**FORMATO DE ANÁLISIS DE RIESGOS**

1. Robo de información o credenciales de usuario, daño del sistema operativo, perdida de acceso a los archivos.
2. Intersección de la información a través de la red o los puertos de los equipos.
3. Destrucción de la información a través de ataques de denegación de servicios.
4. Falta de políticas de seguridad, posibilidades de sabotaje, fuga o alteración de la información.
5. Pérdida, alteración de la información o daño en el sistema de calificaciones.
6. Pérdida de información, alteración del acceso a la misma, no se hacen respaldos digitales de la información.
7. Datos no homogéneos en la base de datos de la aplicación.
8. Pérdida de información o alteración del acceso a la misma por daños en la infraestructura (equipos y dispositivos).
9. No se tienen procedimiento que establezcan las reglas claras para el copiado y manejo de la información de la compañía.
10. No se tienen establecidos programas de capacitación para el manejo de la información por parte de los funcionarios de la compañía.
11. Perdida de conectividad a la red
12. Fácil acceso a información confidencial.
13. Los sistemas de información disponibles no cifran los datos cuando se están almacenando o transmitiendo.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **N°** | **Descripción** | **Probabilidad** | | | **Impacto** | | |
| **Baja** | **Media** | **Alta** | **Leve** | **Moderado** | **Catastrófico** |
| **R1** | Robo de información o credenciales de usuario, daño del sistema operativo, perdida de acceso a los archivos. | **X** |  |  |  |  | **X** |
| **R2** | Intersección de la información a través de la red o los puertos de los equipos. | **X** |  |  |  |  | **X** |
| **R3** | Destrucción de la información a través de ataques de denegación de servicios. | **X** |  |  |  |  | **X** |
| **R4** | Falta de políticas de seguridad, posibilidades de sabotaje, fuga o alteración de la información. | **X** |  |  |  |  | **X** |
| **R5** | Pérdida, alteración de la información o daño en el sistema de calificaciones. |  | **X** |  |  |  | **X** |
| **R6** | Pérdida de información, alteración del acceso a la misma, no se hacen respaldos digitales de la información. |  | **X** |  |  |  | **X** |
| **R7** | Datos no homogéneos en la base de datos de la aplicación. | **X** |  |  | **X** |  |  |
| **R8** | Pérdida de información o alteración del acceso a la misma por daños en la infraestructura (equipos y dispositivos). | **X** |  |  |  |  | **X** |
| **R9** | No se tienen procedimiento que establezcan las reglas claras para el copiado y manejo de la información del colegio. |  |  | **X** |  | **X** |  |
| **R10** | No se tienen establecidos programas de capacitación para el manejo de la información por parte de los funcionarios del colegio. |  | **X** |  |  | **X** |  |
| **R11** | Perdida de conectividad a la red. | **X** |  |  | **X** |  |  |
| **R12** | Fácil acceso a información confidencial. | **X** |  |  |  |  | **X** |
| **R13** | Los sistemas de información disponibles no cifran los datos cuando se están almacenando o transmitiendo. |  | **X** |  |  | **X** |  |

**Resultado Matriz de riesgos para hardware**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PROBABILIDAD | Alto  61-100% |  | R9 |  |
| Medio  31-60% |  | R10, R13 | R5 a R6 |
| Bajo  0-30% | R7, R11 |  | R1 a R4, R8, R12 |
|  | Leve | Moderado | Catastrófico |
| IMPACTO | | | |

Menor impacto o probabilidad de ocurrencia

Probabilidad y ocurrencia media

Alta probabilidad de ocurrencia

Nota: La probabilidad se establece analizando qué tan posible es que se materialice el riesgo, situación en la que es necesario conocer la organización y el contexto que la rodea. El impacto se evalúa según la gravedad de los daños (información, dispositivos, funcionamiento) que puedan ocurrir en la empresa al materializarse un riesgo.La probabilidad se establece analizando qué tan posible es que se materialice el riesgo, situación en la que es necesario conocer la organización y el contexto que la rodea. El impacto se evalúa según la gravedad de los daños (información, dispositivos, funcionamiento) que puedan ocurrir en la empresa al materializarse un riesgo.