


<u>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”</u> <u>CARRERA DE INGENIERÍA DE SISTEMAS</u>			
Nombre	Univ. Luis Daniel Acuña Oyola		
Materia:	Seguridad de Sistemas (SIS-737)		
Docente:	M.Sc. Ing. Javier Alexander Durán Miranda		N° Práctica
Auxiliar:	Univ. Aldrin Roger Perez Miranda		2
Fecha publicación:	06/10/2025		
Fecha de entrega:	20/10/2025		
Grupo:	1	Sede:	Potosí

1. Alcance

Departamento de (T.I.).

2. Identificar Activos

Software y Aplicaciones: (Nuevo sistema de gestión, licencia de antivirus, firewall de red).

Dispositivos: (Servidores, unidades de almacenamiento, equipos de redes, laptops).

Personal: (Practicantes, responsable de redes, jefe de T.I.).

Telecomunicaciones: (Acceso remoto).

Instalaciones: (Departamento de T.I.).

Valorar Activos

ACTIVO	VALORACION				IMPORTANCIA
SOFTWARE Y APLICACIONES	D	I	C	TOTAL	
Sistema de gestión	4	4	4	4	ALTA
Antivirus	5	5	5	5	MUY ALTA
DISPOSITIVOS	D	I	C	TOTAL	
Servidores	5	4	5	4.667 -> 5	AMUY ALTA
Unidad de almacenamiento	4	5	4	4.33 -> 4	ALTA
Equipos de red	5	4	3	4	ALTA
Laptops	1	1	5	2.33 -> 2	BAJA
PERSONAL	D	I	C	TOTAL	
Practicantes	2	1	5	2.667 -> 3	MEDIA
Responsable de redes	3	2	5	3.33 -> 3	MEDIA
Jefe de T.I.	3	2	5	3.33 -> 3	MEDIA
TELECOMUNICACIONES	D	I	C	TOTAL	
Acceso remoto	3	4	5	4	ALTA
INSTALACIONES	D	I	C	TOTAL	
Edificio departamento de T.I.	4	4	1	3	MEDIA

3. Identificar Amenazas

ACTIVO: SOFTWARE Y APLICACIONES
<ul style="list-style-type: none">Debido al volumen de información generada diariamente y para extender el espacio de almacenamiento, se decide deshabilitar las tablas de auditoría del sistema (AMENAZA: ATAQUES INTENCIONADOS) -> Manipulación de los registros de actividad (I), Al hacerlo, el sistema pierde la capacidad de garantizar el no repudio, lo que implica que ya no es posible verificar con certeza la veracidad e integridad de la información registrada.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. (ERRORES Y FALLOS NO INTENCIONADOS) -> Difusión de software dañino (I, D, C), Destrucción de información (D), No obstante, al emplear un antivirus menos robusto, los equipos quedan más expuestos a software malicioso y otras amenazas que podrían propagarse a través de la red, poniendo en riesgo incluso el servidor que contiene la información crítica.
ACTIVO: PERSONAL
<ul style="list-style-type: none">Como parte de un convenio interinstitucional, se reciben semestralmente tres 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. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> Fugas de información (I, C), Sin embargo, al permitir el acceso desde equipos personales, se incrementa el riesgo de que información sensible sea filtrada o copiada de manera involuntaria, lo que podría comprometer la confidencialidad de los datos de la institución.

4. Identificar Vulnerabilidades

ACTIVO: SOFTWARE Y APLICACIONES
<p>Debido al volumen de información generada diariamente y para extender el espacio de almacenamiento, se decide deshabilitar las tablas de auditoría del sistema -> AUSENCIA DE PISTAS DE AUDITORÍA, la ausencia de tablas de auditoria permitirá realizar cambios, sin dejar registro, lo que seria muy ineficiente en caso de ocurrir algo grande.</p> <p>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. -> AUSENCIA DE CONTROL DE CAMBIOS, DEFECTOS BIEN CONOCIDOS DE SOFTWARE, el hecho de no contar con un antivirus con funciones y seguridad avanzada hace vulnerable no solo a un dispositivo, sino a toda la red que queda expuesta a softwares dañinos.</p>
ACTIVO: PERSONAL
<p>Como parte de un convenio interinstitucional, se reciben semestralmente tres 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. -> TRABAJO NO SUPERVISADO DE PERSONAL EXTERNO, Los practicantes externos acceden a la red sin una supervisión completa, lo que incrementa la posibilidad de fugas accidentales de información o de errores que afecten la red.</p>

5. Evaluar Riesgos

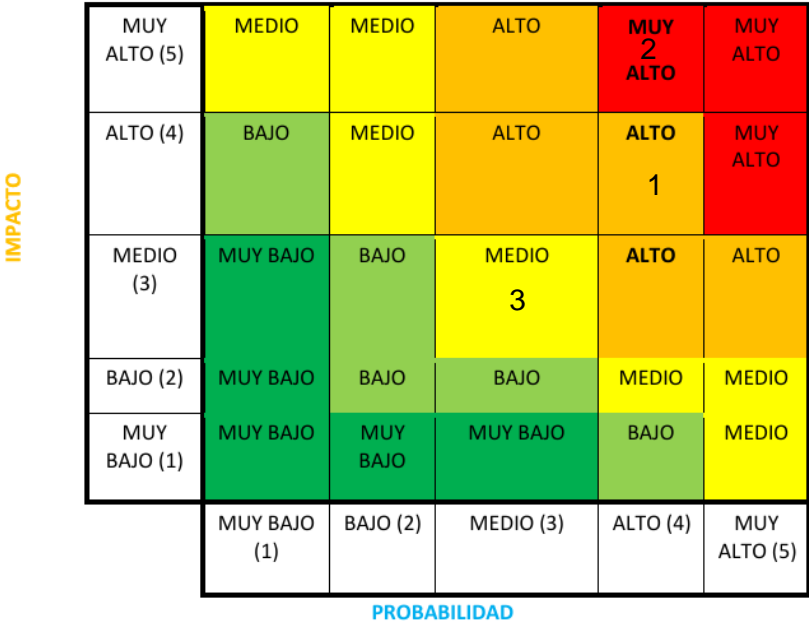
ACTIVO: SOFTWARE Y APLICACIONES							
N°	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
1	Tablas de auditoría deshabilitadas, riesgo de pérdida de integridad.	4	4	5	3	4	12
2	Antivirus menos robusto, posible propagación de malware al servidor y demás equipos.	4	5	4	5	5	18.667
RIESGO PROMEDIO							15.3335

ACTIVO: PERSONAL							
N°	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
1	Fuga de información por laptops personales de practicantes conectadas a la red.	3	3	4	3	3	10
RIESGO PROMEDIO							10

Resumen de probabilidad/riesgo

DESCRIPCIÓN		PROBABILIDAD	IMPACTO	ACTIVO
1	Tablas de auditoría deshabilitadas, riesgo de pérdida de integridad.	4	4	Software y Aplicaciones
2	Antivirus menos robusto, posible propagación de malware al servidor y demás equipos.	4	5	Software y Aplicaciones
3	Fuga de información por laptops personales de practicantes conectadas a la red.	3	3	Personal

Matriz de Riesgos



6. Tratar Riesgo

ACTIVO	RIESGO	CONTRAMEDIDAS
Software y Aplicaciones	Tablas de auditoría deshabilitadas, riesgo de pérdida de integridad.	Habilitar los logs con rotación automática o ampliar el almacenamiento para conservar el registro completo sin comprometer la integridad de la información.
Software y Aplicaciones	Antivirus menos robusto, posible propagación de malware al servidor y demás equipos.	Mantener el antivirus siempre actualizado y segmentar la red, de modo que, en caso de infección, el servidor no se vea afectado.
Personal	Fuga de información por laptops personales de practicantes conectadas a la red.	Limitar su acceso a una VLAN o VPN separada y supervisada, evitando que los dispositivos externos comprometan la red interna.