada.

Elemento	Respuesta
Servicios X.800 comprometidos.	Disponibilidad
Definición(es) aplicable(s) RFC 4949.	**Operational failure**: Error o evento no deseado que resulta en pérdida de la capacidad del sistema para realizar su función
Tipo de amenaza.	Interna
Vector de ataque.	No aplica (Error técnico)
Impacto técnico / operativo.	Caída simultánea de servidores globales
Medida de control recomendada.	Implementar actualizaciones por fases

Escenario 9: Suplantación de Sitios Oficiales

Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible, suplantando identidades legítimas.

Elemento	Respuesta
Servicios X.800 comprometidos.	Autenticación, Confidencialidad de Datos
Definición(es) aplicable(s) RFC 4949.	**Masquerade**: Ataque en el que entidad no autorizada finge ser una autorizada **Phishing**: Técnica de ingeniería social que utiliza comunicaciones engañosas
Tipo de amenaza.	Externa (suplantación de identidad)
Vector de ataque.	Ingenieria social / Web Spoofing
Impacto técnico / operativo.	Robo de identidad a gran escala y perdida de confianza ciudadana en canales oficiales
Medida de control recomendada.	Implementar firmas digitales en correos y fomentar el uso de certificados de validación extendida para asegurar la identidad del dominio.

Escenario 10: Ataque Destructivo y Exfiltración

Tras exfiltrar información, los atacantes ejecutaron acciones destructivas para borrar sistemas completos y eliminar rastros, configurando un compromiso total de la tríada de seguridad.

Elemento	Respuesta
Servicios X.800 comprometidos.	Confidencialidad de Datos, Disponibilidad, Integridad de Datos
Definición(es) aplicable(s) RFC 4949.	**Destructive attack**: Ataque diseñado para causar daños permanentes o catastróficos a los activos del sistema
Tipo de amenaza.	Externa (Acceso a datos y sistemas)
Vector de ataque.	Filtrado y seguridad de la información
Impacto técnico / operativo.	Perdida total de datos y sistemas
Medida de control recomendada.	Implementar bóvedas de datos aisladas y segmentación estricta de redes para contener la propagación.

Conclusiones

La aplicación de los marcos X.800 y RFC 4949 demuestra que la ciberseguridad en Latinoamérica debe dejar de ser reactiva. En nuestra región, donde el error humano y la falta de presupuestos robustos son comunes, estandarizar el lenguaje y los servicios de seguridad es el primer paso para construir defensas reales. No basta con instalar antivirus; es crítico implementar controles como el privilegio mínimo y la inmutabilidad de datos para proteger infraestructuras que, aunque modernas, suelen ser frágiles ante ataques dirigidos. Adoptar estos estándares internacionales permite que nuestras organizaciones hablen el mismo idioma técnico que el resto del mundo, facilitando la respuesta ante crisis y fortaleciendo la confianza digital en el entorno local.

Referencias bibliográficas

- **IETF (2007).** *Internet Security Glossary, Version 2 (RFC 4949)*. RFC Editor. Recuperado de: https://datatracker.ietf.org/doc/html/rfc4949
- **ITU-T (1991).** *Recommendation X.800: Security architecture for Open Systems Interconnection for CCITT applications*. International Telecommunication Union. Recuperado de: https://www.itu.int/rec/T-REC-X.800-199103-I/en