Universidad Autónoma Tomás Frías Ingeniería de Sistemas	Nota
SIS 737 SEGURIDAD DE SISTEMAS	
NOMBRE: UNIV. SAAVEDRA MARCA PATRICIA EMILIA	
DOCENTE: ING. ALEXANDER DURÁN	
AUXILIAR: UNIV. ALDRIN ROGER PEREZ MIRANDA	**RU:** 109457
Practica N°2: Análisis de riesgos	

Producto del análisis realizado a la financiera La Caridad, se identificaron los siguientes puntos:

- La comunicación entre el edificio principal y su única sucursal se realiza mediante fibra óptica, además que se cuenta con un segundo proveedor de servicios ISP, para evitar cortes de servicio.
- Producto de algunos inconvenientes con la generación de reportes, se optó por comprar una solución de pago incluyendo el soporte para esta generación de reportes en tiempos y formas más optimas, dicho software agilizó de gran forma este proceso en la institución.
- Para la administración remota de todos los switches de la red interna, se tiene habilitado el protocolo telnet para hacer modificaciones de manera rápida.
- En los últimos seis meses, se identificaron en los registros o logs del servidor web, peticiones de conexión provenientes de direcciones Ips que de acuerdo a una revisión la gran mayoría de ellas corresponden a ip registradas para países europeos.
- 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.
- Ninguna de las PCs permite la utilización de memorias USB, DVDs, o cualquier tipo de medio removible sin la habilitación y revisión por le oficial de seguridad de la información.
- Recientemente finalizó el tiempo de licencia que se cancelaba por un software (DLP) que monitoreaba el tráfico, controlando que ningún documento digital etiquetado como confidencial pueda ser enviado por email, mensajería, etc.
- Para asignar un activo de información (PC) a un nuevo funcionario, primeramente se procede a realizar la eliminación segura de toda la información que se almacenaba anteriormente en dicha PC (formato en bajo nivel).

1. **ALCANCE**

Alcance: El análisis se centra en los activos de la financiera La Caridad con riesgos altos, relacionados con la red interna (switches), el servidor web, la aplicación móvil, y la gestión de datos confidenciales (sin DLP). Se evaluarán impactos en la disponibilidad, integridad, y confidencialidad de la información y servicios.

2. **IDENTIFICAR ACTIVOS:**

Equipamiento informático:

- Switches de la red interna: Administrados vía Telnet, vulnerables a accesos no autorizados (punto 2).

Software - Aplicaciones informáticas:

- **Software DLP (desactivado)**: Inactivo, permite fugas de datos confidenciales (punto 5).
- **Aplicación móvil**: Lanzada con pruebas limitadas, susceptible a vulnerabilidades (punto 4).
- **Software del servidor web**: Gestiona peticiones externas, expuesto a ataques (punto 3).

Personal:

- **Usuarios**: Pueden enviar datos confidenciales por error (sin DLP, punto 5).

Redes de comunicaciones:

- **Red interna (switches)**: Administrada vía Telnet, vulnerable a interceptaciones (punto 2).

Valorar activos:

ACTIVO	ESPECIFICACIONES	VALORACIÓN				IMPORTANCIA
Equipamiento informático	Switches	**D 4**	**I 4**	**C 5**	**TOTAL 13/3=4**	ALTA

ACTIVO	ESPECIFICACIONES	VALORACIÓN				IMPORTANCIA
Software - Aplicaciones informáticas	Aplicación móvil	**D 5**	**I 5**	**C 5**	**TOTAL 5**	MUY ALTO
	Software del servidor web	**D 5**	**I 5**	**C 5**	**TOTAL 5**	MUY ALTO

ACTIVO	ESPECIFICACIONES	VALORACIÓN				IMPORTANCIA
Personal	Usuarios	**D**	**I**	**C**	**TOTAL**	ALTO

		2	**4**	**5**	**11/3=3.7=4**	
Redes de comunicaciones	Red interna (switches)	**D 2**	**I 4**	**C 5**	**TOTAL 11/3=3.7=4**	ALTO

3. **IDENTIFICAR LAS AMENAZAS:**

ACTIVO: Equipamiento informático
Ataques intencionados: Acceso no autorizado **(I,C),** denegación de servicio **(D)** (servidor web, IPs europeas)
Ataques intencionados: manipulación de la configuración (switches vía Telnet). **(D,I,C)**
ACTIVO: **Software - Aplicaciones informáticas**
Errores no intencionados: Vulnerabilidades de software (aplicación móvil por pruebas limitadas). **(D,I,C)**
Ataques intencionados: Difusión de software dañino: al Servidor web. **Vulnerabilidades:** Defectos bien conocidos de software (vulnerabilidades no parcheadas). Configuración incorrecta de parámetros.
ACTIVO: **Personal**
Errores no intencionados: Escapes de información (envío de datos confidenciales sin DLP) **(I,C)** **Vulnerabilidad:** Ausencia de mecanismos de monitoreo (no controla datos confidenciales).
ACTIVO: **Redes de comunicaciones**
Ataques intencionados: Interceptación de información **(C)** ,acceso no autorizado **(I,D)** (Telnet en switches) **Vulnerabilidades:** Transferencia de contraseñas en claro (Telnet) Y Gestión inadecuada de la red (configuración incorrecta)

4. **IDENTIFICAR VULNERABILIDADES**

ACTIVO: Equipamiento informático
(servidor web, IPs europeas). **Vulnerabilidad: Ausencia de pistas de auditoría** (Falta de registros (logs) o monitoreo adecuado para rastrear actividades sospechosas).
Ataques intencionados: manipulación de la configuración (switches vía Telnet). **(D,I,C)** **Vulnerabilidad: Ausencia de un eficiente control de cambios en la configuración**, lo cual, facilita **manipulación no autorizada** o **errores de configuración** que pueden causar interrupciones o accesos indebidos.
ACTIVO: **Software - Aplicaciones informáticas**
Errores no intencionados: Vulnerabilidades de software (aplicación móvil por pruebas limitadas). **(D,I,C)** **Vulnerabilidad: Software nuevo o inmaduro**, la aplicación no ha sido suficientemente probada, lo que introduce vulnerabilidades desconocidas.
Ataques intencionados: Difusión de software dañino: al Servidor web. **Vulnerabilidad: Defectos bien conocidos de software (vulnerabilidades no parcheadas),** lo cual, permite acceso no autorizado, ejecución de código malicioso o denegación de servicio.
ACTIVO: **Personal**
Errores no intencionados: Escapes de información (envío de datos confidenciales sin DLP) **(I,C)** **Vulnerabilidad: Ausencia de mecanismos de monitoreo y Ausencia de políticas para el uso de telecomunicaciones/mensajería**, lo cual, facilita **divulgación de información sensible** por errores no intencionados o ataques intencionados
ACTIVO: **Redes de comunicaciones**
Ataques intencionados: Interceptación de información **(C)** ,acceso no autorizado **(I,D)** (Telnet en switches)

Vulnerabilidad: Transferencia de contraseñas en claro (Telnet), lo cual, permite **interceptación de credenciales** y **acceso no autorizado** a la red. Relacionado con amenazas de ataques intencionados

5. **EVALUAR RIESGOS**

ACTIVO: Equipamiento informático							
N	**DESCRIPCION DEL RIESGO**	**PROBABILIDAD**	**IMPACTO**				**RIESGO**
			FINANCIERO	**IMAGEN**	**OPERATIVO**	**TOTAL**	**P*I**
1	Ausencia de pistas de auditoría en el servidor web (falta de logs/monitoreo).	4	4	4	4	4	16
2	Ausencia de control de cambios en la configuración en los switches (manipulación no autorizada)	4	4	4	5	4,33333 3333	17,3333 3333
		total					33,3333 3333

ACTIVO: Software - Aplicaciones informáticas							
N	**DESCRIPCION DEL RIESGO**	**PROBABILIDAD**	**IMPACTO**				**RIESGO**
			FINANCIERO	**IMAGEN**	**OPERATIVO**	**TOTAL**	**P*I**
3	Software nuevo/inmaduro con pruebas limitadas de la app (vulnerabilidades desconocidas y fallos o accesos no autorizados por software poco probado).	5	4	5	4	4,33333 3333	21,6666 6667
4	Defectos conocidos no parcheados del software de la web(acceso no autorizado, código malicioso).	4	4	4	5	4,33333 3333	17,3333 3333
		total					39

ACTIVO: personal							
N	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	P*I
5	Ausencia de monitoreo y políticas de telecomunicaciones/ mensajería (fuga de datos por falta de monitoreo y políticas de mensajería).	3	3	5	4	4	12
		total					12

ACTIVO: Redes de comunicaciones							
N	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	P*I
6	Transferencia de contraseñas en claro (ntercepción de credenciales y accesos indebidos por contraseñas en claro, telnet)	4	4	5	3	4	16
		total					16

MATRIZ DE RIESGOS

MUY ALTO (5)	MEDIO	MEDIO	ALTO	**4**	MUY ALTO
ALTO (4)	BAJO	MEDIO	5	**1,2**	**3**
MEDIO -3	MUY BAJO	BAJO	MEDIO	**6**	ALTO
BAJO (2)	MUY BAJO	BAJO	BAJO	MEDIO	MEDIO
MUY BAJO (1)	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	MEDIO
	MUY BAJO (1)	BAJO (2)	MEDIO (3)	ALTO (4)	MUY ALTO (5)

6. **TRATAR RIESGO**

Activo	Riesgo	Contramedida
Equipamiento informático (Servidor web, IPs europeas)	Intrusiones no detectadas por falta de logs/monitoreo (D, I, C).	Implementar un sistema de registro de logs y monitoreo en tiempo real (SIEM).
	Manipulación no autorizada por ausencia de control de cambios (D, I, C).	Establecer un proceso formal de control de cambios con auditorías regulares.
Software - Aplicaciones informáticas	Fallos o accesos no autorizados por software poco probado (D, I, C).	Realizar pruebas exhaustivas de seguridad (pentesting) antes del despliegue.
	Código malicioso o denegación de servicio por vulnerabilidades no parcheadas (D, I, C).	Aplicar parches de seguridad regularmente y usar herramientas de gestión de vulnerabilidades.
Personal	Fuga de datos por falta de monitoreo y políticas de mensajería (I, C).	Implementar DLP (Data Loss Prevention) y políticas claras de uso de mensajería.
Redes de comunicaciones	Intercepción de credenciales y accesos indebidos por contraseñas en claro (Telnet) (I, D, C).	Reemplazar Telnet por SSH y usar autenticación multifactor (MFA).

Notas:

- **D**: Disponibilidad, **I**: Integridad, **C**: Confidencialidad.