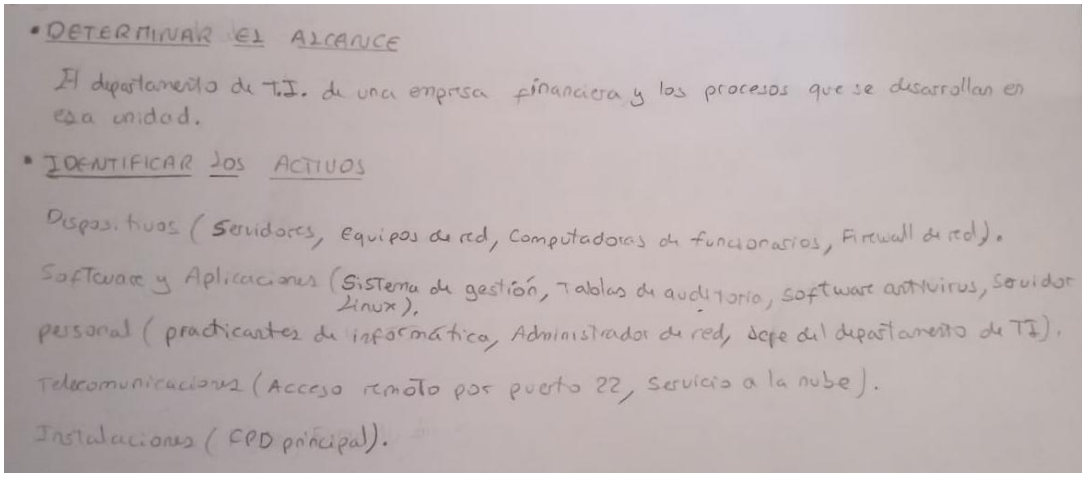
El Dpto de T.I. de una empresa financiera, tiene más de 15 años en el mercado y como parte de la información recopilada de un estudio, se identificaron los siguientes puntos:

1. Se desarrollo un nuevo sistema de gestión que será utilizado en la institución, el cual tiene todas las medidas de seguridad correctas en criptografía, controles de accesos, tiempo de sesiones, bitácoras o tablas de auditoría.
2. Se cuenta con un equipamiento de última generación a nivel de servidores, unidades de almacenamiento y equipos de redes que están operando por 1 año.
3. Debido al volumen de información generada diariamente y para extender el espacio de almacenamiento, se decide deshabilitar las tablas de auditoria del sistema.
4. Se realizan back ups con un esquema de 10 copias, mismas que son almacenadas a mas de 25 Km del CPD principal.
5. Cómo parte de un convenio interinstitucional, se reciben semestralmente 3 practicantes de Informática, los cuales pueden llevar sus laptops y acceder a la red a partir de ellas para realizar las actividades que les soliciten.
6. Existe un firewall de red, donde se habilita el puerto 22 para el acceso remoto, habilitado únicamente para el responsable de redes y Jefe de T.I. de la institución en caso de necesitar acceder los servidores.
7. Recientemente finalizó la licencia de antivirus de pago que se contrataba anualmente, y considerando que es una inversión elevada, se opta por utilizar la versión gratuita, ya que no existen información importante almacenada en las computadoras que usan los funcionarios, toda información importante está en el servidor que usa una distribución Linux.
8. Debido a la necesidad de garantizar el 24/7, se cancela por el servicio en la nube para tener el equipamiento virtualizado mínimo en caso de que el CDP sufra algún desastre.

Identificar los elementos que deban ser analizados siguiendo la metodología de 6 pasos.



- DETERMINAR EL ALCANCE

El departamento de T.I. de una empresa financiera y los procesos que se desarrollan en esa unidad.

- IDENTIFICAR LOS ACTIVOS

Dispositivos (Servidores, Equipos de red, Computadoras de funcionarios, Firewall de red).

Software y Aplicaciones (Sistema de gestión, Tablas de auditoría, software antivirus, Servidor Linux).

personal (practicantes de informática, Administrador de red, Jefe del departamento de TI).

Telecomunicaciones (Acceso remoto por puerto 22, Servicio a la nube).

Instalaciones (CPD principal).

- VALORACION DE ACTIVOS.

ACTIVO	VALORACIÓN	D+I+C = # /3 = Total	IMPORTANCIA
Dispositivos	Servidores	5+5+5 = 15/3 = 5	MUY ALTO
	Equipos de red	4+4+5 = 13/3 = 4	ALTO
	Comp. de Funcionarios	3+4+5 = 12/3 = 4	ALTO
	Firewall de Red.	4+4+5 = 13/3 = 4	ALTO
Software y Aplicaciones	Sis. de gestión	4+4+4 = 16/3 = 5	MUY ALTO
	Tablas de Auditoria	4+4+4 = 16/3 = 5	MUY ALTO
	Software antivirus	5+4+4 = 13/3 = 4	ALTO
	Servidor Linux	5+5+5 = 15/3 = 5	MUY ALTO
Personal	Practicantes de informática	2+3+3 = 8/3 = 3	MEDIO
	Adm. de Red	4+4+4 = 16/3 = 5	MUY ALTO
	Jefe. de Dpt. de TI.	5+4+5 = 14/3 = 5	MUY ALTO
Telecomunicaciones	Acceso remoto P: ??	4+4+5 = 13/3 = 4	ALTO
	Servicio a la nube	3+4+5 = 12/3 = 4	ALTO
Instalaciones	CPD principal	4+4+5 = 13/3 = 4	ALTO

- IDENTIFICAR LAS AMENAZAS

Dispositivos

- Recientemente finalizó la licencia de antivirus de pago que se contrataba anualmente y considerando que es una inversión elevada, se opta por utilizar la versión gratuita, ya que no existen información importante almacenada en las computadoras que usan los funcionarios, toda información importante esta en el servidor que usa una distribución linux. (AMENAZA : Ataques Intencionados) → Acceso no Autorizado (I,C), Uso no previsto (D, I, C), Personal no Autorizado podría infectar las PCs de los funcionarios con algun tipo de Malware y así manipular o sacar información que le interese al Atacante.

Software y Aplicaciones.

- Debido al volumen de Información generada diariamente y para extender el espacio de almacenamiento, se decide deshabilitar las tablas de auditoria del sistema. (AMENAZA: Errores y Fallos no intencionados) → Deficiencias en la organización (D), Escape de Información (I, C), Fugas de Información (C), Sin las las tablas de auditoria la información de la institución corre peligro de ser alterada. Así mismo, no se tendría la información exacta de los activos de Información que tiene la institución.

Personal

- Como parte de un convenio internacional, se reciben semestralmente 3 practicantes de informática, las cuales pueden llevar sus laptops y acceder a la red a partir de ellas para realizar las actividades que lo soliciten. (AMENAZA : Errores y Fallos no intencionados) → Difusión de software dañino (D, I, C), (AMENAZA : Ataques intencionados) → Abuso de privilegios de acceso (D, I, C), Uso no previsto (D, I, C), Acceso no autorizado (I, C), Por las políticas de la institución no es permitido realizar trabajos o Actividades de un equipo, como este caso de una laptop personal ya que podría estar infectado por algun Malware o podría ser una entrada para el atacante.

- IDENTIFICAR VULNERABILIDAD

Dispositivos

- Recientemente finalizó la licencia de antivirus de pago que se contrataba anualmente y considerando que es una inversión elevada, se opta por utilizar la versión gratuita ya que no existen información importante almacenada en las computadoras que usan los funcionarios, Toda información importante esta en el servidor que usa una distribución linux. → Almacenamiento sin protección. Personal no Autorizado podría infectar las PCs de los funcionarios con algun tipo de Malware y así manipular o sacar información que le interese al Atacante.

Software y aplicaciones

- Debido al volumen de información generada diariamente y para extender el espacio de almacenamiento, se decide deshabilitar las Tablas de auditoria del sistema. → Ausencia de pistas de auditoría, Habilitación de servicios innecesarios. Sin las tablas de Auditoria la información de la institución corre peligro de ser alterada. Asi mismo, no se Tendria la información exacta de los activos de información que tiene la institución.

Personal.

- Como parte de un convenio internacional, se reciben semestralmente 3 practicantes de informática, los cuales pueden llevar sus laptops y acceder a la red a partir de ellas para realizar las actividades que los soliciten. → Ausencia de políticas para el uso de los medios de telecomunicaciones y mensajería, Entrenamiento insuficiente en seguridad. Por las políticas de la institución no es permitido realizar trabajos o actividades con un equipo externo, como en este caso de una laptop personal ya que podria estar infectado por algun Malware o podria ser una entrada para el atacante.

• EVALUAR EL RIESGO

Activo: Dispositivos

Nº	Descripción del riesgo	Probabilidad	Impacto Financiero	Imagen	Operativo	Total	Riesgo
	Posibles Accesos no Autorizados y infecciones de algún Malware	4	4	4	5	4	17,332
							17,332

Riesgo promedio

Impacto = 4+4+5 = 13/3 = 4,333 → Riesgo = 4 * 4,333 = 17,332.

Activo: Software y aplicaciones

Nº	Descripción del riesgo	Probabilidad	Impacto Financiero	Imagen	Operativo	Total	Riesgo
	Riesgo de pérdidas de información, por falta de una Tabla de Auditoria	4	4	3	5	4	16
							16

Riesgo Promedio

Impacto = 4+3+5 = 12/3 = 4 → Riesgo = 4 * 4 = 16

Activo: Personal

Nº	Descripción del riesgo	Probabilidad	Impacto Financiero	Imagen	Operativo	Total	Riesgo
	Incumplimiento de Políticas de la institución, corre peligro de ser vulnuado el sistema.	4	5	4	5		18,664
							18,664

Riesgo Promedio

Impacto = 5+4+5 = 14/3 = 4,666 → Riesgo = 4 * 4,666 = 18,664

• MATRIZ DE RIESGO

IMPACTO						
	MUY ALTO (5)	MEDIO	MEDIO	ALTO	2	MUY ALTO
	ALTO (4)	BAJO	MEDIO	1	3	MUY ALTO
	MEDIO (3)	MUY ALTO	BAJO	MEDIO	4	ALTO
	BAJO (2)	MUY ALTO	BAJO	BAJO	MEDIO	MEDIO
	MUY BAJO (1)	MUY ALTO	MUY ALTO	MUY ALTO	BAJO	MEDIO
		MUY BAJO (1)	BAJO (2)	MEDIO (3)	ALTO (4)	MUY ALTO (5)
		PROBABILIDAD				

- TRATAR EL RIESGO

Activo	Riesgo Identificado	Contramedida
Dispositivos	Posibles intentos de vulnerar las computadoras de los funcionarios	Instalar antivirus para detectar intrusos
Software Aplicaciones.	Perdida de informaciones importantes de la institución	habilitar las tablas de auditoria para mayor control y obtener información
Personal	Falta de cumplimiento de las políticas de la institución	establecer políticas en la institución para mayor desarrollo.