**Matriz de riesgos de 3 X 3 y 5 X 5**

Se realiza una tasación matemática donde se marcan las zonas de riesgo de la siguiente manera:

**Probabilidad** lleva a una zona de riesgo:

* aceptable,
* tolerante,
* moderado,
* importante e
* inaceptable.

**Tabla 1**

Matriz de Riesgos de 3 X 3

| Probabilidad | 3 | ALTA | 15 | 30 | 60 |
| --- | --- | --- | --- | --- | --- |
|
| 2 | MEDIA | 10 | 20 | 40 |
|
| 1 | BAJA | 5 | 10 | 20 |
|
|  |  |  | Bajo | Medio | Alto |
|  |  |  | 5 | 10 | 20 |
|  |  |  | Impacto | | |

Dependiendo del nivel de la aplicación web, servicios o productos que ofrezcan las probabilidades y los impactos, podrían ser más por lo que se podría también trabajar en una matriz de 5\*5 dónde se encontrarían dos tipos de riesgos detectados:

**Tabla 2**

*Tipos de riesgos*

| Ítem | Riesgo | Probabilidad | Impacto |
| --- | --- | --- | --- |
| 1 | Perdidas del control de acceso (*Broken Access Control*). | 3 | 5 |
| 2 | * Configuración de seguridad defectuosa (*Security Misconfiguration*). | 4 | 3 |

Al observar la tabla anterior, se evidencia que la **probabilidad** en el *ítem 1* es de 3 y en el *ítem 2* es de 4, ahora bien, al revisar el i**mpacto** en el *ítem 1* es de 5 y el *ítem 2* es de 3; por tanto y para observar mejor la clasificación de **Probabilidad e Impacto**, se encuentra en la siguiente tabla:

**Tabla 3**

*Datos de probabilidad e impacto*

| Probabilidad |  | Impacto |  |
| --- | --- | --- | --- |
| 1 | Muy bajo | 1 | Muy bajo |
| 2 | Bajo | 2 | Bajo |
| 3 | Moderado | 3 | Moderado |
| 4 | Alto | 4 | Alto |
| 5 | muy alto | 5 | Muy alto |

Se puede definir la clasificación de dónde se encuentra la misma, entonces se procede a realizar una matriz de riesgo de 5 X 5 de la siguiente manera:

**Tabla 4**

*Matriz de riesgo de 5 X 5*

| Probabilidad |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5 |  | 10 | 15 | 20 | 25 |  |
| 4 |  | 8 | | 12 | | --- | | 16 | 20 |  |
| 3 |  | 6 | 9 | | 12 | | --- | | 15 |  |
| 2 |  | 4 | 6 | 8 | 10 |  |
| 1 |  |  |  |  |  |  |
|  | 1 | 2 | 3 | 4 | 5 | Impacto |

En la tabla se puede observar en qué nivel se encuentran dentro de la matriz, los dos riesgos planteados, se evidencia el **R1** “Pérdidas del control de acceso” (*Broken Access Control*) en 15 y el **R2** “Configuración de seguridad defectuosa” (*Security Misconfiguration*) en 12.

La recomendación, plan de mejora o seguimiento sería poder crear una política de control en directriz por parte del departamento **TI** o de políticas de seguridad de la información; esta propuesta se debe realizar coordinada con las recomendaciones del experto el técnico de seguridad en aplicaciones web.