UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CNO V Seguridad Informática

27/01/2026

ACTIVIDAD 2

ANÁLISIS DE SERVICIOS DE SEGURIDAD

Elaborado por:
Elisa Alejandra Arellano Wratny

Contenido

Tabla de ilustraciones 2
Introducción 4
Desarrollo 5
Conclusiones 18
Referencias 19

Tabla de ilustraciones

Tabla 1.- Escenario 01 _____ 6
Tabla 2.- Escenario 02 _____ 7
Tabla 3.- Escenario 03 _____ 9
Tabla 4.- Escenario 04 _____ 10
Tabla 5.- Escenario 05 _____ 12
Tabla 6.- Escenario 06 _____ 13
Tabla 7.- Escenario 07 _____ 14
Tabla 8.- Escenario 08 _____ 15
Tabla 9.- Escenario 09 _____ 16
Tabla 10.- Escenario 10 _____ 17

Introducción

En la actualidad, la seguridad informática enfrenta escenarios de amenaza cada vez más complejos, donde los incidentes no solo afectan activos digitales, sino también servicios esenciales, procesos organizacionales y la confianza en los sistemas de información. Ante este panorama, el análisis de incidentes de seguridad requiere el uso de marcos conceptuales y terminológicos estandarizados que permitan describir, evaluar y comunicar las vulneraciones de manera clara, precisa y profesional.

El estándar ITU-T X.800 establece un modelo conceptual basado en seis servicios fundamentales de seguridad (autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad) cuyo propósito es identificar qué propiedades de seguridad deben protegerse dentro de un sistema de información. Este marco permite evaluar de forma estructurada qué servicios fueron comprometidos durante un incidente y comprender el impacto de dichas fallas sobre la operación del sistema.

Por su parte, el RFC 4949 proporciona un marco terminológico estandarizado para la seguridad de la información, definiendo con precisión conceptos como amenaza, vulnerabilidad, ataque, impacto y riesgo. Su propósito principal es unificar el lenguaje técnico, evitando ambigüedades y permitiendo una comunicación clara y consistente entre profesionales, analistas y responsables de la toma de decisiones en materia de ciberseguridad.

La relación entre ambos marcos es complementaria: mientras el ITU-T X.800 permite identificar qué servicios de seguridad han sido afectados, el RFC 4949 facilita describir cómo y por qué ocurrió la vulneración, utilizando un vocabulario técnico común. Esta combinación resulta especialmente relevante en la seguridad informática actual, donde la correcta documentación y análisis de incidentes es clave para la respuesta, la prevención y la mejora continua de los controles de seguridad.

En este sentido, la presente actividad tiene como objetivo analizar escenarios reales de incidentes de seguridad informática mediante la aplicación conjunta del ITU-T X.800 y el RFC 4949, fortaleciendo la capacidad del estudiante para identificar, explicar y documentar vulneraciones de seguridad de manera rigurosa, estandarizada y alineada con las prácticas profesionales vigentes.

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**
Servicios X.800 comprometidos.	**Confidencialidad**: comprometida debido a la exfiltración de información sensible antes del cifrado. **Integridad**: comprometida por la modificación no autorizada de datos y sistemas durante el despliegue del ransomware. **Disponibilidad**: comprometida por el cifrado masivo de servidores que impide el acceso a los sistemas y servicios afectados.
Definición(es) aplicable(s) RFC 4949.	**Ransomware:** tipo de malware que niega el acceso a un sistema o datos hasta que se paga un rescate. **Multi-stage attack**: ataque compuesto por múltiples fases secuenciales, donde cada etapa prepara o amplifica el impacto de la siguiente. **Data breach:** incidente de seguridad que resulta en la divulgación o acceso no autorizado a información sensible. **Availability attack:** ataque diseñado para degradar o eliminar el acceso legítimo a sistemas. **Exfiltration:** transferencia no autorizada de datos desde un sistema comprometido hacia un entorno controlado por el atacante.
Tipo de amenaza.	**Externa,** organizada y persistente, asociada a un grupo criminal especializado en Ransomware-as-a-Service (RaaS).
Vector de ataque.	Acceso inicial no autorizado. Movimiento lateral y escalamiento de privilegios dentro del entorno. Exfiltración de datos sensibles como mecanismo de presión. Despliegue final de ransomware LockBit para el cifrado masivo de servidores.

Impacto técnico / operativo.	Pérdida total de disponibilidad de sistemas críticos y servidores. Exposición de información sensible, con riesgo de sanciones legales, daño reputacional y extorsión adicional. Interrupción prolongada de operaciones, al no contar con respaldos inmutables para recuperación rápida. Incremento del impacto económico, al combinar indisponibilidad operativa con amenazas de publicación de datos.
Medida de control recomendada.	Implementación de respaldos inmutables (immutable backups) con pruebas periódicas de restauración. Monitoreo y detección temprana de comportamientos anómalos (detección de exfiltración). Segmentación de red y principio de mínimo privilegio para limitar el movimiento lateral. Gestión continua de vulnerabilidades y parches en servicios expuestos. Planes de respuesta a incidentes específicos para ransomware y doble extorsión.

Tabla 1.- Escenario 01

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.	**Confidencialidad**: comprometida debido a la exposición pública de bases de datos sin controles adecuados de acceso. **Control de acceso**: comprometido por la incorrecta definición o ausencia de políticas de autorización sobre los recursos almacenados.
Definición(es) aplicable(s) RFC 4949.	**Misconfiguration**: configuración incorrecta o incompleta de un sistema que introduce una vulnerabilidad de seguridad. **Exposure**: condición en la cual información o recursos quedan accesibles a entidades no autorizadas.

	Access control: mecanismo que limita el acceso a recursos del sistema a entidades autorizadas. **Confidentiality**: propiedad de seguridad que asegura que la información no sea divulgada a sujetos no autorizados.
Tipo de amenaza.	**Externa** pasiva, derivada de una exposición no intencional.
Vector de ataque.	Configuración incorrecta de servicios en la nube. Acceso directo a los datos mediante URL pública o endpoint expuesto, sin necesidad de autenticación ni explotación técnica.
Impacto técnico / operativo.	Pérdida de confidencialidad de datos sensibles o personales. Impacto legal y regulatorio, incluyendo posibles sanciones por incumplimiento de normativas de protección de datos, aun sin evidencia de acceso malicioso comprobado. Daño reputacional significativo para la organización afectada. Dificultad de atribución, ya que no siempre es posible demostrar si terceros accedieron efectivamente a la información expuesta.
Medida de control recomendada.	Revisión y hardening de configuraciones en la nube, aplicando el principio de deny by default. Auditorías periódicas de control de acceso y permisos sobre recursos expuestos. Implementación de herramientas de Cloud Security Posture Management (CSPM) para detección automática de misconfigurations. Clasificación de la información y aplicación de controles acordes a su nivel de sensibilidad. Capacitación técnica del personal en buenas prácticas de configuración segura en entornos cloud.

Tabla 2.- Escenario 02

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.	**Integridad**: comprometida al distribuirse una actualización de software legítima que incluía código malicioso no autorizado, alterando el estado esperado del sistema. **Confidencialidad**: comprometida de forma subsecuente al permitir accesos no autorizados, espionaje o exfiltración de información tras la ejecución del código malicioso. **Control de acceso**: comprometido indirectamente, al ejecutarse el software malicioso con los privilegios confiados al proveedor legítimo.
Definición(es) aplicable(s) RFC 4949.	**Supply chain attack**: ataque que compromete un componente o proveedor confiable con el fin de afectar a múltiples objetivos aguas abajo. **Integrity violation**: modificación no autorizada de software o datos. **Trusted relationship**: relación de confianza establecida entre sistemas o entidades que reduce o elimina verificaciones adicionales. **Malicious code**: software diseñado para ejecutar acciones no autorizadas dentro de un sistema. **Unauthorized access**: acceso a recursos del sistema sin autorización explícita.
Tipo de amenaza.	**Externa,** altamente sofisticada y dirigida, con capacidad para comprometer infraestructura de desarrollo o distribución de un proveedor legítimo.
Vector de ataque.	Compromiso del entorno de desarrollo o de la cadena de distribución del proveedor. Inserción de código malicioso en una actualización legítima. Distribución firmada y confiable del software comprometido a clientes finales. Ejecución automática del código malicioso en entornos productivos debido a la confianza previa en el proveedor.
Impacto técnico / operativo.	Violación masiva de la integridad de sistemas en múltiples organizaciones. Compromiso de la confidencialidad mediante accesos persistentes, espionaje o exfiltración de información.

	Dificultad extrema de detección temprana, al tratarse de software legítimo y firmado. Impacto operativo prolongado, al requerir análisis forense profundo y reconstrucción de entornos confiables. Pérdida de confianza en el proveedor, con consecuencias legales, contractuales y reputacionales tanto para el proveedor como para los clientes afectados.
Medida de control recomendada.	Validación reforzada de actualizaciones. Modelo Zero Trust aplicado a software y proveedores, reduciendo la confianza implícita. Segmentación y aislamiento de sistemas críticos frente a software de terceros. Monitoreo continuo post-actualización para detectar comportamientos anómalos. Evaluaciones de seguridad y auditorías periódicas a proveedores. Planes de respuesta específicos para ataques a la cadena de suministro.

Tabla 3.- Escenario 03

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**: comprometida a nivel conceptual, ya que el mecanismo validó credenciales robadas, identificando erróneamente al atacante como un usuario legítimo. **Control de acceso**: comprometido como consecuencia directa, al concederse privilegios y accesos basados en una identidad falsamente autenticada. **Confidencialidad**: potencialmente comprometida debido al acceso prolongado no autorizado a información sensible. **Integridad**: potencialmente comprometida por la capacidad del atacante de modificar datos o configuraciones durante su permanencia.
Definición(es) aplicable(s) RFC 4949.	**Phishing**: técnica de ingeniería social utilizada para obtener credenciales u otra información sensible mediante engaño.

	Credential compromise: situación en la que credenciales legítimas son obtenidas por un atacante no autorizado. **Authentication failure**: falla en la autenticación donde el sistema valida una identidad incorrecta debido al uso de credenciales comprometidas, sin existir un fallo técnico del mecanismo. **Unauthorized access**: acceso a recursos del sistema por una entidad no autorizada, aunque se utilicen credenciales válidas. **Persistent access**: mantenimiento de acceso continuo a un sistema comprometido durante un periodo prolongado.
Tipo de amenaza.	**Externa,** basada en ingeniería social, con capacidad de mantener acceso prolongado sin ser detectada.
Vector de ataque.	Campañas de phishing dirigidas a usuarios corporativos. Robo de credenciales válidas mediante engaño. Acceso remoto a sistemas corporativos usando credenciales legítimas. Persistencia prolongada facilitada por la ausencia de controles adicionales de verificación y monitoreo.
Impacto técnico / operativo.	Acceso no autorizado persistente durante meses sin generación de alertas. Exposición prolongada de información sensible, con riesgo acumulativo creciente. Dificultad de detección, al tratarse de accesos que aparentan ser legítimos. Compromiso de la confianza en los mecanismos de autenticación, afectando la postura de seguridad general de la organización.
Medida de control recomendada.	Implementación obligatoria de autenticación multifactor (MFA) en todos los accesos críticos. Monitoreo de comportamiento y detección de anomalías (UEBA). Capacitación continua en concienciación de phishing para usuarios. Limitación de privilegios y revisión periódica de accesos. Alertas por patrones atípicos (horarios, ubicaciones, volúmenes de acceso).

Tabla 4.- Escenario 04

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**: comprometida de forma crítica al eliminarse o cifrarse los respaldos, impidiendo la restauración de los sistemas afectados. **Integridad**: comprometida debido a la destrucción y alteración deliberada de la información de respaldo. **Confidencialidad**: puede verse afectada si el atacante accede o exfiltra información durante la fase previa al cifrado, aunque no sea el objetivo principal del escenario.
Definición(es) aplicable(s) RFC 4949.	**Data destruction**: eliminación o corrupción intencional de datos con el objetivo de impedir su uso o recuperación. **Availability attack**: ataque diseñado para negar o degradar el acceso a sistemas, servicios o información. **Ransomware**: tipo de malware que cifra datos o sistemas para extorsionar a la organización afectada. **Intentional damage:** daño causado de manera deliberada como parte de una estrategia de ataque planificada.
Tipo de amenaza.	**Externa,** altamente intencional y dirigida.
Vector de ataque.	Acceso previo al entorno de respaldo. Eliminación o cifrado de respaldos antes del despliegue del ransomware en sistemas productivos. Uso de privilegios elevados para garantizar el daño irreversible.
Impacto técnico / operativo.	Imposibilidad de recuperación de sistemas y datos, incluso tras la contención del ransomware. Interrupción total de operaciones críticas, con tiempos de inactividad prolongados o indefinidos. Incremento drástico del impacto financiero, al forzar decisiones extremas como el pago del rescate. Daño reputacional y legal, especialmente en organizaciones con obligaciones regulatorias de continuidad y protección de la información.

Medida de control recomendada.	Implementación de respaldos inmutables (immutable backups) y offline (air-gapped). Separación de credenciales y privilegios entre sistemas productivos y de respaldo. Monitoreo y alertas sobre operaciones de borrado o cifrado de respaldos. Pruebas periódicas de restauración para validar la efectividad de los respaldos. Principio de mínimo privilegio aplicado a la infraestructura de backup.

Tabla 5.- Escenario 05

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**: comprometida de forma directa al extraerse y divulgarse información sensible a terceros no autorizados. **Control de acceso**: comprometido debido a la asignación excesiva de privilegios que permitió el acceso completo a bases de datos sin necesidad operacional. **No repudio**: debilitado si no existen registros, trazabilidad o mecanismos de auditoría que permitan atribuir la acción al responsable.
Definición(es) aplicable(s) RFC 4949.	**Insider threat:** amenaza originada por un usuario autorizado que abusa de sus privilegios para causar daño a la organización. **Data exfiltration**: extracción no autorizada de información desde un sistema. **Least privilege violation:** asignación de permisos superiores a los estrictamente necesarios para cumplir una función. **Unauthorized disclosure:** revelación de información a entidades no autorizadas.
Tipo de amenaza.	**Interna,** intencional y maliciosa.
Vector de ataque.	Uso indebido de credenciales legítimas. Acceso directo a bases de datos gracias a privilegios excesivos. Extracción masiva de información (dumping/exportación) sin mecanismos de detección.
Impacto técnico / operativo.	Pérdida total de confidencialidad de los datos comprometidos.

	Impacto legal y regulatorio (protección de datos, privacidad, cumplimiento normativo). Daño reputacional severo, especialmente si los datos se comercializan o publican. Pérdida de confianza interna y externa, afectando relaciones comerciales y contractuales.
Medida de control recomendada.	Aplicación estricta del principio de mínimo privilegio (PoLP). Segregación de funciones (SoD) en el acceso a bases de datos sensibles. Monitoreo continuo de actividades privilegiadas (UEBA). Auditorías periódicas de accesos y permisos. Políticas claras de manejo de información y concientización interna.

Tabla 6.- Escenario 06

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**: comprometida debido a la alteración o cifrado de los registros del sistema, afectando la veracidad y confiabilidad de la información. **No repudio**: comprometido al perderse la capacidad de demostrar acciones, eventos y responsabilidades de manera verificable. **Confidencialidad**: potencialmente afectada si los registros fueron accedidos o exfiltrados durante el ataque.
Definición(es) aplicable(s) RFC 4949.	**Evidentiary integrity**: propiedad que garantiza que la evidencia digital no ha sido alterada y es admisible para análisis forense o procesos legales. **Audit trail**: conjunto de registros que documentan actividades y eventos relevantes dentro de un sistema. **Log tampering**: modificación o destrucción intencional de registros para ocultar acciones maliciosas. **Accountability failure:** incapacidad de asociar acciones a entidades responsables.
Tipo de amenaza.	**Externa,** generalmente post-explotación.
Vector de ataque.	Acceso privilegiado al sistema de registros.

	Cifrado, borrado o manipulación de logs tras el compromiso inicial. Desactivación o evasión de mecanismos de auditoría.
Impacto técnico / operativo.	Imposibilidad de reconstruir la línea temporal del ataque. Dificultad o imposibilidad de atribución del incidente. Invalidación de procesos forenses y de respuesta a incidentes. Impacto legal y probatorio, al no contar con evidencia confiable ante auditorías, litigios o autoridades regulatorias.
Medida de control recomendada.	Centralización de logs en sistemas inmutables. Separación de privilegios entre administradores de sistemas y de auditoría. Firmado digital y sellado temporal (timestamping) de registros críticos. Monitoreo de integridad de logs y alertas ante modificaciones. Planes de respuesta a incidentes con preservación de evidencia.

Tabla 7.- Escenario 07

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**: comprometida de manera crítica debido a la interrupción simultánea de múltiples servicios esenciales. **Integridad**: potencialmente afectada si la actualización alteró estados de configuración o datos operativos. **No repudio**: debilitado si no existen registros claros del proceso de actualización y de los responsables.
Definición(es) aplicable(s) RFC 4949.	**Operational failure**: interrupción causada por errores internos de operación, mantenimiento o configuración. **Availability failure**: incapacidad de un sistema para prestar el servicio esperado. **Change management failure**: falla en los procesos de control y validación de cambios. **Single point of failure**: elemento cuya falla provoca un impacto sistémico.
Tipo de amenaza.	**Interna,** no maliciosa.

Vector de ataque.	Despliegue de actualización sin pruebas suficientes. Ausencia de entornos de staging o pruebas controladas. Falta de mecanismos de reversión (rollback) tras detectar el fallo.
Impacto técnico / operativo.	Interrupción global de servicios críticos. Pérdidas económicas significativas por tiempo de inactividad. Afectación a usuarios finales y clientes, con impacto reputacional. Exposición a riesgos legales y contractuales.
Medida de control recomendada.	Procesos formales de gestión de cambios. Pruebas exhaustivas en entornos de preproducción. Planes de reversión automatizados (rollback). Despliegues progresivos. Planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP).

Tabla 8.- Escenario 08

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:** comprometida al suplantarse identidades legítimas, induciendo a los usuarios a confiar en entidades falsas. **Confidencialidad**: comprometida debido a la recolección de información sensible de los usuarios engañados. **Control de acceso**: afectado si las credenciales obtenidas permiten accesos posteriores no autorizados a sistemas legítimos.
Definición(es) aplicable(s) RFC 4949.	**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. **Social engineering**: manipulación psicológica de usuarios para inducirlos a violar políticas de seguridad. **Credential harvesting**: recolección fraudulenta de credenciales.
Tipo de amenaza.	**Externa,** intencional y dirigida.

Vector de ataque.	Clonación de sitios web oficiales. Envío de correos electrónicos falsificados (spoofing). Redirección a portales fraudulentos para captura de información.
Impacto técnico / operativo.	Compromiso de información personal o credenciales de ciudadanos o usuarios. Accesos no autorizados posteriores a sistemas legítimos. Daño reputacional a la entidad suplantada. Impacto legal y regulatorio, especialmente en entornos gubernamentales o de datos personales.
Medida de control recomendada.	Implementación de mecanismos de autenticación de dominio (SPF, DKIM, DMARC). Certificados digitales y uso estricto de HTTPS. Concientización y capacitación continua de usuarios. Filtros avanzados anti-phishing y detección de dominios similares. Políticas claras de comunicación institucional.

Tabla 9.- Escenario 09

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:** comprometida completamente debido a la exfiltración previa de información sensible. **Integridad**: comprometida de forma grave al destruirse sistemas y datos, imposibilitando su validación o recuperación. **Disponibilidad**: comprometida de manera total por la eliminación de sistemas y servicios. **No repudio:** afectado si la destrucción de evidencias impide la atribución del ataque.
Definición(es) aplicable(s) RFC 4949.	**Destructive attack:** ataque cuyo objetivo principal es causar daño irreversible a sistemas o información. **Data exfiltration**: extracción no autorizada de información previa a la fase destructiva.

	Data destruction: eliminación intencional de datos y sistemas. **Advanced persistent threat (APT):** patrón compatible con ataques altamente dirigidos y planificados.
Tipo de amenaza.	**Externa,** altamente intencional y destructiva.
Vector de ataque.	Acceso no autorizado prolongado con preparación previa. Exfiltración de información sensible. Ejecución de acciones destructivas (wipers, borrado masivo, sabotaje de infraestructura). Eliminación de rastros y evidencias.
Impacto técnico / operativo.	Pérdida total e irreversible de información. Colapso completo de operaciones críticas. Imposibilidad de análisis forense adecuado. Impacto económico, legal y reputacional extremo. Riesgo para la continuidad institucional o nacional, según el sector afectado.
Medida de control recomendada.	Detección temprana y respuesta automatizada. Segmentación de red estricta para limitar movimientos laterales. Respaldos inmutables y offline, probados periódicamente. Monitoreo continuo y correlación de eventos. Planes de respuesta a incidentes y recuperación ante desastres. Simulacros de ataque destructivo.

Tabla 10.- Escenario 10

Conclusiones

El análisis de los escenarios presentados revela que los problemas de seguridad informática no siguen un solo patrón técnico, sino que se deben a una compleja mezcla de fallos tecnológicos, errores humanos y debilidades organizacionales. La implementación del modelo de servicios de seguridad del ITU-T X. 800 facilitó la identificación estructurada de cómo los principios de autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad pueden estar en riesgo, tanto por ataques intencionados como por errores internos.

Adicionalmente, la utilización del RFC 4949 ofreció un marco terminológico claro y estandarizado para la clasificación de amenazas, vulnerabilidades y tipos de ataque, lo que permitió una comunicación técnica efectiva y profesional. Esta relación demuestra que X. 800 indica qué elementos son protegidos, mientras que RFC 4949 detalla cómo y por qué se comprometen, haciendo su uso conjunto esencial en el análisis contemporáneo de incidentes.

Un descubrimiento significativo es que muchos de los efectos más graves no provienen de ataques complejos, sino de fallas fundamentales en la gobernanza, tales como la falta de autenticación multifactor, derechos excesivos, ausencia de monitoreo, falta de copias de seguridad inmutables o ineficiencias en la gestión de cambios. Además, varios ejemplos indican que la detección tardía convierte incidentes controlables en crisis, especialmente cuando se ven afectadas la confidencialidad, integridad y disponibilidad al mismo tiempo.

Desde un enfoque latinoamericano, estos escenarios son especialmente relevantes. Muchas organizaciones en la región enfrentan limitaciones en sus presupuestos, dependencia de proveedores externos, niveles de madurez en ciberseguridad desiguales y una cultura reactiva, lo que aumenta el riesgo ante amenazas internas, ataques de ingeniería social y fallos operativos. No obstante, el análisis también revela que muchas de las medidas de control sugeridas, como políticas de mínimos privilegios, capacitación, segmentación de redes, copias de seguridad offline y gestión formal de cambios, son factibles y aplicables incluso en entornos con recursos escasos.

En resumen, mejorar la seguridad informática en situaciones reales requiere no solo tecnología, sino también procesos claros, formación continua y marcos conceptuales robustos. La combinación de ITU-T X. 800 y RFC 4949 permite realizar análisis técnicos rigurosos, optimizar la documentación de incidentes y respaldar decisiones estratégicas, contribuyendo a una postura de seguridad más robusta y acorde con las necesidades actuales de las organizaciones, particularmente en América Latina.

Referencias

- *Internet Engineering Task Force (IETF). (2007). RFC 4949: Internet Security Glossary, Version 2. https://datatracker.ietf.org/doc/html/rfc4949*
- *International Telecommunication Union – Telecommunication Standardization Sector (ITU-T). (1991). Recommendation X.800: Security Architecture for Open Systems Interconnection. https://www.itu.int/rec/T-REC-X.800-199103-I/es*