**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. En la valoración de activos ¿Puede un activo tener un valor igual a cero? ¿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 en un proyecto de migración a la nube.

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 en la nube | 3 | 3 | 3 | 9 |
| Base de datos en la nube | 3 | 3 | 3 | 9 |
| **Hardware** | Servidores locales | 2 | 2 | 2 | 6 |
| Pc de usuarios | 0 | 0 | 0 | 0 |
| Red de comunicaciones | 2 | 3 | 3 | 8 |
| **Servicio** | Proveedores de servicio en la nube | 3 | 2 | 3 | 8 |
| **Instalaciones** | Oficinas | 0 | 0 | 0 | 0 |
| **Personal** | Empleados | 1 | 0 | 2 | 3 |
| Subcontratados | 1 | 0 | 1 | 2 |
| **Datos** | Datos de clientes | 3 | 3 | 3 | 9 |
| Registros de actividad | 2 | 2 | 3 | 7 |
| Información financiera | 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** | **Fallo de conectividad** | **Acceso no autorizado** | **Fallo de software** | **Ciberataque** | **Pérdida de datos** | **Riesgo** |
| **Probabilidad de amenaza** |  | 20% | 30% | 40% | 60% | 40% |  |
| **Aplicaciones de gestión en la nube** | 9 |  |  |  |  |  |  |
| **Base de datos en la nube** | 9 |  |  |  |  |  |  |
| **Servidores locales** | 6 |  |  |  |  |  |  |
| **Pc de usuario** | 0 |  |  |  |  |  |  |
| **Red de comunicaciones** | 8 |  |  |  |  |  |  |
| **Proveedores de servicio en la nube** | 8 |  |  |  |  |  |  |
| **Oficinas** | 0 |  |  |  |  |  |  |
| **Empleados** | 3 |  |  |  |  |  |  |
| **Subcontratados** | 2 |  |  |  |  |  |  |
| **Datos de clientes** | 9 |  |  |  |  |  |  |
| **Registros de actividad** | 7 |  |  |  |  |  |  |
| **Información financiera** | 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 de desarrollo de software "SoftTech" crea aplicaciones personalizadas para clientes en diversas industrias. La empresa depende de la estabilidad de sus sistemas y la seguridad de su código para mantener la confianza de los clientes y la continuidad del negocio. Para mitigar riesgos potenciales, se debe realizar un análisis de riesgo de sus activos de información frente a varias 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: Puede ocurrir en ocasiones, valor 2.

Alta: Probabilidad alta de ocurrencia, valor 3.

Impacto (I):

Bajo: Impacto leve y manejable, valor 1.

Moderado: Impacto considerable pero no crítico, valor 2.

Alto: Impacto grave con implicaciones significativas, 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)** |
| **Repositorio de Código** | P = 3 | I = 2 | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP = 6 | | RP = | | RP = | | RP = | | RP = | |
| **Base de Datos de Clientes** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP = | | RP = | | RP = | | RP = | | RP = | |
| **Servidores de Desarrollo** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP = | | RP = | | RP = | | RP = | | RP = | |
| **Aplicaciones de Producción** | P = | I = | P = | I = | P = | I = | P = | I = | P = | I = |  |
| RP = | | RP = | | RP = | | RP = | | RP = | |
| **Sistemas de Comunicación** | 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.