	UNIVERSIDAD AUTÓNOMA "TOMÁS FRÍAS" INGENIERÍA DE SISTEMAS				
	Estudiante:	Univ.Cristian Sixto Sunagua Gira			
	Docente:	M.Sc.Ing.J. Alexander Durán.M	**Materia:**	SIS-737	**GRUPO 1**
	Auxiliar:	Univ. Aldrin Roger Perez Miranda	**Fecha:**	28/04/2025	**PRACTICA 2**
Enlace:	https://github.com/Cristian-sg01/sis-737_practica_2		**C.I:**	8600448	

DETERMINAR EL ALCANCE

Departamento Financiera La Caridad

IDENTIFICAR Y VALORAR ACTIVOS

DISPOSITIVOS: Switches, Servidor, PCs

SOFTWARE Y APP: App Movil, DLP, Generación de Reportes

PERSONAL: Funcionarios

INSTALACIONES: Edificio Principal, Sucursal

TELECUMUNICAIONES: Fibra

IDENTIFICAR Y VALORAR ACTIVOS

DISPOSITIVOS:	**Disp.**	**Integ.**	**Confi.**	**Importancia**
Switches	5	+ 4	+4 = 13/3 =4	alto
Servidor	5	+ 4	+4 = 13/3 =4	alto
PCs	5	+ 4	+4 = 13/3 =4	alto

SOFTWARE Y APP:

App Movil	4 + 5 + 5 = 14/3 = 5	muy alto
DLP	4 + 5 + 5 = 14/3 = 5	muy alto
Generación de reportes	4 + 5 + 5 = 14/3 = 5	muy alto

PERSONAL:

Funcionarios	3 + 2 + 4 = 9/3 = 3	medio

INSTALACIONES:

Edif. Principal	5 + 5 + 5 = 15/3 = 5	muy alto
Sucursal	4 + 4 + 5 = 15/3 = 4	alto

TELECOMUNICACIONES:

Fibra Óptica	4 + 3 + 1 = 8/3 = 3	medio

IDENTIFICAR LAS AMENAZAS

DISPOSITIVOS: **Servidor:**

Ataques intencionados: acceso no autorizado/manipulación de configuración

Ataques de fuerza bruta, escaneo de vulnerabilidades, acceso no autorizado, los ataques malintencionados obtienen acceso indebido al servidor para alterar su configuración, comprometiendo su funcionamiento y exponiendo datos sensibles. Esto puede provocar interrupciones en los servicios, pérdida de información crítica o vulneración de sistemas completos.

Switches:

Ataques intencionados: divulgación de la información/destrucción de la información

Ocurre cuando atacantes acceden a los switches de red para interceptar o eliminar datos que circulan a través de ellos. Esto puede derivar en pérdida de integridad de la información, filtraciones de datos confidenciales y caídas parciales o totales de la red institucional.

SOFTWARE Y APP: App Movil:

Errores y fallos no intencionados: vulnerabilidades de los programas/errores de configuración

Se presentan cuando existen fallos de programación o configuraciones incorrectas en la aplicación móvil, lo que facilita que usuarios no autorizados exploten estos errores para acceder o modificar datos. El impacto incluye el robo de información personal, accesos indebidos y daños a la reputación de la organización.

DLP:

Errores y fallos no intencionados: escapes de información/fugas de información

Sucede cuando los mecanismos del DLP fallan, permitiendo que documentos sensibles sean enviados o copiados sin control. Esto podría desencadenar filtraciones de información estratégica o confidencial, afectando la competitividad y la confianza de clientes y socios.

IDENTIFICACION DE VULNERAVILIDADES Y SALVAGUARDAS

DISPOSITIVOS: **Servidor:**

Personal: Ausencia de mecanismo de monitoreo

No contar con herramientas que supervisen la actividad del servidor permite que incidentes de seguridad pasen desapercibidos. Esto facilita accesos no autorizados, alteraciones en la configuración o la extracción de datos sin ser detectados a tiempo.

Redes de comunicaciones: Ausencia de identificación y autentificación de emisor y receptor

La falta de métodos seguros para verificar quién envía o recibe información en la red puede permitir que atacantes suplanten identidades o intercepten comunicaciones, provocando robo de información o fraudes internos.

Switches:

Redes de comunicaciones: Transferencia de contraseñas en claro/ trafico sensible sin protección

Cuando los datos y contraseñas circulan por la red sin encriptación, se vuelven vulnerables a ser capturados por atacantes mediante técnicas como "sniffing". Esto puede permitir accesos ilegítimos, espionaje de datos y alteraciones en la red interna.

Como el protocolo TELNET no es un protocolo 100% seguro si un atacante hace un "sniffing" o escucha la red, puede capturar las credenciales y los datos fácilmente

Salvaguarda-→ Se considera que al menos tenga algún protocolo, aunque no sea 100% seguro

SOFTWARE Y APP: **App Movil:**

Software – Aplicaciones informáticas: Software nuevo o inmaduro

Las aplicaciones móviles recientes o no suficientemente probadas suelen tener errores de programación o vulnerabilidades desconocidas. Estos fallos pueden ser explotados para obtener acceso a bases de datos, manipular funcionalidades o comprometer la privacidad de los usuarios.

Como solo fue probada con caja blanca y caja negra puede explotar los fallos o errores de la aplicación

DLP:

Personal: Ausencia de mecanismo de monitoreo/falta de conciencia acerca de la seguridad

Si el personal encargado no monitorea adecuadamente el funcionamiento del DLP o desconoce su importancia, las políticas de protección de datos pueden ser fácilmente ignoradas o desactivadas. Esto aumenta el riesgo de fugas accidentales o intencionales de información confidencial.

Como ya no se va pagando el software DLP esto llegaría a fallar la y que hubiera fugas

EVALUAR RIESGO

ACTIVO: DISPOSITIVOS

N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
01	Acceso no autorizado o manipulación del servidor por falta de monitoreo	4	4	4	5	4.33	17.33
						Riesgo Promedio	17.33
N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
02	Robo de información por falta de autenticación en comunicaciones del servidor	4	5	5	4	4.33	17.33
						Riesgo Promedio	17.33

N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
03	Captura de contraseñas y tráfico sensible no protegido en switches	3	5	4	5	4.33	13
						Riesgo Promedio	13

Salvaguarda-> Probabilidad reducida de 4 a 3 considerando que tiene al menos un protocolo de seguridad

ACTIVO: SOFTWARE Y APLICACIONES

N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
01	Explotación de vulnerabilidades en app móvil por ser software nuevo o inmaduro	3	3	4	3	3.33	10
						Riesgo Promedio	10
N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
02	Fugas de información por falta de monitoreo y baja conciencia de seguridad en DLP	3	2	3	3	2.66	8
						Riesgo Promedio	8

ACTIVO	DESCRIPCION DE RIESGO	PROBABILIDAD	IMPACTO	RIESGO
Dispositivos	Acceso no autorizado o manipulación del servidor por falta de monitoreo	4	4	ALTO
Dispositivos	Robo de información por falta de autenticación en comunicaciones del servidor	4	4	ALTO
Dispositivos	Captura de contraseñas y tráfico sensible no protegido en switches	3	4	ALTO
Software y aplicaciones	Explotación de vulnerabilidades en app móvil por ser software nuevo o inmaduro	3	3	MEDIO
Software y aplicaciones	Fugas de información por falta de monitoreo y baja conciencia de seguridad en DLP	3	3	MEDIO

TRATAR EL RIESGO

ACTIVO	DESCRIPCION DE RIESGO	CONTRAMEDIDA
Dispositivos	Acceso no autorizado o manipulación del servidor por falta de monitoreo	Implementar un sistema de monitoreo centralizado (como SIEM) que registre accesos, actividades sospechosas y cambios en configuraciones del servidor en tiempo real.
Dispositivos	Robo de información por falta de autenticación en comunicaciones del servidor	Aplicar mecanismos de autenticación mutua mediante certificados digitales o protocolos seguros como TLS para asegurar la identidad del emisor y receptor.
Dispositivos	Captura de contraseñas y tráfico sensible no protegido en switches	Configurar cifrado de datos en tránsito (SSH), segmentar la red y deshabilitar protocolos inseguros que transmitan datos en texto claro.
Software y aplicaciones	Explotación de vulnerabilidades en app móvil por ser software nuevo o inmaduro	Realizar pruebas de seguridad antes del despliegue y establecer un ciclo de actualizaciones frecuentes para corregir errores.
Software y aplicaciones	Fugas de información por falta de monitoreo y baja conciencia de seguridad en DLP	Mantener sigue el servicio del software DPL