

PRACTICA_02_SEGURIDAD DE SISTEMAS

Nombre: Jacob Santos Ayaviri Condori

C.I. 13229452



Git hub

Name: Ayaviri_Condori_Jacob_Santos

Link: https://github.com/jacob-santos-0/Practica_01_seguridad_1_2025.git

The screenshot shows the GitHub interface for the repository 'Practica_01_seguridad_1_2025'. The repository is public and has 1 branch (master) and 0 tags. The owner is 'jacob-santos-0' with a commit hash of '94457f5' made 2 weeks ago. A single commit with 3 commits is shown, containing a file named 'ayaviri_Condori_Jacob_Santos.pdf'. The README section is currently empty, displaying a message to 'Add a README' to help people understand the project.

PRÁCTICA # 2

Nombre: Jacob Santos Ayaviri Condori RU: 109417 CI: 13229452

Docente: Ing. Duran Miranda Javier Alexander

1

DETERMINAR EL ALCANCE

El departamento de T.I. y sus procesos de identificación

IDENTIFICAR LOS ACTIVOS

Dispositivos (servidores, equipos de redes, unidades de almacenamiento, laptops)

Software y Aplicaciones (sistema de gestión de seguridad, Antivirus software de auditoría)

Personal (3 practicantes, responsable de redes, jefe T.I.)

Telecomunicaciones (firewall)

Instalaciones (CPU principal, CPD de respaldo)

VALORACION DE ACTIVOS

ACTIVO	VALORACION	IMPORTANCIA
DISPOSITIVOS	Servidores ($D=5 \ I=5 \ C=4$) $\Rightarrow 14/3 \Rightarrow 4.66 \Rightarrow 5$	muy alta
	equipos de redes ($D=5 \ I=4 \ C=4$) $\Rightarrow 13/3 \Rightarrow 4.33 \Rightarrow 4$	alta
	unidades de almacenamiento ($D=3 \ I=3 \ C=3$) $\Rightarrow 9/3 \Rightarrow 3$	media
	laptops ($D=1 \ I=3 \ C=2$) $\Rightarrow 6/3 \Rightarrow 2$	baja
SOFTWARE Y APLICACIONES	sistema de gestión de seguridad ($D=5 \ I=4 \ C=4$) $\Rightarrow 13/3 \Rightarrow 4.33 \Rightarrow 4$	alta
	Antivirus ($D=3 \ I=3 \ C=2$) $\Rightarrow 8/3 \Rightarrow 2.66 \Rightarrow 3$	media
	software de auditoría ($D=4 \ I=4 \ C=3$) $\Rightarrow 11/3 \Rightarrow 3.66 \Rightarrow 4$	alta

PERSONAL	3 auditores (D=1 I=2 C=1) $\Rightarrow 4/3 \Rightarrow 1.33 \Rightarrow 1$	muy bajo
	responsable de redes (D=2 I=3 C=1) $\Rightarrow 6/3 \Rightarrow 2$	bajo
	jefe T.I. (D=3 I=4 C=1) $\Rightarrow 8/3 \Rightarrow 2.66 \Rightarrow 3$	medio
TELECOMUNICACIONES	firewall (D=4 I=4 C=4) $\Rightarrow 12/3 \Rightarrow 4$	alto
INSTALACIONES	CPD principal (D=4 I=3 C=2) $\Rightarrow 9/3 \Rightarrow 3$	medio
	CPD de respaldo (D=2 I=2 C=2) $\Rightarrow 6/3 \Rightarrow 2$	bajo

IDENTIFICACION DE AMENAZAS

SOFTWARE Y APLICACIONES

- 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) \Rightarrow modificación deliberada de la información (I) / divulgación de información (C), el hecho de deshabilitar las tablas de auditoría da al acceso de que el personal de la empresa o cualquiera que trabaje en la empresa pueda modificar la información sin tener pruebas de quien hizo la modificación, también pueden divulgar la información, haciendo que la empresa pierda confiabilidad.
- Recientemente finalizó la licencia de antivirus de pago, que se contrataba anualmente, y considerando que es una versión elevada se opta, por utilizar la versión gratuita, ya que no existe información importante almacenada en las computadoras que usan los funcionarios toda información importante está en el servidor que usa una distribución Linux (AMENAZA: Errores y fallos no intencionados) \Rightarrow destrucción de información (D) / escape de información (I, C), al no contar con un buen antivirus, puede llegar a que entre malware a las computadoras, causando la destrucción de información y escapes de información, y al conectarse con el servidor puede causar problemas al servidor.

DISPOSITIVOS

- * Como 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 actividades que se les solicite (**AMENAZA Ataques intencionados**) \Rightarrow abuso de privilegios de acceso (D, I, C) / difusión de software dañino (D, I, C) \Rightarrow Al conectar sus laptops directamente con la red puede causar la difusión de software dañino y problemas en la red, al poder conectarse directamente con la red tiene privilegios de acceso que puede causar muchos problemas en la red.
- IDENTIFICAR VULNERABILIDADES

SOFTWARE Y APLICACIONES

- Debido al volumen de información generado diariamente y para extender el espacio de almacenamiento se decide desactivar los tablos de auditoría del sistema **AUSENCIA DE PISTAS DE AUDITORIA**, debido a la falta de tablos de auditoría podría cualquier persona al de la empresa borrar db, etc, copiar información y modificar la base de datos.
- Recientemente finalizó la licencia del antivirus de pago que se controlaba manualmente y considerando que es una inversión elevada se opta por utilizar la versión gratuita, ya que no existe información importante almacenada en las computadoras que usen los funcionarios, toda información importante está en el servidor que usa una distribución Linux. **AUSENCIA DE CONTROL DE CAMBIO ERIC42**, debido a la ausencia del control de antivirus puede que entre virus informático, troyanos y ransomware a las laptops, causando que las laptops almacene mucho virus informático, y al conectarse con el servidor o red, estoy exponiendo al servidor o red causando que al servidor o red tengan problemas.

DISPOSITIVOS

- Como 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 se les solicite **COPIA NO CONTROLADA**, al tener tanta libertad hasta de conectar sus laptops pueden copiar archivos no autorizados, y hacer modificaciones no autorizadas, también al conectarse puede que tengan software dañino que cause la caída de la red y infecte a los demás dispositivos causando muchos problemas a la empresa

EVALUACION DE RIESGO

Activo: Software y Aplicaciones

No	Descripción de Riesgo	Probabilidad	Impacto				Riesgo
			F	I	O	Total	
1	Ausencia de tablas de auditoría en el sistema	5	5	5	3	4	21.66
2	Ausencia de Antivirus y control sobre las computadoras	4	4	4	2	3	13.33
Riesgo Promedio							15.333

Activo: Dispositivos

No	Descripción de Riesgo	Probabilidad	Impacto				Riesgo
			F	I	O	Total	
1	Vulneración a la red y falta de control	4	4	4	5	4	17.33

TABLA RESUMEN

No	Descripción	Probabilidad	Impacto	Activo
1	Ausencia de tablas de auditoría en el sistema	5	4	Software y Aplicaciones
2	Vulneración a la red y falta de control	4	4	Software y Aplicaciones
3	Ausencia de Antivirus y control sobre las Computadoras	4	3	Dispositivo

MATRIS DE RIESGO

Muy Alto	medio	medio	alto	muy alto	muy alto
Alto	bajo	medio	alto	2	1
medio	muy bajo	bajo	medio	3	alto
Bajo	muy bajo	bajo	bajo	medio	medio
muy bajo	muy bajo	muy bajo	muy bajo	bajo	medio
	muy bajo	bajo	medio	alto	muy alto

TRATAR EL RIESGO

Activo	Riesgo Identificado	Contramedida
Software y Aplicaciones	Ausencia de tablas de auditoría en el sistema	Implementar nuevamente las tablas de auditoría en el sistema y hacer pruebas de auditoría
Software y Aplicaciones	Vulneración a la red y falta de control	Negar el acceso directo a la red con dispositivos que no sean de la empresa
Dispositivos	Ausencia de antivirus y control sobre las computadoras	Renovar el antivirus a las computadoras de los funcionarios

EJERCICIO Nº 2

DETERMINAR EL ALCANCE

Institucion financiera "Oportunidad" y sus procesos

IDENTIFICAR LOS ACTIVOS

Dispositivos (Computadoras)

Software y Aplicaciones (Antivirus Gratuito)

Personal (funcionarios)

VALORACION DE LOS ACTIVOS

Activo	Valoración	Importancia
Dispositivos	Computadoras ($D=5, I=4, C=4$) $\Rightarrow 13/3 \Rightarrow 4.3 \Rightarrow 4$	alto
Software y aplicaciones	antivirus Gratuito ($D=3, I=2, C=2$) $\Rightarrow 7/3 \Rightarrow 2.3 \Rightarrow 2$	bajo
Personal	Funcionarios ($D=2, I=2, C=2$) $\Rightarrow 6/3 \Rightarrow 2 \Rightarrow 2$	bajo

IDENTIFICACION DE RIESGO

DISPOSITIVOS

Las computadoras utilizados por los funcionarios les permiten instalar cualquier tipo de software (**AMENAZA: Errores y fallos no intencionados**) \Rightarrow Difusion de software dañino (D, I, C) / destruccion de informacion (D). Al poder instalar cualquier tipo de programa puede aver diffusion de software dañino, destruccion de informacion y violacion de politicas.

SOFTWARE Y APLICACIONES

Como respuesta a los ataques de ransomware, los cuales se estan masificando en varias organizaciones similares, se produce a instalar antivirus y antimalware gratuitos en cada computo-

dora (AMENAZA Errores y fallos no intencionados) => difusión de software dañino (D, I, C) / fugas de información (C) / actualizaciones de programas (software) (I, C). Al tener un antivirus gratuito se tiene una protección insuficiente ante infección por ransomware cifrado de datos, pérdida de información institucional

IDENTIFICAR VULNERABILIDADES

DISPOSITIVOS

Las computadoras utilizadas por los funcionarios les permiten instalar cualquier tipo de software. Almacenamiento sin protección, al poder instalar facilita la introducción de malware o programas piratas que hacen que las computadoras terminen dañadas y la información quede expuesta.

SOFTWARE Y APLICACIONES

Como respuesta a los ataques ransomware, los cuales se están masificando en varias organizaciones similares, se procede a instalar antivirus y antimalware gratuitos en cada computadora => defectos bien conocidos de software, si se usa antivirus gratuitos incrementa la posibilidad de tener malware en todas las equipos de la institución, haciendo que se pierda, robe, modifique mucha documentación importante.

EVALUACION DE RIESGO

Activos Dispositivo							
No	Descripción de Riesgo	Probabilidad	Impacto			Riesgo	
			F	I	C		
1	Ausencia de políticas de restricción a la instalación de softwares	5	4	4	5	4	21.66

Activo: Software y Aplicaciones

No	Descripción de Riesgo	Probabilidad	Impacto				Riesgo
			F	I	O	total	
1	Ausencia de un buen Antivirus para las computadoras	4	4	3	3	4	16

TABLA RESUMEN

No	Descripción	Probabilidad	Impacto	Activo
1	Ausencia de políticas de restricción a la instalación de software	5	4	Dispositivo
2	Ausencia de un buen antivirus para las computadoras	4	4	Software y Aplicaciones

MATRIZ DE RIESGO

muy alto	medio	medio	alto	M alto	M alto
alto	bajo	medio	alto	2	1
medio	M bajo	bajo	medio	alto	alto
bajo	M bajo	bajo	bajo	medio	medio
muy bajo	M bajo	M bajo	M bajo	bajo	bajo
	muy bajo	bajo	medio	alto	muy alto

TRATAR EL RIESGO

Activo	Riesgo identificado	Control medida
Dispositivo	Ausencia de políticas de restricción a la instalación de software	Implementar políticas de restricción a software no autorizados y control de privilegios
software y aplicaciones	Ausencia de un buen anti-virus para las computadoras	Implementar un Antivirus de licencia empresarial y copias de seguridad