**UNIVERSIDAD NACIONAL DE JUJUY - FACULTAD DE INGENIERÍA**

**SEGURIDAD Y AUDITORIA INFORMATICA**

**TRABAJO PRÁCTICO Nº 2**

1. ¿El análisis de riesgo siempre debe hacerse para toda la organización?
2. Los aires acondicionados y los mata fuegos ¿Pueden considerarse como activos de información? ¿Por qué?
3. Si los activos no se pueden valorar de manera económica ¿Qué escala de valoración se podría utilizar?
4. Una vez calculado los riesgos ¿Cuáles son los riesgos que se deben tratar?
5. ¿Cómo se puede eliminar un riesgo? ¿Es viable?
6. A continuación, se muestran las tablas necesarias para realizar un análisis de riesgos.

Tabla 1. Disponibilidad

|  |  |
| --- | --- |
| **Valor**  | **Criterio** |
| 0 | No aplica / No es relevante |
| 1 | Debe estar disponible al menos el 10% del tiempo |
| 2 | Debe estar disponible al menos el 50% del tiempo |
| 3 | Debe estar disponible al menos el 99% del tiempo |

Tabla 2. Integridad

|  |  |
| --- | --- |
| **Valor**  | **Criterio** |
| 0 | No aplica / No es relevante |
| 1 | No es relevante los errores que tenga o la información que falte |
| 2 | Tiene que estar correcto y completo al menos en un 50% |
| 3 | Tiene que estar correcto y completo al menos en un 95% |

Tabla 3. Confidencialidad

|  |  |
| --- | --- |
| **Valor**  | **Criterio** |
| 0 | No aplica / No es relevante |
| 1 | Daños muy bajos, el incidente no trascendería del área afectada |
| 2 | Los daños serían relevantes, el incidente implicaría a otras áreas |
| 3 | Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas |

Tabla 4. Probabilidad de ocurrencia de amenazas

|  |  |
| --- | --- |
| **Valor** | **Criterio** |
| 10% | Ocurre una vez cada 10 años |
| 20% | Ocurre una vez cada 5 años |
| 40% | Ocurre una al año |
| 60% | Ocurre una vez al mes |
| 80% | Ocurre una vez a la semana |
| 100% | Ocurre varias veces a la semana |

Tabla 5. Valoración de activos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tipo** | **Activo** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Valor total** |
| **Software** | Aplicaciones de gestión | 1 | 1 | 2 | 4 |
| Base de datos | 3 | 3 | 3 | 9 |
| **Hardware** | Servidores | 3 | 2 | 3 | 8 |
| Pc de usuarios | 2 | 1 | 2 | 5 |
| Red de comunicaciones | 2 | 2 | 3 | 7 |
| **Instalaciones** | Oficinas | 0 | 2 | 1 | 3 |
| **Personal** | Empleados | 1 | 0 | 2 | 3 |
| Subcontratados | 1 | 0 | 1 | 2 |
| **Datos** | Expedientes | 3 | 3 | 3 | 9 |
| Contabilidad | 3 | 3 | 3 | 9 |

Los valores totales son la suma de los valores para los tres parámetros.

En base a las tablas anteriores y a la identificación de las amenazas se confecciona la siguiente tabla.

Tabla 6. Riesgos

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Valor del activo** | **Fuego** | **Inundación** | **Falla del suministro eléctrico** | **Acceso no autorizado** | **Errores humanos** | **Virus** | **Divulgación de información** | **Robo** | **Riesgo** |
| **Probabilidad de amenaza** |  | 20% | 10% | 40% | 40% | 100% | 80% | 40% | 30% |  |
| **Aplicaciones de gestión** | 4 |  |  |  |  |  |  |  |  |  |
| **Base de datos** | 9 |  |  |  |  |  |  |  |  |  |
| **Servidores** | 8 |  |  |  |  |  |  |  |  |  |
| **Pc de usuario** | 5 |  |  |  |  |  |  |  |  |  |
| **Red de comunicaciones** | 7 |  |  |  |  |  |  |  |  |  |
| **Oficinas** | 3 |  |  |  |  |  |  |  |  |  |
| **Empleados** | 3 |  |  |  |  |  |  |  |  |  |
| **Subcontratados** | 2 |  |  |  |  |  |  |  |  |  |
| **Expedientes** | 9 |  |  |  |  |  |  |  |  |  |
| **Contabilidad** | 9 |  |  |  |  |  |  |  |  |  |

Se pide:

Determinar el valor del riesgo al que está expuesto cada activo teniendo en cuenta que:

**Riesgo = valor del activo \* probabilidad de amenaza**

***Se tomará como valor del riesgo para el activo el valor promedio que arrojen los valores individuales de cada amenaza.***

1. En base a los resultados obtenidos, explique cómo trataría cada uno de los riesgos (transferirlo, eliminarlo, mitigarlo, asumirlo). Justifique cada respuesta.
2. Análisis de riesgo con probabilidad e impacto

La empresa PYME "ConexiónWeb" se dedica a proporcionar servicios de internet a clientes en su área local. Dado que la confiabilidad y seguridad de los servicios de internet son fundamentales para el negocio, la empresa busca identificar y gestionar los riesgos asociados. A continuación, se presenta una matriz de riesgo con algunos activos de información y amenazas.

El riesgo parcial (RP) que tiene un activo de ser atacado por una amenaza se calcula como P \* I, donde P es la probabilidad de ocurrencia e I es el impacto. Los valores de P e I son:

Probabilidad (P):

Baja: Poco probable, valor 1.

Moderada: Posible, pero no frecuente, valor 2.

Alta: Probable que ocurra, valor 3.

Impacto (I):

Bajo: Impacto mínimo, valor 1.

Moderado: Impacto significativo, pero manejable, valor 2.

Alto: Impacto severo, con consecuencias graves, valor 3.

De manera grupal, asignen un valor de probabilidad e impacto para cada activo y amenaza luego calculen el riesgo parcial (RP). El riesgo total se calcula como la suma de los riesgos parciales.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activo de Información / Amenaza** | **Amenaza: Acceso no Autorizado** | **Amenaza: Pérdida de Datos** | **Amenaza: Ataques de Malware** | **Amenaza: Fallo de Hardware** | **Amenaza: Fuga de Código Fuente** | **Riesgo Total (RT)** |
| **Datos de Clientes** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP =  |  |  |  |  |
| **Registros de Conexión** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP =  | RP =  | RP =  | RP =  | RP =  |
| **Facturación de Clientes** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP =  | RP =  | RP =  | RP =  | RP =  |
| **Infraestructura de Red** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
|  |  |  |  |  |
| **Recursos de Ancho de Banda** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP =  | RP =  | RP =  | RP =  | RP =  |

En base a los resultados obtenidos, explique cómo trataría cada uno de los riesgos (transferirlo, eliminarlo, mitigarlo, asumirlo). Justifique cada respuesta.