

Fecha:

UNIVERSIDAD AUTÓNOMA "TOMAS FRÍAS"  
CARRERA DE INGENIERÍA DE SISTEMAS

Materia:	Seguridad de Sistemas (SIS - 737)
Docente:	M. Sc. Ing. Javier Alexander Durán Miranda
Auxiliar:	Univ. Aldair Roger Pérez Miranda
Estudiante:	Univ. Nelly Mamaní Tupía
Grupo:	1
Fecha:	27/04/2025

### Análisis de Riesgo

3: Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida.

#### Determinar el Alcance

Departamento de la Red Corporativa y los tres switches de la infraestructura.

#### Identificar y Valorar Activos

##### Dispositivos

Dispositivo	Disponibilidad	Integridad	Confidencialidad	Importancia
Switches de red	4 + 4	4 + 5		4 Alto

##### Software y APP:

Software / Aplicación	D.	I	C	I
Protocolo Telnet	3 + 2	2 + 2		2 medio

##### Personal

##### Personal

Administradores	D	I	C	I
	4 + 5	5 + 5		5 muy alto

### Instalaciones

Instalación	D	I	C	I	
Instalación	D	I	C	I	
Edificio central	S	S	S	S	5 muy alto

### Identificar las Amenazas

#### Dispositivos

#### Switches de red:

Amenaza: Acceso no autorizado a la configuración de red

Causado por la interceptación de credenciales a través del protocolo telnet, que no cifra la información

#### Software y APP:

#### Protocolo telnet

Amenaza: Acceso no autorizado al sistema debido a la falta cifrado de las credenciales de acceso

Possibles ataques de interceptación (MITM) o fuerza bruta para obtener contraseñas

#### Personal

#### Administradores

Amenaza: Error humano en la configuración o manejo de las credenciales de acceso a través de telnet

Falta de concientización sobre la inseguridad del protocolo

#### Instalaciones

#### Edificio central

Amenaza: Acceso no Autorizado a la infraestructura física donde se alojan los switches lo que permite manipular las

configuración, directamente.

## Identificar Vulnerabilidades y Salvaguardas

### Dispositivos

#### Switches de red

Vulnerabilidad: Uso inadecuado o descuido del control de acceso Fisico

Salvaguarda: Deshabilitar telnet y utilizar SSL para cifrar

las comunicaciones, configurar control de acceso

basado en direcciones IP confiables y habilitar autenticación

multifactor para el acceso remoto.

#### Software y APP:

##### Protocolo Telnet:

Vulnerabilidad: Falta de cifrado en las comunicaciones

Salvaguarda: Migrar a SSL y asegurarse de que todos los

accesos remotos sean cifrados

#### Personal:

##### Administradores:

Vulnerabilidad: Falta de conciencia acerca de la seguridad

Salvaguarda: Capacitar a los administradores de red sobre

la importancia de utilizar protocolos seguros

como SSH y la gestión adecuada de contraseñas

### Instalaciones

#### Edificio Central

Vulnerabilidad: Uso inadecuado o descuidado del control de

acceso físico a las instalaciones o recintos

Salvaguarda: Implementar controles de acceso físicos

a las salas de servidores y switches utilizando

cerraduras electrónicas y sistemas de

video vigilancia.

### Evaluar el riesgo

#### Probabilidad de ocurrencias

Alta: La exposición a ataques es probable, especialmente

si se sigue utilizando Telnet en los switches

y no se implementan controles adecuados de acceso

#### Impacto

Alto: El acceso no autorizado a la configuración

de los switches podría interrumpir toda la

la infraestructura de red, afectando la disponibilidad y la seguridad de los servicios de la empresa.

### Riesgo global:

**Alto:** da posibilidad de que un ataque complejo comprometa el sistema de administración de los switches. Representa un riesgo significativo para la organización, tanto en términos de impacto de probabilidad.

### Tratar el Riesgo

- 1.- Deshabilitar telnet y migrar a SSH; Asegurar que toda la ~~información~~ administración remota esté cifrada y protegida.
- 2.- Implementar autenticación multifactor (MFA); Esto asegura que solo personas autorizadas puedan acceder a la configuración de los switches.
- 3.- Formación continua a los administradores; Asegurarse de que comprendan la importancia de las mejores prácticas de seguridad, incluyendo el uso de contraseñas fuertes y políticas de acceso seguro.
- 4.- Implementar control de acceso físico; Proteger las instalaciones, mediante sistemas de acceso biométrico, cerraduras electrónicas, y monitoreo con cámaras de seguridad.
- 5.- Monitoreo y auditoría continua; Implementar herramientas de monitoreo para detectar intentos de acceso no autorizado a la configuración de la red y realizar auditorías regulares de seguridad.

- ④ En los últimos seis meses, se identificaron en los registros del servidor web, peticiones de conexión provenientes de direcciones IP que de acuerdo a una revisión la gran mayoría a ellas corresponden al IP registrado para países europeos.

### Determinar el Alcance

Departamento de Tecnologías de información y el servidor web de la banca en línea.

#### Identificar y Valorar Actores

Dispositivos	D	I	C	I.
Computadoras	3	+	2	+
Servidor Web	5	+	4	+

Software y APP	D	I	C	I
Antivirus	4	+	5	+
Antimalware	4	+	5	+

Personal	D	I	C	I
Funcionarios	3		2	4

#### Identificar las amenazas

##### Dispositivos

Computadoras

Amenaza: Errores del administrador

Amenaza:

##### Servidor web

Amenaza: Errores de configuración

Amenaza: Vulnerabilidad de los programas (software)

##### Software APP:

###### Antivirus:

Amenaza: Vulnerabilidad de los programas de software

###### Antimalware:

Amenaza: Errores y fallos no intencionados, Errores de configuración

##### Personal

###### Funcionarios:

Amenaza: Manipulación de programas

Amenaza: Falta de capacitación en seguridad lo que puede llevar a errores humanos

## Identificar Vulnerabilidades y Salvaguardas

### Propósitos Computadoras

Vulnerabilidad: Ausencia de control o eficiente control de cambios en la configuración

Salvaguarda: Implementar controles de acceso más estrictos y procedimientos de autorización

Vulnerabilidad: Falta de conciencia acerca de la seguridad

Salvaguarda: Aplicar políticas de acceso basadas en el principio de menor privilegio.

### Servidor Web

Vulnerabilidad: Software nuevo o inmaduro

Salvaguarda: Implementar un ciclo adecuado de pruebas antes de la implementación de software nuevo

### Software APP

#### Antivirus

Vulnerabilidad: Programas con vulnerabilidades sin parches aplicados

Salvaguarda: Mantener actualizado el antivirus y realizar auditorías periódicas de seguridad

#### Antimalware

Vulnerabilidad: Configuración incorrecta de parámetros

Salvaguarda: Realizar pruebas periódicas de efectividad y capacitación del personal

#### Personal

#### Funcionario

Vulnerabilidad: Procedimientos inadecuados de contratación

Salvaguarda: Realizar un programa de capacitación continua en seguridad y políticas informáticas

## Evaluar el riesgo

Probabilidad: Media (las amenazas son previsibles pero no ocurren siempre)

Impacto: Alto (puede comprometer la integridad de la aplicación bancaria y la seguridad de los clientes).

Riesgo global: Alto

Fecha:

## Tratar el riesgo

### Computadoras

- Establecer procedimientos más estrictos de configuración y control de cambios.
- Implementar políticas de seguridad de acceso.

### Servidor Web

- Implementar un ciclo de pruebas exhaustivas para todas las actualizaciones del servidor.
- Adoptar nuevas tecnologías con un proceso de estabilización más riguroso.

### Software (Antivirus y Antimalware)

- Mantener software actualizado y realizar auditorías de seguridad regulares.
- Asegurar que el personal esté capacitado en el uso correcto de las herramientas de seguridad.

### Personal (Funcionarios)

- Realizar entrenamientos de seguridad continua, especialmente en el uso de aplicaciones críticas.

(3) Debido a presión de la alta dirección, la aplicación móvil fue lanzada a producción, únicamente siendo testeada con pruebas de caja blanca y caja negra.

### Determinar el Alcance

Departamento de Tecnologías de Información y la aplicación móvil.

#### Identificar y Valorar Activos

Dispositivos	D	I	C	I	
Dispositivos móviles	5	+	4	+	4

$$13/3 = 4 \text{ alto}$$

Software y APP	D	I	C	I	
Aplicación móvil	4	3	5		
Framework de prueba (casa blanca / negra)	3	+	3	+	2

$$12/3 = 4 \text{ alto}$$
$$8/3 = 3 \text{ medio}$$

Personal	D	I	C	I	
Equipo de desarrollo y QA	4	+	4	+	4

$$12/3 = 4 \text{ alto}$$

#### Identificar las Amenazas

Dispositivos móviles

Amenaza: Phishing o ingeniería social para instalar versiones maliciosas de la app

Amenaza: Malware o permisos excesivos en el dispositivo cliente

#### Aplicación móvil:

Amenaza: Explotación de vulnerabilidades de lógica o inyección por falta de prueba de penetración (pen-testing)

Amenaza: Crashs y fugas de datos sensibles (credenciales, información personal)

#### Frameworks de prueba

Amenaza: Cobertura incompleta de caso de uso, dejando vectores de ataque sin evaluar

#### Equipos de desarrollo y QA

Amenaza: Errores de configuración

#### Identificar Vulnerabilidades y salvaguardas

Dispositivos móviles

Vulnerabilidad: Uso de dispositivos con SD desactivado o rota da

Salvaguardia: Requerir versiones mínimas de SD y validar la integridad del dispositivo (safeNet, DeviceCheck)

## Aplicación móvil

Vulnerabilidad: Ausencia de prueba de penetración y fuzzing

Salvaguarda: Incluir pentesting regular, fuzzing de entradas y análisis estático / dinámico en el pipeline CI/CD

## Frameworks de prueba

Vulnerabilidad: Limitación a pruebas funcionales (caja blanca / negra) sin enfoque en seguridad

Salvaguarda: Integrar herramientas de SAST / DAST y pruebas de seguridad automatizadas

## Equipos de desarrollo y QA

Vulnerabilidad: Falta de formación en seguridad de API's móviles

Salvaguarda: Capacitación continua en OWASP Mobile Top 10 y políticas de codificación segura

## Evaluar el riesgo

Probabilidad: Media - alta (la presión de lanzamiento sin pruebas exhaustivas favorece exposición a ataques)

Impacto: Alto (la explotación puede exponer datos de clientes, dañar la reputación y originar sanciones)

Riesgo global: Alto

## Tratar el riesgo

1. Incorporar Pentesting y Fuzzing en cada release: Contratar terceros y usar herramientas automáticas.

2. Automatizar análisis de seguridad (SAST / DAST) en el pipeline CI/CD

⑦ Recientemente finalizó el tiempo de licencia que se cancela por un software (DLP) que monitoreaba el tráfico, controlando que ningún documento digital etiquetado como confidencial pueda ser enviado por email, mensajería, etc.

### Determinar el alcance

Departamento de tecnologías de información y el sistema DLP

#### Identificar y valorar activos

Activos	D	I	C	I	
Servidor DLP	4	+	5	+	5

$$14/3 = 5 \text{ muy alto}$$

Activos	D	I	C	I	
Licencia DLP	2	+	5	+	5

$$12/3 = 4 \text{ alto}$$

Activos	D	I	C	I	
Equipo de seguridad	4	+	4	+	5

$$14/3 = 5 \text{ muy alto}$$

#### Identificar las amenazas

Servidor DLP:

Amenaza: Fugas de información

Amenaza: Desactivación de políticas DLP al expirar la licencia

#### Licencia DLP:

Amenaza: Falta de notificación oportuna de caducidad provocando lapsos sin protección

#### Equipo de seguridad

Amenaza: Confianza excesiva en un sistema no operativo retrasando la respuesta a incidentes

#### Identificar Vulnerabilidades y Salvaguardias

Servidor DLP

Vulnerabilidad: Dependencia de un único servidor sin respaldo  
Salvaguardia: Implementar alta disponibilidad y backup periódico de la configuración

#### Licencia DLP

Vulnerabilidad: Proceso manual de renovación sin alertas automáticas

Salvaguardia: Configurar alertas de expiración (30/15/7d)

#### Equipo de seguridad

Vulnerabilidad: Ausencia de procedimientos alternativos

Salvaguardia: Definir playbooks de respuesta que incluyan controles manuales y soluciones temporales

## Evaluar el riesgo

Probabilidad: Media-alta (Olvidos en renovaciones son comunes)

Impacto: Alto (exposición de datos críticos y cumplimientos normativos comprometidos)

Riesgo global: Alto

## Tratar el riesgo:

- 1.- Automatizar la renovación de licencias con recordatorios escalonados a niveles gerenciales.
- 2.- Desplegar un control DLP secundario o política de prevención de fuga en el gateway de correo HTTPS como respaldo.
- 3.- Actualizar play books de incidentes, respuesta para cubrir periodos sin DLP activo.
- 4.- Auditorías periódicas del estado de licencias y efectividad de las salvaguardas.

- ⑧ Para asignar un activo de información (PC) a un nivel funcional, primero se procede a realizar la eliminación segura de toda la información que se almacenaba anteriormente en dicha PC (formato en bajo nivel)

### Determinar el Alcance

Departamento de Tecnologías de Información y el proceso de reasignación de PC de ex-funcionarios a nuevos usuarios

### Identificar y valorar Activos

#### Dispositivos

Computadoras reasignadas  $D = 4 + I = 4 + 5 = 13 / 3 = 4$  Alto

#### Software y APP

Utilidad de formato  $D = 2 + I = 2 + 2 = 6 / 3 = 2$  medio

#### Personal

Nuevos usuarios de PC  $D = 4 + I = 4 + 4 = 12 / 3 = 4$  alto

### Identificar las Amenazas

#### Computadoras reasignadas

Amenaza: Recuperación de datos residuales (documentos, credenciales)

Amenaza: Divulgación accidental de información confidencial previa

#### Utilidad de Formato

Amenaza: Borrado superficial que deja datos recuperables

Amenaza: Ausencia de registro o certificación del proceso de borrado

#### Nuevos usuarios de PC

Amenaza: Acceso accidental o malicioso a información residual almacenada

Amenaza: uso inadecuado de datos que no les corresponden

### Identificar Vulnerabilidades y Salvaguardas

#### Computadoras reasignadas

Vulnerabilidad: Formateo "bajo nivel"

Salvaguardia: Usar herramientas de borrado seguro / DOD 5220.22-M o equivalentes, y cifrado completo de disco

#### Utilidad de Formato

Vulnerabilidad: No genera informes ni logs de borrado

Salvaguardia: Implementar solución centralizada que genere certificados de destrucción y almacene logs de la operación

## Nuevos usuarios de PC

Vulnerabilidad: Desconocimiento de riesgos de datos residuales.

Salvaguardia: Capacitación obligatoria en políticas de seguridad de dispositivos antes de asignar el equipo.

## Evaluación del riesgo

Probabilidad: Alta (es habitual omitir procesos de borrado seguro)

Impacto: Muy alto (exposición de datos personales, comerciales o regulatorios)

Riesgo global: Muy alto.

## Tratar el Riesgo

- 1.- Implementar cifrado de disco en todos los endpoints para que incluso sin borrado, los datos queden inaccesibles.
- 2.- Adoptar herramientas de wiping certificadas con generación automática de reportes y almacenamiento en repositorio de auditoría.
- 3.- Establecer cadena de custodia para equipos en espera de borrado, con registro de cada paso.
- 4.- Formación continua de TI y Recursos humanos en procedimientos de borrado seguro y políticas de reasignación.
- 5.- Auditorías periódicas de los equipos reasignados para verificar que no queden datos residuales.