

	<b>UNIVERSIDAD AUTÓNOMA “TOMÁS FRÍAS”</b> <b>INGENIERÍA DE SISTEMAS</b>			
	<b>Estudiante:</b>	Univ.Cristian Sixto Sunagua Gira		
	<b>Docente:</b>	M.Sc.Ing.J. Alexander Durán.M	<b>Materia:</b>	SIS-737
	<b>Auxiliar:</b>	Univ. Aldrin Roger Perez Miranda	<b>Fecha:</b>	20/04/2025
<b>Enlace:</b>		<b>C.I:</b>	8600448	<b>MICROTALLER 2</b>

## DETERMINAR EL ALCANCE

Departamento Financiera Oportunidad

## IDENTIFICAR Y VALORAR ACTIVOS

DISPOSITIVOS: Computadoras

SOFTWARE Y APP: Antivirus, Antimalware

PERSONAL: Funcionarios

INSTALACIONES: Edificio Central

## IDENTIFICAR Y VALORAR ACTIVOS

DISPOSITIVOS:	Disp.	Integ.	Confi.		Importancia
Computadoras	5	+ 4	+4	$= 13/3 = 4$	alto
SOFTWARE Y APP:					
Antivirus	4	+ 5	+ 5	$= 14/3 = 5$	muy alto
Antimalware	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

## IDENTIFICAR LAS AMENAZAS

DISPOSITIVOS: **Computadoras:**

Errores y fallos no intencionados: errores de administrador

Libertad a los funcionarios de instalar cualquier software

SOFTWARE Y APP: Antivirus y Malware:

Errores y fallos no intencionados: vulnerabilidades de los programas

Protección inadecuada contra amenazas avanzadas (por ser gratuitos)

PERSONAL: funcionarios:

Errores no intencionados: manipulación de programas desconocidos

Falta de capacitación a los funcionarios

## IDENTIFICACION DE VULNERABILIDADES Y SALVAGUARDAS

DISPOSITIVOS: **Computadoras:**

Equipamiento Informático: ausencia de un eficiente control de cambios en la configuración

Falta de restricciones en los permisos de los funcionarios que llegaría a dañar los equipos

SOFTWARE Y APP: **Antivirus y Antimalware**

Software – Aplicaciones Informáticas: Defectos bien conocidos del software:

El software que instalamos como ser gratis no es bien efectivo: Salvaguardas—considerando el taller tenemos algo que reduzca el impacto del ransomware o otros virus.

FUNCONARIOS: **Personal: Falta de conciencia acerca de la seguridad**

Al tener poco conocimiento de seguridad necesitan una capacitación mas adecuada.

## EVALUAR RIESGO

### ACTIVO: DISPOSITIVOS

N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
01	Computadoras sin restricciones de instalación de software	4	3	4	5	4	16
Riesgo Promedio							16
N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
02	Cambios de contraseñas con cambios después de 3 meses	2	2	2	4	3	5.33
Riesgo Promedio							5.33

### ACTIVO: SOFTWARE Y APLICACIONES

N°	DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO				RIESGO
			FINANCIERO	IMAGEN	OPERATIVO	TOTAL	
01	Software no ejecutivo que puede llegar a tener fallas y vulnerabilidades	2	4	4	3	4	7.33
Riesgo Promedio							7.33

**Salvaguarda---** Probabilidad reducida de 4 a 2 por salvaguarda considerando que se instaló con anticipación para prevenir los ataques de ransomware

ACTIVO	DESCRIPCION DE RIESGO	PROBABILIDAD	IMPACTO	RIESGO
Dispositivos	Computadoras sin restricciones de instalación de software	4	4	ALTO
Dispositivos	Cambios de contraseñas con cambios después de 3 meses	2	3	MEDIO
Software y aplicaciones	Software no ejecutivo que puede llegar a tener fallas y vulnerabilidades	2	4	MEDIO

## TRATAR EL RIESGO

ACTIVO	DESCRIPCION DE RIESGO	CONTRAMEDIDA
Dispositivos	Computadoras sin restricciones de instalación de software	Realizar una política de de control de software en las computadoras.
Dispositivos	Cambios de contraseñas con cambios después de 3 meses	Realizar los cambios cada mes para tener mas seguridad en las computadoras
Software y aplicaciones	Software no ejecutivo que puede llegar a tener fallas y vulnerabilidades	Realizar un contrato con alguna empresa para tener un antivirus, antimalware ejecutivo que tiene mayor protección ante amenazas