	UNIVERSIDAD AUTÓNOMA "TOMÁS FRÍAS" **CARRERA DE INGENIERÍA DE SISTEMAS**
MATERIA: Seguridad de Sistemas (SIS - 737)	
NOMBRE: Univ. Dietmar Alex Apaza **DOCENTE: Ing.** Alexander J. Duran Miranda **AUXILIAR: Univ.** Aldrin Roger Perez Miranda **GitHub** **Nombre: AlexTheLion99** **Enlace_lab_4:** https://github.com/AlexTheLion99/Microtaller_analisis_de_riesgos_2	**Microtaller_analisis_de_riesgos_2**

CASO 1-SEGURIDAD DE SISTEMAS

Institución: Financiera Oportunidad

ENUNCIADO

- Producto del análisis realizado a la financiera Oportunidad, se identificaron los siguientes puntos:
- Las computadoras utilizadas por los funcionarios les permiten instalar cualquier tipo de software
- Los cambios de contraseña se realizan cada 90 días, utilizando contraseñas fuertes de al menos 8 caracteres.
- Cómo respuesta a los ataques de ransomware, los cuales se están masificando en varias organizaciones similares, se procede a instalar antivirus y antimalware gratuitos en cada computadora.

Toda operación realizada en los sistemas, queda registrada, desde el usuario, Ip, hora, y las acciones que realizó en dicho sistema, en tablas de auditoría o bitácoras.

TAREAS

1.- Seleccionando únicamente los puntos donde se pueda suscitar un incidente, identifique las amenazas, vulnerabilidades para poder realizar un análisis de riesgos siguiendo un enfoque metódico. (Utilice los 6 pasos aprendidos en clase)

1. DETERMINAR EL ALCANCE

Los riesgos asociados a los equipos, contraseñas, antivirus y bitácoras utilizados por los funcionarios de la Financiera Oportunidad. Se excluyen redes externas y sistemas ajenos.

2. IDENTIFICAR Y VALORAR LOS ACTIVOS

Se identifican los activos de información y tecnológicos que podrían verse afectados.

Nº	Activo	Valor	Justificación
1	Computadoras de funcionarios	Alto	Son esenciales para el trabajo diario.
2	Información institucional (datos, registros)	Muy Altas	Pérdida o corrupción podría paralizar la operación.
3	Contraseñas de acceso	Alto	Son la principal barrera de seguridad.
4	Bitácoras de auditoría	Alto	Permiten rastrear actividades y detectar incidentes.
5	Software antivirus gratuito	Medio	Protege, pero con limitaciones.

Valoración de los activos

ACTIVO	DISPONIBILIDAD (D)	INTEGRIDAD (I)	CONFIDENCIALIDAD (C)	SUMA	PROMEDIO	IMPORTANCIA
Computadoras de funcionarios	5	4	3	12	4.0	ALTA
Contraseñas de acceso	3	5	5	13	4.33	ALTA
Información institucional	5	5	5	15	5.0	MUY ALTA
Bitácoras de auditoría	4	4	3	11	3.66	ALTA
Antivirus gratuito instalado	3	3	2	8	2.66	MEDIA

3. IDENTIFICAR LAS AMENAZAS

Las amenazas son eventos o acciones que podrían explotar vulnerabilidades y dañar los activos.

DISPOSITIVOS

- Las computadoras permiten instalar cualquier tipo de software sin restricciones. **(AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Instalación de software malicioso o incompatible (I)**, que puede comprometer la estabilidad o seguridad de los sistemas.
- No se indica control sobre la integridad del sistema operativo o software base. **(AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Fallas por configuraciones incorrectas (D)**, al no tener control sobre las instalaciones.

SOFTWARE Y APLICACIONES

- Se permite instalación de cualquier software, sin validación. **(AMENAZA: ATAQUES INTENCIONADOS) → Instalación de ransomware o spyware (C)** que robe información confidencial.

- Uso de antivirus y antimalware gratuitos.
  (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Falsa protección (I) por software que podría estar desactualizado o no detectar amenazas reales.

CONTRASEÑAS

- El cambio de contraseñas se realiza cada 90 días, aunque sin mención de verificación adicional.
  (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Contraseñas débiles o reutilizadas (C) que podrían ser adivinadas fácilmente.
- Solo se exige un mínimo de 8 caracteres.
  (AMENAZA: ATAQUES INTENCIONADOS) → Ataques de fuerza bruta (C) si no se aplican mecanismos adicionales como bloqueo de cuenta.

AUDITORÍA Y BITÁCORAS

- Las bitácoras registran IP, usuario, hora y acciones realizadas, pero no se menciona cifrado o respaldo.
  (AMENAZA: ATAQUES INTENCIONADOS) → Modificación o eliminación de registros (I) para ocultar actividades maliciosas.
- No se especifica supervisión activa de los logs.
  (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → No detección de incidentes (D) por falta de revisión de las bitácoras.

PERSONAL

- Los funcionarios tienen privilegios administrativos para instalar software.
  (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Desconfiguración del sistema (I) o introducción de malware involuntario.
- No se menciona capacitación o políticas claras sobre seguridad informática.
  (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) → Manejo inadecuado de la información (C) por falta de conciencia de seguridad.

4. IDENTIFICAR VULNERABILIDADES Y SALVAGUARDAS

Analizamos las debilidades actuales y las medidas de protección existentes.

Activo	Vulnerabilidad Detectada	Tipo	Salvaguarda Propuesta	Tipo de Salvaguarda
Dispositivos	Los funcionarios pueden instalar cualquier software sin restricción	Técnica / Procedimental	Implementar políticas de control de software (lista blanca) y permisos restringidos	Administrativa / Técnica
	No se realiza control sobre el sistema operativo ni sobre configuraciones críticas	Técnica	Establecer una imagen estándar de sistema con configuraciones seguras y control de cambios	Técnica
Software y Aplicaciones	Uso de antivirus/antimalware gratuitos posiblemente ineficaces	Técnica	Adquirir soluciones de seguridad con licenciamiento adecuado y actualizaciones automáticas	Técnica
	No hay control sobre la procedencia o validación del software instalado	Técnica / Procedimental	Establecer una política de adquisición de software validado y firmado digitalmente	Administrativa / Técnica
Contraseñas	Requieren cambio cada 90 días, pero no se aplican controles de complejidad adicionales ni doble factor	Técnica / Procedimental	Aplicar autenticación multifactor y política de contraseña robusta (mayúsculas, minúsculas, símbolos)	Técnica / Administrativa

Bitácoras	No se especifica respaldo, cifrado o monitoreo activo	Técnica	Habilitar registros protegidos, con cifrado y respaldo automático; usar SIEM para monitoreo	Técnica
	No se verifica ni revisa la integridad de los registros	Técnica	Aplicar revisiones periódicas y alertas automáticas ante modificaciones no autorizadas	Técnica
Telecomunicaciones	No se menciona firewall, ni segmentación de red	Técnica	Implementar firewalls, IDS/IPS y segmentación de red	Técnica
	No hay protección contra intrusos externos/internos	Técnica	Aplicar políticas NAC (Network Access Control) y autenticación por dispositivo	Técnica
Personal	Los usuarios no están capacitados en buenas prácticas de seguridad	Humana / Organizacional	Programas de concientización y capacitación continua	Administrativa / Educativa
	No hay separación de funciones ni control de privilegios	Organizacional	Aplicar principio de mínimo privilegio y control de accesos basado en roles (RBAC)	Administrativa / Técnica

5. EVALUAR LOS RIESGOS

Combinamos la **probabilidad** de ocurrencia con el **impacto** sobre los activos.

RIESGO = PROBABILIDAD × IMPACTO
Impacto = Promedio entre Impacto Financiero, Imagen y Operativo

Nº	Activo	Descripción del Riesgo	Riesgo	Nivel de Prioridad
1	Dispositivos	Instalación no autorizada de software (posible malware o vulnerabilidad)	16	Muy alta
2	Dispositivos	Fallo de hardware por antigüedad (pérdida de datos o interrupciones)	11	Alto
3	Software y Aplicaciones	Antivirus gratuito no detecta malware avanzado	10	Medio
4	Software y Aplicaciones	Script borra logs automáticamente (afecta trazabilidad)	17.32	Muy alta
5	Software y Aplicaciones	Puertos abiertos (23, 445) exponen a ataques	23.3	Muy alta

6. TRATAR EL RIESGO

Se proponen medidas de mitigación o eliminación de los riesgos identificados.

Activo	Riesgo Identificado
Activo: Dispositivos	Daño de componentes por antigüedad del servidor (10 años de uso)
Activo: Software y Aplicaciones	Exposición por puertos abiertos 23 y 445 (vulnerabilidades tipo DoS y exploits)
Activo: Software y Aplicaciones	Borrado de logs automáticamente, impide identificar accesos ilegítimos
Activo: Software y Aplicaciones	Uso de SQL Server desactualizado, vulnerable a ataques como SQL Injection

Contramedidas Propuestas

Cerrar los puertos 23 y 445 si no son necesarios. Si se requiere acceso remoto, usar el puerto 22 (SSH).
Detener el script de borrado de logs o modificarlo para respaldar previamente dichos logs.
Actualizar SQL Server a una versión soportada por el fabricante o migrar a una alternativa moderna.
Realizar mantenimiento y reemplazo de componentes del servidor periódicamente.
Implementar una solución de respaldo profesional para respaldar automáticamente y de forma segura.
Capacitar al personal técnico en seguridad de red y gestión de logs, especialmente ante auditorías.