|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Nombre | Descripción | A | V | S | Ocurrencia | Responsables / Afectados |
| U | Aplicaciones no son soportadas | La aplicación no es soportada ya sea por compatibilidad o requisitos mínimos |  |  | X | Media | **Afectado**: La sección en la que la aplicación valla a funcionar  **Responsable**: El encargado de analizar los requisitos mínimos del sistema |
| V | Fallas críticas del sistema | Se producen errores que afectan el funcionamiento del sistema. | X |  |  | Baja | **Afectado**: La sección en la que el sistema valla a funcionar  **Responsable**: El encargado de darle mantenimiento al sistema |
| W | Incapacidad para manejar la carga | No cuenta con la infraestructura necesaria para poder manejar la carga de datos | X |  |  | Media | **Afectado**: La parte administrativa de la empresa  **Responsable**: El DBA |
| X | Asuntos de configuración | El sistema no fue configurado total o parcialmente |  | X |  | Baja | **Afectado:** Todo el personal que valla a interactuar con el sistema  **Responsable**: El encargado de darle mantenimiento al sistema |
| Y | Mala administración de credenciales | Permite el acceso a los distintos niveles a cualquier personal activo |  | X |  | Media | **Afectado**: Todo el sistema en general, debido a la falta de control  **Responsable**: El encargado del sistema para las secciones del mismo y el DBA para los accesos en la base de datos |
| Z | Incompatibilidad entre aplicaciones | Las aplicaciones no pueden intercambiar información entre ellas |  |  | X | Media | **Afectado**: Los módulos que no puedan interactuar entre si  **Responsable**: El encargado de analizar los requisitos mínimos del sistema |
| AA | Daño a los servicios | Daños ocasionados por terceras personas al sistema (hackers) | X |  |  | Baja | **Afectado**: El sistema en general debido a la vulnerabilidad y posible pérdida de información.  **Responsable**: El encargado de la seguridad del sistema |
| BB | Arquitectura de TI inflexible | No permite o tolera cambios a las practicas que ya definió |  | X |  | Media | **Afectado**: El personal en general debido a la resistencia a cambios  **Responsable**: Gobierno de TI |
| CC | Robo | Robo total o parcial a los equipos de cómputo o maquinaria en general | X |  |  | Media | **Afectado**: La empresa en general  **Responsable**: La seguridad con la que cuente la empresa |
| DD | Tecnología obsoleta | Falta de recursos para implantar un sistema actualizado |  | X |  | Alta | **Afectado**: El sistema debido a que no podrá instalarse o correr óptimamente.  **Responsable**: El encargado de analizar los requisitos mínimos del sistema |
| EE | Certificación de redes | Se comprueba que la instalación de esa red cumple los parámetros técnicos necesarios para cumplir con la normativa internacional relacionada con el tipo de instalación. |  |  | X | Baja | **Afectado**: Interacción entre módulos del sistema (Sistema en general)  **Responsable**: El encargado de instalar y dar mantenimiento a las Redes |
| FF | No soporta múltiples plataformas o entornos de desarrollo | No permite la interacción de sistemas desarrollados en diferentes plataformas |  |  | X | Baja | **Afectado**: El sistema en general debido a la falta de comunicación entre módulos  **Responsable**: El encargado de analizar los requisitos mínimos del sistema |
| GG | Revelación de datos sensibles | Expone información personal sobre clientes y proveedores así como datos privados de la compañía | X |  |  | Alta | **Afectado**: Toda la empresa, ya que podríamos perder datos que nos produzcan perdidas económicas, como la cartera de clientes  **Responsable**: El encargado de la seguridad del sistema |
| HH | Fuga de datos | La información de nuestros clientes y proveedores puede ser robada. | X |  |  | Alta | **Afectado**: Toda la empresa, ya que podríamos perder datos que nos produzcan perdidas económicas, como la cartera de clientes  **Responsable**: El encargado de la seguridad del sistema o el DBA a la base de datos |
| II | Acceso no autorizado | Personal no autorizado o ajeno a la compañía acceda a nuestra base de datos |  | X |  | Alta | **Afectado:** La empresa en general debido a la posible pérdida o robo de datos.  **Responsable**: El encargado de la seguridad del sistema o el DBA a la base de datos |
| JJ | Falta de minería de datos | No se pueden extraer datos precisos o analizar grandes volúmenes de datos |  | X |  | Media | **Afectado**: La área productiva de la empresa por la falta de datos para tomar decisiones importantes  **Responsable**: El encargado de analizar la base de datos |
| KK | Falta de respaldo de datos | No se realizan respaldos preventivos lo que puede ocasionar pérdida total de información |  | X |  | Alta | **Afectado**: La empresa y sistema en general por la posible pérdida de datos importantes  **Responsable**: El DBA |
| LL | Errores del operador durante el respaldo de los datos | El encargado comete un error al respaldar provocando daño o perdida de información |  |  | X | Media | **Afectado**: La empresa y sistema en general por la posible pérdida de datos importantes  **Responsable**: El DBA por la falta de supervisión y el encargado por la falta de experiencia |
| MM | Fallas en los procesos operativos | No se cumplen los requisitos de los clientes |  | X |  | Media | **Afectado**: La empresa debido a la inconformidad que presentaran los clientes  **Responsable**: El encargado de supervisar y monitorear las peticiones de los clientes |
| NN | No existen roles para los distintos niveles de acceso | Permite el acceso a los distintos niveles a cualquier personal activo |  | X |  | Media | **Afectado:** La empresa en general debido a la posible pérdida o robo de datos.  **Responsable**: El encargado de la seguridad del sistema o el DBA a la base de datos |