UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Análisis de servicios de seguridad

Alan Gilberto Sánchez Zavala

177263

Universidad Politécnica de
San Luis Potosi

Ciberseguridad

Contents

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.	Autenticación, Control de Acceso, Confidencialidad de Datos, Integridad de Datos, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	**Data Breach:** Una violación de seguridad en la que se accede a datos sensibles sin autorización, lo que resulta en su visualización, copia o exfiltración por parte de una entidad no autorizada. **Attack:** Un asalto a la seguridad del sistema que se deriva de una amenaza inteligente; es decir, un acto inteligente que es un intento deliberado de evadir los servicios de seguridad y violar la política de seguridad de un sistema. **Availability:** La propiedad de un sistema o un recurso del sistema que garantiza que es accesible y utilizable a solicitud por una entidad autorizada del sistema. **Data Integrity:** La propiedad de que los datos no han sido alterados o destruidos de manera no autorizada. **Exfiltration:** El traslado o transferencia no autorizada de información desde un sistema de información
Tipo de amenaza.	Externo (Grupo criminal LockBit).
Vector de ataque.	Acceso inicial no autorizado (explotación de vulnerabilidades o compromiso de credenciales), seguido de un ataque en múltiples etapas (multi-stage attack) que incluye exfiltración de datos y ejecución de ransomware para cifrado masivo.
Impacto técnico / operativo.	Pérdida de confidencialidad (exfiltración), pérdida de integridad y disponibilidad (cifrado de servidores), e interrupción crítica de operaciones debido a la falta de respaldos inmutables.
Medida de control recomendada	Implementación de respaldos inmutables, sistemas de detección temprana (EDR/XDR), segmentación de red para limitar el movimiento lateral y una política estricta de MFA (autenticación multifactor) para prevenir el acceso inicial.

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, Confidencialidad de Datos.
Definición(es) aplicable(s) RFC 4949.	**Misconfiguration:** Un error en la configuración de un sistema o componente de seguridad que puede crear una vulnerabilidad y permitir que el sistema sea atacado o utilizado de manera no autorizada. **Exposure:** Una forma de amenaza en la cual los datos sensibles son liberados o accedidos por una entidad no autorizada de forma accidental o deliberada. **Vulnerability:** Una falla o debilidad en el diseño, implementación, operación o gestión de un sistema que podría ser explotada para violar la política de seguridad del sistema.
Tipo de amenaza.	Interno (Falla de configuración por parte de los administradores del sistema).
Vector de ataque.	Mala configuración de permisos en servicios de almacenamiento en la nube (cloud storage), dejando los repositorios con acceso de lectura para "todos" o "público".
Impacto técnico / operativo.	Pérdida de confidencialidad de datos sensibles, exposición pública de información privada, posibles sanciones legales (GDPR/locales) y daño severo a la reputación institucional.
Medida de control recomendada	Implementación de políticas de IAM (Identity and Access Management) bajo el principio de menor privilegio, auditorías automatizadas de configuración de nube, y el uso de herramientas de CSPM (Cloud Security Posture Management).

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, Control de Acceso, Confidencialidad de Datos, Integridad de Datos.

Definición(es) aplicable(s) RFC 4949.	**Supply Chain Attack:** Un ataque que desplaza el objetivo desde una organización directamente a un tercero en su cadena de suministro, como un proveedor de software o servicios, para obtener acceso o comprometer los sistemas del objetivo final. **Malicious Code:** Software (por ejemplo, un virus, un troyano o un gusano) que se introduce intencionadamente en un sistema para fines no autorizados. **Integrity:** La propiedad de que la información no ha sido alterada o destruida de forma no autorizada.
Tipo de amenaza.	Externo (Atacante compromete al proveedor tercero para llegar a la organización).
Vector de ataque.	Inyección de código malicioso en el ciclo de vida de desarrollo de software (SDLC) del proveedor y distribución mediante el mecanismo oficial de actualizaciones.
Impacto técnico / operativo.	Ejecución de código arbitrario con privilegios de sistema, compromiso masivo de la infraestructura, pérdida de control sobre la integridad del software instalado y ruptura de la cadena de confianza.
Medida de control recomendada	Implementación de Análisis de Composición de Software (SCA), verificación rigurosa de firmas digitales, monitoreo de comportamiento post-actualización (Sandboxing) y adopción de un modelo de Zero Trust.

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 de Datos.
Definición(es) aplicable(s) RFC 4949.	**Phishing:** Un proceso de engaño para intentar adquirir información sensible, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por una entidad de confianza en una comunicación electrónica. **Credential:** Datos que se presentan para establecer una identidad reclamada, como una contraseña o una clave criptográfica. **Authentication:** El proceso de verificar una identidad reclamada por o para un sistema o entidad. **Identity Theft:** El acto de adquirir deliberadamente la información de identidad de otra persona sin su consentimiento y utilizarla con fines fraudulentos

Tipo de amenaza.	Externo (Atacante utiliza ingeniería social para obtener acceso).
Vector de ataque.	Ingeniería social mediante campañas de phishing para el robo de credenciales, seguido de un acceso persistente mediante el uso de identidades legítimas comprometidas.
Impacto técnico / operativo.	Acceso no autorizado persistente y prolongado (dwell time), elusión de controles perimetrales, posible exfiltración silenciosa de datos y pérdida de confianza en el sistema de identidad.
Medida de control recomendada	Implementación de MFA (Autenticación Multifactor), monitoreo de Análisis del Comportamiento de Usuarios y Entidades (UEBA) para detectar accesos inusuales y capacitación en concienciación sobre seguridad (Security Awareness).

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.	Integridad de Datos, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	**Data Destruction:** Una forma de ataque a la disponibilidad que ocurre cuando los datos son borrados o hechos ilegibles, impidiendo que el sistema los utilice para sus propósitos originales. **Availability Attack:** Un ataque que impide a los usuarios autorizados el acceso a la información o a los recursos del sistema. **Integrity:** La propiedad de que la información no ha sido alterada o destruida de forma no autorizada.
Tipo de amenaza.	Externo
Vector de ataque.	Movimiento lateral y escalada de privilegios para alcanzar los sistemas de almacenamiento de respaldo, procediendo a su cifrado o eliminación total antes de atacar el entorno de producción.
Impacto técnico / operativo.	Incapacidad total de recuperación ante desastres (*disaster recovery*), pérdida permanente de datos críticos y paralización prolongada de las operaciones del negocio.
Medida de control recomendada	Implementación de respaldos offline (fuera de línea) o respaldos inmutables (WORM - Write Once, Read Many), además de la separación de privilegios para que los administradores de sistemas no puedan eliminar los respaldos.

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.	Control de Acceso, Confidencialidad de Datos.
Definición(es) aplicable(s) RFC 4949.	**Insider Threat:** Una entidad con acceso legítimo que tiene el potencial de dañar un sistema de información a través de la destrucción de recursos, la revelación de información, la modificación de datos o la denegación de servicio. **Risk:** Una expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad específica con una consecuencia dañina.
Tipo de amenaza.	Interno
Vector de ataque.	Abuso de privilegios legítimos para la extracción y exfiltración de bases de datos, aprovechando la falta de controles de supervisión sobre el comportamiento del usuario.
Impacto técnico / operativo.	Fuga masiva de información sensible, pérdida de propiedad intelectual, ventaja competitiva para terceros y posibles consecuencias legales por incumplimiento de custodia de datos.
Medida de control recomendada	Aplicación estricta del Principio de Mínimo Privilegio, implementación de herramientas de DLP (Data Loss Prevention) y sistemas de monitoreo de actividad de usuarios (User Activity Monitoring).

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 de Datos, No Repudio.
Definición(es) aplicable(s) RFC 4949.	**Integrity:** La propiedad de que los datos no han sido alterados o destruidos de forma no autorizada. **No-repudiation:** Un servicio de seguridad que proporciona prueba de la integridad y el origen de los datos, de manera que

	sea imposible negar de forma falsa que se ha producido una comunicación. **Audit Trail:** Un conjunto de registros que contiene evidencia de la secuencia de actividades que han afectado en cualquier momento a una operación, procedimiento o evento específico
Tipo de amenaza.	Externa
Vector de ataque.	Modificación o cifrado de archivos de log (registros del sistema) y bases de datos de auditoría para eliminar evidencia de la intrusión y dificultar el análisis forense.
Impacto técnico / operativo.	Pérdida de visibilidad sobre el incidente, incapacidad para realizar una reconstrucción forense, nulidad de pruebas para procesos legales y compromiso del cumplimiento normativo.
Medida de control recomendada	Implementación de centralización de logs en un servidor externo (SIEM) con permisos de solo escritura, uso de hashing para verificar la integridad de los registros y almacenamiento en medios de solo lectura (WORM).

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:** Una falla de seguridad que resulta de un error interno en la operación del sistema, en lugar de un ataque externo o malicioso. **Availability:** La propiedad de un sistema o de un recurso del sistema de ser accesible y utilizable a petición de una entidad del sistema autorizada.
Tipo de amenaza.	Interno (Error humano/técnico durante una actualización de mantenimiento).
Vector de ataque.	No aplica un vector de ataque malicioso; se trata de una falla en el proceso de gestión de cambios (*Change Management*) que resultó en la caída de servicios críticos.
Impacto técnico / operativo.	Indisponibilidad global de servicios, interrupción de procesos de negocio críticos, pérdida de ingresos y afectación a la continuidad operativa.
Medida de control recomendada	Implementación de protocolos estrictos de pruebas en entornos de pre-producción (staging), desarrollo de planes de reversión (rollback) inmediatos y despliegues escalonados (canary deployments).

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 de Datos.
Definición(es) aplicable(s) RFC 4949.	**Masquerade:** Un tipo de amenaza en la que una entidad no autorizada se hace pasar por una entidad autorizada para obtener acceso a un sistema o recurso. **Phishing:** Un proceso de engaño para intentar adquirir información sensible, como nombres de usuario o contraseñas, haciéndose pasar por una entidad de confianza. **Authentication:** El proceso de verificar una identidad reclamada por o para un sistema o entidad
Tipo de amenaza.	Externo (Atacantes que suplantan sitios oficiales).
Vector de ataque.	Ingeniería social mediante el uso de phishing (correos falsos) y creación de sitios web espejo (masquerade) para engañar a los usuarios y capturar sus datos.
Impacto técnico / operativo.	Robo masivo de credenciales e información sensible, compromiso de identidades de ciudadanos y pérdida de confianza en los canales digitales oficiales.
Medida de control recomendada	Implementación de protocolos de autenticación de correo como DMARC, SPF y DKIM, uso de certificados SSL/TLS con validación extendida y programas de concientización para usuarios.

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 de Datos, Integridad de Datos, Disponibilidad.
Definición(es) aplicable(s) RFC 4949.	**Destructive Attack:** Un ataque que daña los recursos del sistema de tal manera que no pueden ser utilizados o recuperados fácilmente.

	Confidentiality: La propiedad de que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. **Integrity:** La propiedad de que los datos no han sido alterados o destruidos de forma no autorizada. **Availability:** La propiedad de un sistema o de un recurso del sistema de ser accesible y utilizable a petición de una entidad del sistema autorizada.
Tipo de amenaza.	Externa
Vector de ataque.	Exfiltración de datos seguida de la ejecución de comandos o software destructivo (*wiper*) para eliminar archivos del sistema, registros y estructuras de datos, con el fin de borrar rastros y maximizar el daño.
Impacto técnico / operativo.	Destrucción total de la infraestructura digital, pérdida permanente de información, imposibilidad de realizar análisis forense y cese completo de la continuidad del negocio.
Medida de control recomendada	Implementación de sistemas de detección y respuesta (EDR/XDR) con capacidades de contención automática, segmentación de red para evitar el movimiento lateral y una estrategia de respaldos inmutables y aislados (Air-gap).

Conclusión

El análisis de estos diez escenarios, bajo la óptica de la Recomendación X.800 y el RFC 4949, muestra puntos importantes para la seguridad de la información

Los incidentes rara vez afectan a un solo servicio. Como vimos en los ataques de ransomware o de cadena de suministro (*supply chain*), la pérdida de Integridad suele llevar a la pérdida de Disponibilidad y Confidencialidad. La Amenaza no siempre es un "Hacker" externo, como se muestra en el RFC 4949 al clasificar tanto el Insider Threat (empleado malintencionado) como el Operational Failure (error de configuración o actualización) como riesgos de alto impacto. La seguridad debe cubrir tanto la defensa perimetral como la higiene operativa interna.

Debido a que el riesgo nunca es cero, la diferencia entre un incidente manejable y uno catastrófico es en la capacidad de recuperación. La falta de respaldos convierte una intrusión técnica en un daño irreversible. Para mitigar la mayoría de los vectores analizados, las organizaciones deben migrar hacia un modelo de Zero Trust, donde la confianza nunca se asume (ni siquiera para actualizaciones de proveedores legítimos) y siempre se verifica mediante MFA robusto, monitoreo continuo de comportamiento y una política estricta de mínimo privilegio.