UNIVERSIDAD AUTÓNOMA "TOMAS FRÍAS" CARRERA DE INGENIERÍA DE SISTEMAS				
Materia:	Arquitectura de computadoras (SIS-522)			
Docente: **Auxiliar:**	Ing. Gustavo A. Puita Choque Univ. Aldrin Roger Perez Miranda			N° Práctica
Nombre:	**Jhon Jairo Gomez Cordova**			8
Grupo:	**1**	**Sede**	**Potosí**	

Con base en el concepto de "mantenimiento proactivo", realiza el análisis de riesgos del siguiente problema

La universidad cuenta con una infraestructura tecnológica importante para sus actividades académicas, pero enfrenta riesgos significativos debido a problemas eléctricos. Algunos cables están mal conectados, lo que aumenta el riesgo de cortocircuitos y sobrecargas. Además, los UPS tienen más de 10 años de uso y no garantizan un respaldo confiable, dejando expuestos a los equipos críticos ante interrupciones eléctricas. Sin embargo, la institución ha mostrado un compromiso por mantener sus sistemas tecnológicos en funcionamiento y dispone de un equipo técnico que podría implementar mejoras. Con una inversión moderada en mantenimiento preventivo y renovación de equipos, se puede reducir el riesgo y garantizar una operación más segura y eficiente.

DETERMINARA EL ALCANCE

El alcance del análisis de riesgos se centra en la infraestructura tecnológica de la universidad, específicamente en los sistemas de energía eléctrica y los equipos críticos.

Identificar y valorar los activos

Podemos clasificar los activos por grupo
- Equipos críticos (servidores, routers, switches, etc.) ✓
- Sistemas de energía eléctrica (UPS, generadores, etc.) ✓
- Infraestructura de red (cables, conectores, etc.) ✓
- Software y aplicaciones: $10,000 ✓
- Datos y información ✓

valorar los activos

- Disponibilidad: ¿Qué importancia tiene que el activo no esté disponible?
- Integridad: ¿Qué importancia tiene que la información asociada al activo sea modificada sin control?
- Confidencialidad: ¿Qué importancia tiene que la información asociada al activo sea conocida por personas no autorizadas?
- Muy baja (1): El activo no es crítico y su pérdida no tendría un impacto significativo.
- Baja (2): El activo es importante, pero su pérdida no tendría un impacto crítico.
- Media (3): El activo es crítico y su pérdida tendría un impacto significativo.
- Alta (4): El activo es muy crítico y su pérdida tendría un impacto muy significativo.
- Muy alta (5): El activo es extremadamente crítico y su pérdida tendría un impacto extremadamente significativo.

Identificar las amenazas

Software y aplicaciones

Amenazas naturales

1. Terremotos: Daños a la infraestructura y equipos.
2. Inundaciones: Daños a la infraestructura y equipos.
3. Huracanes: Daños a la infraestructura y equipos.
4. Incendios: Daños a la infraestructura y equipos.

Amenazas físicas

1. Robo: Robo de equipos y dispositivos.
2. Vandalismo: Daños intencionales a la infraestructura y equipos.
3. Accidentes: Daños no intencionales a la infraestructura y equipos.
4. Intrusiones: Intrusiones no autorizadas en la infraestructura y equipos.

Amenazas lógicas

1. Ataques de malware: Ataques de virus, gusanos y otros tipos de malware.
2. Ataques de phishing: Ataques de engaño para obtener información confidencial.
3. Ataques de SQL injection: Ataques para obtener acceso no autorizado a bases de datos.
4. Ataques de cross-site scripting (XSS): Ataques para obtener acceso no autorizado a información confidencial.

Amenazas de gestión

1. Falta de políticas de seguridad: Falta de políticas y procedimientos de seguridad.
2. Falta de capacitación: Falta de capacitación en seguridad para el personal.
3. Falta de mantenimiento: Falta de mantenimiento preventivo y correctivo de la infraestructura y equipos.
4. Falta de recursos: Falta de recursos financieros y humanos para implementar medidas de seguridad.

Identificar vulnerabilidad y salvaguardas

Vulnerabilidades

1. Cables mal conectados: Cables eléctricos mal conectados pueden causar cortocircuitos y sobrecargas.
2. UPS y generadores obsoletos: Equipos de respaldo de energía obsoletos pueden fallar en caso de una interrupción eléctrica.
3. Falta de mantenimiento preventivo: La falta de mantenimiento preventivo puede causar fallos en los equipos y sistemas.
4. Contraseñas débiles: Contraseñas débiles pueden ser vulnerables a ataques de fuerza bruta.
5. Software desactualizado: Software desactualizado puede contener vulnerabilidades conocidas que pueden ser explotadas por atacantes.
6. Falta de políticas de seguridad: La falta de políticas de seguridad puede causar una falta de claridad en la implementación de medidas de seguridad.
7. Falta de capacitación: La falta de capacitación en seguridad puede causar que el personal no esté preparado para identificar y responder a incidentes de seguridad.

Salvaguardas

1. Equipo técnico capacitado: Un equipo técnico capacitado puede identificar y responder a incidentes de seguridad de manera efectiva.
2. Políticas de seguridad: Políticas de seguridad claras y bien implementadas pueden ayudar a prevenir incidentes de seguridad.
3. Mantenimiento preventivo: El mantenimiento preventivo regular puede ayudar a prevenir fallos en los equipos y sistemas.
4. Software de seguridad: Software de seguridad como antivirus, firewalls y sistemas de detección de intrusos pueden ayudar a prevenir ataques.
5. Respaldo de datos: El respaldo de datos regular puede ayudar a garantizar la disponibilidad de los datos en caso de una interrupción.
6. Plan de continuidad: Un plan de continuidad puede ayudar a garantizar la continuidad de las operaciones en caso de una interrupción.

7. Capacitación en seguridad: La capacitación en seguridad para el personal puede ayudar a garantizar que estén preparados para identificar y responder a incidentes de seguridad.

fórmula Riesgo = Probabilidad x Impacto

| 1 (Muy baja) | Es muy improbable que ocurra | 1 (Muy bajo) | El impacto es mínimo | 1 (Muy bajo) |
| 2 (Baja) | Es improbable que ocurra | 2 (Bajo) | El impacto es moderado | 4 (Moderado) |
| 3 (Media) | Es posible que ocurra | 3 (Medio) | El impacto es significativo | 9 (Alto) |
| 4 (Alta) | Es probable que ocurra | 4 (Alto) | El impacto es grave | 16 (Muy alto) |
| 5 (Muy alta) | Es muy probable que ocurra | 5 (Muy alto) | El impacto es catastrófico | 25 (Extremadamente alto) |

Evaluación del Riesgo

Para evaluar el riesgo, se debe asignar un valor de probabilidad y un valor de impacto para cada riesgo identificado. Luego, se multiplica la probabilidad por el impacto para obtener el valor de riesgo.

Por ejemplo, si se identifica un riesgo de incendio en el servidor, se podría asignar un valor de probabilidad de 3 (Media) y un valor de impacto de 4 (Alto). El valor de riesgo sería:

Riesgo = Probabilidad x Impacto = 3 x 4 = 12 (Alto)

Tratar el riesgo

Una vez que se ha identificado y evaluado el riesgo, es importante tratarlo para reducir su impacto. Hay varias formas de tratar el riesgo, dependiendo del tipo de riesgo y de la organización. A continuación, se presentan algunas opciones comunes:

1. Evitar el Riesgo: Si es posible, se puede evitar el riesgo eliminando la causa que lo genera. Por ejemplo, si se identifica un riesgo de incendio en un servidor, se puede evitar el riesgo reubicando el servidor en un área más segura.
2. Reducir el Riesgo: Si no es posible evitar el riesgo, se puede reducir su impacto implementando medidas de control. Por ejemplo, se puede instalar un sistema de detección de incendios y un sistema de extinción de incendios para reducir el riesgo de incendio en un servidor.
3. Transferir el Riesgo: En algunos casos, se puede transferir el riesgo a otra parte, como un seguro o un contrato. Por ejemplo, se puede contratar un seguro para cubrir los daños causados por un incendio en un servidor.
4. Aceptar el Riesgo: En algunos casos, se puede aceptar el riesgo y no tomar medidas para reducirlo. Esto puede ser debido a que el riesgo es muy bajo o que no

hay medidas efectivas para reducirlo.

continuación, se presentan algunas estrategias comunes para tratar el riesgo:

1. Análisis de Costo-Beneficio: Se analiza el costo de implementar medidas de control y se compara con el beneficio de reducir el riesgo.
2. Análisis de Riesgo-Beneficio: Se analiza el riesgo de no implementar medidas de control y se compara con el beneficio de implementarlas.
3. Evaluación de la Eficacia: Se evalúa la eficacia de las medidas de control implementadas para reducir el riesgo.
4. Monitoreo y Revisión: Se monitorea y revisa regularmente el riesgo y las medidas de control implementadas para asegurarse de que sigan siendo efectivas.

EL CONTENIDO ES BUEN SIN EMBARGO SOLO PRESENTAS MEDIDAS DE SEGURIDAD Y CAUSAS PERO NO ATACAS LOS 4 PUNTOS QUE IDENTIFICASTE

- Equipos críticos (servidores, routers, switches, etc.)
- Sistemas de energía eléctrica (UPS, generadores, etc.)
- Infraestructura de red (cables, conectores, etc.)
- Software y aplicaciones: $10,000
- Datos y información