


<b><u>UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”</u></b> <b><u>CARRERA DE INGENIERÍA DE SISTEMAS</u></b>				
<b>Materia:</b>	Arquitectura de computadoras (SIS-522)			
<b>Docente:</b>	Ing. Gustavo A. Puita Choque			N° Práctica  8
<b>Auxiliar:</b>	Univ. Aldrin Roger Perez Miranda			
<b>16/06/2024</b>	<b>Fecha publicación</b>			
<b>30/06/2024</b>	<b>Fecha de entrega</b>			
<b>Grupo:</b>	1	<b>Sede</b>	Potosí	

**Estudiante:** Univ. José Felipe Mamani Azurduy

1) Realizar el análisis de riesgos del siguiente problema:

Imagina que estás encargado de la seguridad de una empresa cuya infraestructura de TI incluye varios servidores críticos ubicados en una sala de servidores.

Estos servidores están físicamente situados cerca de una pared compartida con una panadería adyacente, la cual utiliza grandes hornos industriales que generan mucho calor y vibraciones. Además, la panadería puede ocasionar problemas eléctricos debido a su alto consumo de energía, lo que podría afectar la estabilidad de los servidores.

Considera el riesgo de que las altas temperaturas y las vibraciones continuas puedan afectar la estabilidad y el rendimiento de los servidores, aumentando la probabilidad de fallos en el hardware.

A esto se suma la posibilidad de fluctuaciones en la red eléctrica que podrían provocar interrupciones en el suministro eléctrico a la sala de servidores. En términos de mantenimiento, es crucial implementar un mantenimiento preventivo regular para limpiar los servidores y evitar acumulación de polvo, además de mantener actualizado el software para evitar vulnerabilidades.

También es necesario realizar un mantenimiento correctivo para reparar componentes dañados, y un mantenimiento predictivo para anticipar y prevenir fallos antes de que ocurran.

DETERMINAR EL ALCANCE



Seguridad de la infraestructura de TI de una empresa, específicamente en los servidores críticos.

## IDENTIFICAR LOS ACTIVOS



Se clasifican en los siguientes grupos:

Software y Aplicaciones: (Sistema de Gestión Empresarial, Herramientas de Monitoreo)

Dispositivos: (Servidores Críticos)

Personal: (Equipo de TI)

Telecomunicaciones: (Conexiones de Red)

Instalaciones: (Sala de Servidores, Sistemas de Energía)

## VALORAR LOS ACTIVOS

ACTIVO	FÓRMULA Y RESULTADO	IMPORTANCIA
<b>SOFTWARE Y APLICACIONES</b>	Control de Inventarios ( $D=4+1=5$ , $C=4 \Rightarrow 9/2 = 4.5 \rightarrow 5$ ) Sistema de Reservas ( $D=3+1=4$ , $C=3 \Rightarrow 7/2 = 3.5 \rightarrow 4$ )	<b>MUY ALTO</b> <b>ALTO</b>
<b>DISPOSITIVOS</b>	Servidor ( $D=4+1=5$ , $C=4 \Rightarrow 9/2 = 4.5 \rightarrow 5$ )	<b>ALTO</b>
<b>PERSONAL</b>	Equipo de Desarrollo ( $D=5+1=6$ , $C=3 \Rightarrow 9/2 = 4.5 \rightarrow 5$ )	<b>MUY ALTO</b>
<b>TELECOMUNICACIONES</b>	Red de Fibra Óptica ( $D=3+1=4$ , $C=5 \Rightarrow 8/2 = 4 \rightarrow 4$ )	<b>MEDIO</b>
<b>INSTALACIONES</b>	Centro de Operaciones ( $D=4+1=5$ , $C=4 \Rightarrow 9/2 = 4.5 \rightarrow 5$ ) Sistema de Climatización ( $D=2+1=3$ , $C=4 \Rightarrow 7/2 = 3.5 \rightarrow 4$ )	<b>ALTO</b> <b>MEDIO</b>

## VALORAR LOS ACTIVOS

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Control de Inventarios	Gestión de inventarios para operaciones empresariales.	Jefe del Dep. de IT	Software	Datacenter	Muy Alto
ID_02	Sistema de Reservas	Gestión de reservas de servicios.	Jefe del Dep. de Reservas	Software	Datacenter	Alto
ID_03	Servidor	Servidor principal para el almacenamiento y	Jefe del Dep. de IT	Hardware - Servidor	Sala de Servidores	Alto

		procesamiento de datos.				
ID_04	Red de Fibra Óptica	Infraestructura de red de alta velocidad para conectividad.	Jefe del Dep. de Redes	Infraestructura de Red	Edificio principal	Medio

VALORAR LOS ACTIVOS

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Equipo de Desarrollo	Equipo encargado del desarrollo de software y aplicaciones empresariales.	Jefe del Dep. de IT	Personal	Oficina	Muy Alto

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Importancia
ID_01	Sala de Servidores	Espacio dedicado para los servidores, diseñado para protección y mantenimiento.	Jefe de Seguridad (Portero)	Instalaciones	Edificio principal	Alto
ID_02	Sistemas de Energía	Infraestructura que suministra energía eléctrica a los servidores.	Jefe de Seguridad (Portero)	Instalaciones	Edificio principal	Medio

IDENTIFICAR LAS AMENAZAS



**Software y Aplicaciones:**

- Las vibraciones de la panadería pueden corromper datos críticos. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> corrupción de datos.
- Fluctuaciones eléctricas pueden desestabilizar los sistemas, facilitando accesos no autorizados. (AMENAZA: ATAQUES INTENCIONADOS) -> intrusiones.
- Reinicios inesperados por fluctuaciones eléctricas pueden permitir infiltraciones de malware. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> infección por malware.
- Condiciones ambientales adversas aumentan la probabilidad de errores en el código.

**Dispositivos:**

- El alto consumo eléctrico de la panadería puede sobrecargar los servidores. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> sobrecarga del sistema.
- Las vibraciones constantes pueden causar fallos en los componentes del hardware. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fallos mecánicos.
- Fluctuaciones eléctricas pueden interrumpir actualizaciones críticas. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fallos de actualización.

**Dispositivos:**

- El alto consumo eléctrico de la panadería puede sobrecargar los servidores. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> sobrecarga del sistema.
- Las vibraciones constantes pueden causar fallos en los componentes del hardware. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fallos mecánicos.
- Fluctuaciones eléctricas pueden interrumpir actualizaciones críticas. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fallos de actualización.

**Telecomunicaciones:**

- Interferencias electromagnéticas pueden causar pérdida de conectividad. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> pérdida de conectividad.
- Fluctuaciones eléctricas pueden dejar los equipos de red vulnerables a ataques. (AMENAZA: ATAQUES INTENCIONADOS) -> intrusiones.
- Equipos eléctricos de la panadería pueden afectar la transmisión de datos. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> degradación de la señal.

**Instalaciones:**

- La proximidad de la panadería afecta el hardware. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> fallos mecánicos.
- Fluctuaciones causadas por el alto consumo de la panadería pueden interrumpir el suministro eléctrico. (AMENAZA: ERRORES Y FALLOS NO INTENCIONADOS) -> pérdida de energía.

IDENTIFICAR LAS VULNERABILIDADES



### **SOFTWARE Y APLICACIONES:**

- Las vibraciones de la panadería pueden corromper datos críticos. -> SISTEMAS SUSCEPTIBLES A VIBRACIONES, las vibraciones pueden corromper los datos almacenados.
- Fluctuaciones eléctricas pueden desestabilizar los sistemas, facilitando accesos no autorizados. -> FALTA DE PROTECCIÓN CONTRA INTERRUPCIONES ELÉCTRICAS, desestabilizando sistemas y facilitando accesos no autorizados.
- Reinicios inesperados por fluctuaciones eléctricas pueden permitir infiltraciones de malware. -> INTERRUPCIONES INESPERADAS, reinicios que pueden permitir infiltraciones de malware.
- Condiciones ambientales adversas aumentan la probabilidad de errores en el código. -> AMBIENTE DE OPERACIÓN INADECUADO, condiciones que aumentan la probabilidad de errores en el código.

### **DISPOSITIVOS:**

- El alto consumo eléctrico de la panadería puede sobrecargar los servidores. -> FALTA DE CAPACIDAD PARA MANEJAR SOBRECARGAS, el alto consumo eléctrico puede sobrecargar los servidores.
- Las vibraciones constantes pueden causar fallos en los componentes del hardware. -> HARDWARE VULNERABLE A VIBRACIONES, las vibraciones constantes pueden causar fallos en los componentes.
- Fluctuaciones eléctricas pueden interrumpir actualizaciones críticas. -> INTERRUPCIONES ELÉCTRICAS DURANTE ACTUALIZACIONES, interrumpiendo actualizaciones críticas.

### **PERSONAL:**

- Interrupciones eléctricas pueden facilitar accesos no autorizados. -> FALTA DE POLÍTICAS DE SEGURIDAD DURANTE INTERRUPCIONES, facilitando accesos no autorizados.
- El personal puede cometer errores al corregir problemas causados por fluctuaciones eléctricas. -> ERRORES HUMANOS DURANTE RECUPERACIÓN DE FALLOS, aumentados por fluctuaciones eléctricas.
- Falta de cifrado durante interrupciones puede exponer información sensible. -> AUSENCIA DE CIFRADO EN DATOS SENSIBLES, exponiendo información durante interrupciones.

### TELECOMUNICACIONES:

- Interferencias electromagnéticas pueden causar pérdida de conectividad. -> INFRAESTRUCTURA VULNERABLE A INTERFERENCIAS, pérdida de conectividad debido a interferencias electromagnéticas.
- Fluctuaciones eléctricas pueden dejar los equipos de red vulnerables a ataques. -> EQUIPOS SIN PROTECCIÓN ADECUADA CONTRA FLUCTUACIONES, dejando los equipos de red vulnerables a ataques.
- Equipos eléctricos de la panadería pueden afectar la transmisión de datos. -> INTERFERENCIA EXTERNA EN LA RED, equipos eléctricos de la panadería afectando la transmisión de datos.

### INSTALACIONES:

- La proximidad de la panadería afecta el hardware. -> UBICACIÓN EN UN ÁREA SUSCEPTIBLE A VIBRACIONES Y CALOR, afectando el hardware.
- Fluctuaciones causadas por el alto consumo de la panadería pueden interrumpir el suministro eléctrico. -> ALTO CONSUMO ELÉCTRICO CERCANO, causando fluctuaciones e interrupciones en el suministro eléctrico.

### EVALUAR EL RIESGO



#### Activo: Software y Aplicaciones

N°	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto				Riesgo
			Financiero	Imagen	Operativo	Total	
1	Pérdida de datos debido a errores de programación, fallos en el sistema de almacenamiento, o ataques de malware	4	5	4	5	14	18.67
2	Acceso no autorizado que puede conducir a la exposición de información confidencial	5	4	5	1	10	15
3	Infección de sistemas por malware que causa pérdida de datos y capacidad operativa	4	4	1	3	8	12
Riesgo Promedio							15.22

#### Activo: Dispositivos

N°	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto			Total	Riesgo
			Financiero	Imagen	Operativo		
4	Daño de algún componente de hardware del servidor por ser de hace 10 años	4	4	3	4	11	16
Riesgo Promedio							16

#### Activo: Telecomunicaciones

N°	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto			Total	Riesgo
			Financiero	Imagen	Operativo		
5	Pérdida de conexión con la sucursal por rompimiento de la fibra óptica	2	2	2	2	6	4
Riesgo Promedio							4

Activo: Personal

N°	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto			Total	Riesgo
			Financiero	Imagen	Operativo		
6	Divulgación accidental o intencional de información confidencial por parte del personal	3	3	3	3	9	10
Riesgo Promedio							10

Activo: Instalaciones

N°	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto			Total	Riesgo
			Financiero	Imagen	Operativo		
7	Incendio en instalaciones debido a un incidente en la panadería	4	4	2	3	9	6.67
Riesgo Promedio							6.67

	DESCRIPCIÓN DEL RIESGO	Probabilidad	Impacto	ACTIVO
1	Pérdida de datos debido a errores de programación, fallos en el sistema de almacenamiento, o ataques de malware	4	5	Activo: Software y Aplicaciones
2	Acceso no autorizado que puede conducir a la exposición de información confidencial	5	4	Activo: Software y Aplicaciones
3	Infección de sistemas por malware que causa pérdida de datos y capacidad operativa	4	4	Activo: Software y Aplicaciones
4	Fallos de hardware que provocan interrupciones significativas en la operación del servidor	3	5	Activo: Dispositivos
5	Interrupciones en la conectividad debido a problemas en la infraestructura de la red	3	4	Activo: Telecomunicaciones
6	Divulgación accidental o intencional de información confidencial por parte del personal	3	3	Activo: Personal
7	Incendio en instalaciones debido a un incidente en la panadería	2	4	Activo: Instalaciones

Impacto

MUY ALTO (5)	MEDIO	MEDIO	4	1	MUY ALTO
ALTO (4)	BAJO	7	5	3	2
MEDIO (3)	MUY BAJO	BAJO	6	ALTO	ALTO
BAJO (2)	MUY BAJO	BAJO	BAJO	MEDIO	MEDIO
MUY BAJO (1)	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	MEDIO
	MUY BAJO (1)	BAJO (2)	MEDIO (3)	ALTO (4)	MUY ALTO (5)

Probabilidad

TRATAR EL RIESGO



ACTIVO	DESCRIPCIÓN DEL RIESGO
Activo: Software y Aplicaciones	Pérdida de datos debido a errores de programación, fallos en el sistema de almacenamiento, o ataques de malware
Activo: Software y Aplicaciones	Acceso no autorizado que puede conducir a la exposición de información confidencial
Activo: Software y Aplicaciones	Infección de sistemas por malware que causa pérdida de datos y capacidad operativa
Activo: Dispositivos	Fallos de hardware que provocan interrupciones significativas en la operación del servidor
Activo: Telecomunicaciones	Interrupciones en la conectividad debido a problemas en la infraestructura de la red
Activo: Personal	Divulgación accidental o intencional de información confidencial por parte del personal
Activo: Instalaciones	Incendio en instalaciones debido a un incidente en la panadería

CONTRAMEDIDAS

Controles de calidad en desarrollo, almacenamiento redundante, antivirus y firewalls actualizados.
Autenticación multifactor, cifrado robusto, auditorías de acceso y monitoreo de registros.
Antivirus y anti-malware, restricción de privilegios, educación en seguridad para el personal.
Hardware redundante, monitoreo proactivo, planes de recuperación ante desastres.
Diversificación de proveedores de internet, redundancia en enlaces de red, uso de IDS/IPS.
Políticas claras de manejo de información, capacitación en seguridad, controles de acceso.
Sistemas de detección y extinción de incendios, planificación de evacuación, respaldo externo de datos.