UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Academia de Núcleo General

Activando el pensamiento, generamos conocimiento.

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: CNO V: Seguridad Informática

TRABAJO: Análisis de servicios de seguridad

PARCIAL 1

Donaldo Demián Gómez Arreguín 179822

Profesor: Servando López Contreras

Fecha de entrega: 27/01/2026

Introducción

En el contexto actual, donde las organizaciones dependen de manera crítica de los sistemas de información y de las redes de comunicación para operar, la seguridad informática se ha convertido en un componente estratégico y no únicamente técnico. Los incidentes de ciberseguridad ya no solo afectan a la infraestructura tecnológica, sino que generan impactos operativos, legales, económicos y reputacionales de gran magnitud.

La recomendación ITU-T X.800, emitida por la Unión Internacional de Telecomunicaciones, establece una arquitectura de referencia para la seguridad en sistemas interconectados, definiendo seis servicios fundamentales: autenticación, control de acceso, confidencialidad, integridad, no repudio y disponibilidad (ITU-T, 1991).

De forma complementaria, el RFC 4949, publicado por la Internet Engineering Task Force (IETF), funciona como el glosario oficial de la seguridad en Internet, proporcionando definiciones estandarizadas para amenazas, vulnerabilidades y ataques (Shirey, 2007).

Analisis

Se proporcionaron distintos casos en los que se presentaron diferentes escenarios de ataques cibernéticos. El análisis de estos casos permite identificar de manera más clara las principales áreas afectadas por cada incidente, además de fomentar la reflexión sobre las medidas que pueden mejorarse tanto a nivel individual como desde la perspectiva de quienes se interesan y se forman en el área de la ciberseguridad.

<table>
<tr><td>Escenario</td><td>Analisis de caso</td></tr>
<tr><td>Escenario 01</td><td>
<table>
<tr><th>Elemento</th><th>Respuesta</th></tr>
<tr><td>Servicios X.800 comprometidos.</td><td>Confidencialidad, integridad, disponibilidad</td></tr>
<tr><td>Definición(es) aplicable(s) RFC 4949.</td><td>Ransomware: Código malicioso que cifra o bloquea información para un rescate posterior.
Multi-stage attack: Ataque que se ejecuta en varias fases secuenciales para lograr un objetivo final.
Data breach: Exposición o divulgación no autorizada de información sensible.
Availability attack: Ataque cuyo objetivo es impedir el acceso legítimo a un recurso o servicio.</td></tr>
<tr><td>Tipo de amenazas</td><td>Externa</td></tr>
<tr><td>Vector de ataque</td><td>Acceso sin autorizació y filtración de datos.</td></tr>
<tr><td>Impacto técnico / operativo</td><td>Cifrado masivo de servidores, pérdida de acceso a sistemas críticos, exposición de información sensible y riesgo legal y reputacional elevado.</td></tr>
<tr><td>Medida de control recomendada</td><td>Una mejoría en la forma de control de acceso y en el cifrado de los datos</td></tr>
</table>
</td></tr>
<tr><td>Escenario 02</td><td>
<table>
<tr><th>Elemento</th><th>Respuesta</th></tr>
<tr><td>Servicios X.800 comprometidos.</td><td>Confidencialidad
Control de acceso</td></tr>
<tr><td>Definición(es) aplicable(s) RFC 4949.</td><td>Misconfiguration: Configuración incorrecta de un sistema que introduce vulnerabilidades de seguridad.
Exposure: Condición en la que un sistema o información queda accesible sin la protección adecuada.
Unauthorized Access: Acceso a un sistema o recurso sin autorización válida.</td></tr>
<tr><td>Tipo de amenazas</td><td>Externa por error interno</td></tr>
<tr><td>Vector de ataque</td><td>Mala configuración de los permisos para los servicios de la nube como el almacenamiento</td></tr>
<tr><td>Impacto técnico / operativo</td><td>Exposición pública de datos sensibles, posibles sanciones legales y daño reputacional.</td></tr>
</table>
</td></tr>
</table>

	Medida de control recomendada	Un monitoreo continuo de accesos y auditorias de los cargos superiores.
Escenario 03	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Integridad Confidencialidad
	Definición(es) aplicable(s) RFC 4949.	Supply chain attack: Ataque que compromete un sistema a través de un proveedor o componente confiable. Malicious code: Software diseñado para causar daño, alterar sistemas o acceder sin autorización. Trust exploitation: Abuso de una relación de confianza para realizar acciones no autorizadas.
	Tipo de amenazas	Externa
	Vector de ataque	Compromiso del proveedor de software y distribución de actualizaciones maliciosas.
	Impacto técnico / operativo	Instalación de código malicioso en múltiples organizaciones, acceso no autorizado a sistemas internos y ruptura de la confianza en el proveedor.
	Medida de control recomendada	Verificación de integridad de actualizaciones, firmas digitales.
Escenario 04	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Autenticación Control de acceso
	Definición(es) aplicable(s) RFC 4949.	Phishing es un ataque de ingeniería social para obtener información sensible mediante engaño. Credential compromiso: Situación en la que credenciales válidas son robadas o utilizadas por un atacante. Authentication failure: Falla del servicio de autenticación que permite accesos indebidos o rechaza accesos legítimos.
	Tipo de amenazas	Externa
	Vector de ataque	Obtención de datos personales.
	Impacto técnico / operativo	Acceso persistente no detectado, robo de información.
	Medida de control recomendada	Implementación de doble autenticación y detección de patrones inusuales.
Escenario 05	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Disponibilidad Integridad
	Definición(es) aplicable(s) RFC 4949.	Data destruction: Eliminación intencional o no autorizada de información. Availability attack: Servicios en peligro en la accesibilidad de estos
	Tipo de amenazas	Externa
	Vector de ataque	Manipulación de respaldos y copias de seguridad.
	Impacto técnico / operativo	Perdidas tanto económicas como información.
	Medida de control recomendada	Mejores formas de respaldo y pruebas de restauración de la información.
Escenario 06	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Confidencialidad Control de acceso
	Definición(es) aplicable(s) RFC 4949.	Insider threat Amenaza originada por un usuario autorizado dentro de la organización. Privilege abuse Uso indebido de privilegios legítimos para realizar acciones no autorizadas.
	Tipo de amenazas	Interna.
	Vector de ataque	Acceso a información crítica.
	Impacto técnico /	Filtración de datos y daño en la reputación.

	operativo	
	Medida de control recomendada	Mayor introspección entre el personal y un mayor monitoreo de las acciones internas.
Escenario 07	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Integridad No repudio
	Definición(es) aplicable(s) RFC 4949.	Evidentiary integrity Garantía de que la evidencia digital no ha sido alterada ni manipulada. Audit trail compromiso Alteración o eliminación de registros de auditoría para ocultar actividades.
	Tipo de amenazas	Externa
	Vector de ataque	Manipulación de registros del sistema.
	Impacto técnico / operativo	Privación de información y perdida de esta misma para búsquedas futuras.
	Medida de control recomendada	Un sistema de control para el acceso de los registros y más monitoreo.
Escenario 08	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Disponibilidad
	Definición(es) aplicable(s) RFC 4949.	Operational failure Falla en la operación normal de un sistema que afecta su funcionamiento esperado. Service disruption Interrupción parcial o total de un servicio informático.
	Tipo de amenazas	Interna
	Vector de ataque	Actualizaciones sin supervisión
	Impacto técnico / operativo	No se puede acceder a los servicios.
	Medida de control recomendada	Un entorno dedicado a pruebas y planes de emergencia.
Escenario 09	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Autenticación Confidencialidad
	Definición(es) aplicable(s) RFC 4949.	Masquerade Ataque en el que una entidad se hace pasar por otra legítima. Phishing Ataque de ingeniería social que busca obtener información sensible mediante engaño. Social engineering Técnicas de manipulación en la población
	Tipo de amenazas	Externa
	Vector de ataque	Suplantación de identidad.
	Impacto técnico / operativo	Filtración de información.
	Medida de control recomendada	Implementación de métodos de autenticación y hacerles ver la importancia de estos errores.
Escenario 10	**Elemento**	**Respuesta**
	Servicios X.800 comprometidos.	Confidencialidad Integridad Disponibilidad
	Definición(es) aplicable(s) RFC 4949.	Destructive attack Ataque diseñado para dañar, eliminar o inutilizar sistemas o información. Data destruction Eliminación intencional o no autorizada de datos.
	Tipo de amenazas	Externa
	Vector de ataque	Acceso a sistemas y datos privados y eliminación de estos mismos.
	Impacto técnico / operativo	Daño interno a la organización y perdida de los sistemas y datos.
	Medida de control recomendada	Métodos de detección a tiempo, respaldos y monitoreo seguidos.

Conclusión

A partir del análisis de los distintos escenarios, se refuerza la idea de que un ataque cibernético puede generar repercusiones que van mucho más allá del ámbito tecnológico. Actualmente, la mayoría de los procesos, servicios y actividades con los que interactuamos de manera cotidiana se encuentran directa o indirectamente vinculados a la tecnología, por lo que una falla, mala configuración o ataque a los sistemas informáticos puede derivar en consecuencias graves a nivel operativo, económico y social.

De igual manera, este ejercicio permite reflexionar sobre la relevancia de contar con estándares y marcos de seguridad informática que orienten la implementación de controles adecuados. La adopción de estos estándares contribuye a reducir la exposición a vulnerabilidades y a fortalecer la protección de la información, resaltando la responsabilidad que tienen tanto las organizaciones como los individuos que se forman en el área de la ciberseguridad.

Referencias

International Telecommunication Union. (1991). Security architecture for open systems interconnection for CCITT applications (ITU-T Recommendation X.800).

Shirey, R. (2007). RFC 4949: Internet Security Glossary, Version 2. IETF.