

# Índice

1. Introducción.
2. Análisis de riesgos con Magerit.

* Definición de una empresa.
* Activos.

1. Virtuales.
2. S Servicios.
3. S Información.
4. SW Aplicaciones.
5. HW Equipamiento.
6. COM Redes de comunicación.
7. AUX Equipamientos auxiliares.
8. L Instalaciones.
9. P Personal.
10. Salvaguardas con Pilar.
11. Grafo de dependencias entre activos.
12. Auditoría interna.
13. Conclusiones.
14. Bibliografía.

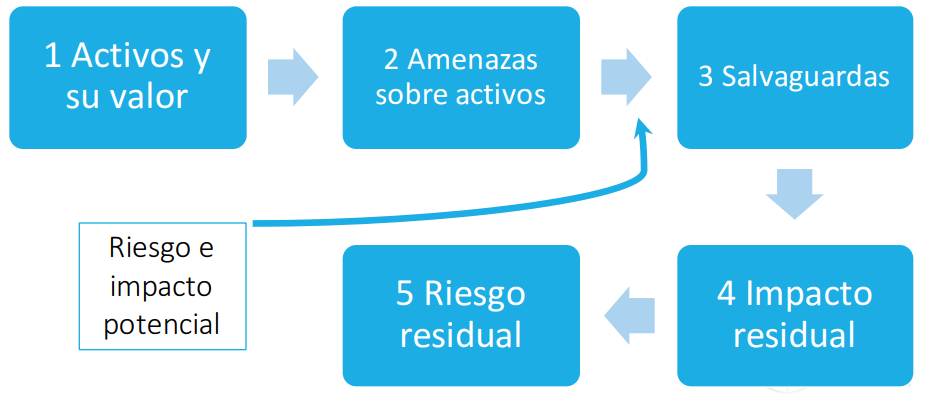
## **Introducción**

¿Cómo podemos conocer los riesgos en una empresa?

Un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización y por ello realizaremos un análisis y gestión de los riesgos.

Un análisis de riesgos es un estudio para evaluar los peligros potenciales y sus posibles consecuencias en una instalación existente o en un proyecto, con el objeto de establecer medidas de prevención y de protección. Comprende la evaluación del riesgo de una plaga, de una enfermedad o de un daño ambiental.

El análisis de riesgos en nuestra nos servirá para poder calificar esas amanezcas ya que nuestro deseo es que ninguna de ellas se materialice y que causen daños a Megastore.

****

**2. Análisis de riesgos con Magerit**

Magerit (basada en la terminología de la normativa ISO 27001), es una metodología de análisis y gestión de riesgos elaborada por El Consejo Superior De Administración Electrónica de España que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

Magerit analiza el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar a la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Definición de una empresa

Realizaremos el análisis de riesgos de una cadena de suministros para distintos procesos o áreas de la empresa, como logística interna(compras) o logística externa(ventas).

Activos:

1. Virtuales:
2. Imagen de la empresa.
3. Reputación.
4. S Servicios.
5. Externos
   1. Distribución de productos (SEUR, NACEX…).
   2. Redes sociales.
6. Internos.
   1. Gestión personal y nóminas.
   2. Gestión de contabilidad
   3. Correo
7. Subcontratados.
   1. SS ADSL
   2. SS Mantenimiento sistemas informáticos
   3. SS Salvaguardia en la nube
8. D Información
   1. Catálogo de productos
   2. Clientes y proveedores
   3. Usuarios registrados
   4. Usuarios internos
   5. Personal y nóminas
   6. Contabilidad
   7. Pedidos
   8. Histórico de compras (clientes, proveedores)
   9. Histórico de precios de productos
9. SW Aplicaciones
   1. Aplicación móvil y de escritorio
   2. Portal web de venta online
   3. Contabilidad(Odoo)
10. HW Equipamiento
    1. Equipos
       1. Servidores WEB
       2. PC
       3. Bases de datos
    2. Comunicaciones
       1. Cortafuegos
       2. Red LAN para usuarios
       3. Conexión ADSL a Internet
    3. Equipos auxiliares
       1. Equipos climatizadores
       2. Detección y extinción de incendios
11. COM Redes de comunicación
    1. Wifi
    2. Telefonía móvil y fija
12. AUX Equipamientos auxiliares
    1. Mobiliario
    2. Telefonía
13. L Instalaciones
    1. Central
       1. Oficinas
       2. Local informático
       3. Almacén
14. P Personal
    1. Usuarios externos registrados
    2. Clientes
    3. Empleados/trabajadores
    4. Proveedores
    5. Administración

#### **1. Virtuales**

**Activos:** Imagen de la empresa y reputación de la empresa.

**Dependencias entre activos:** activos independientes entre sí.

### **Valor de los activos**



**Amenazas**

Estos activos no tienen ninguna amenaza asociada.

#### **2.1 Servicios Externos**

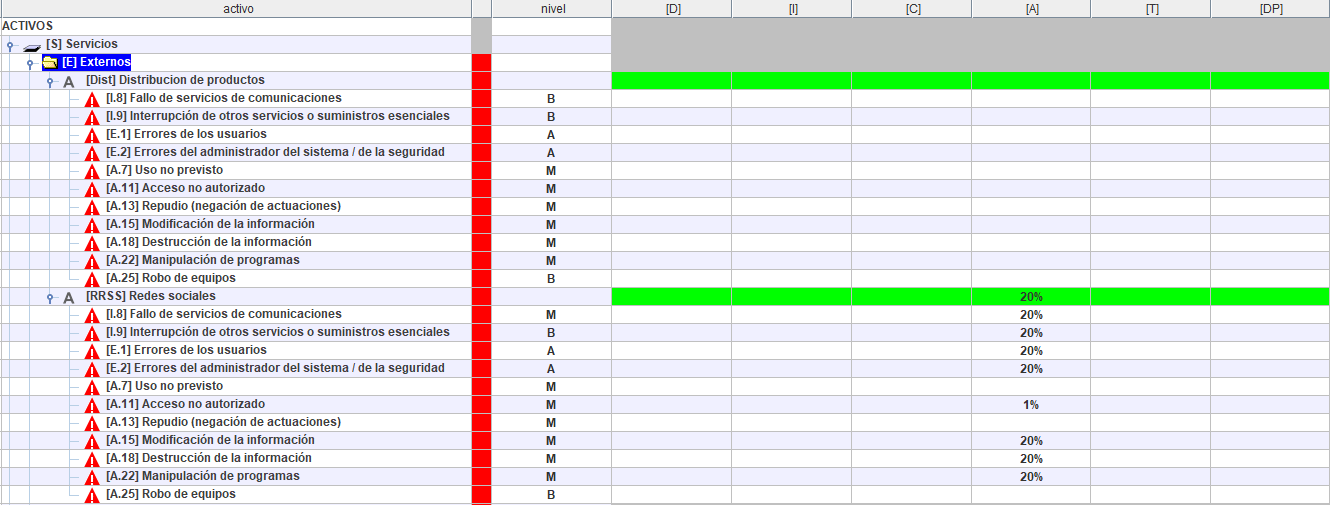
**Activos:** Distribución de productos y redes sociales.

**Dependencias entre activos:** de ellos depende aplicación móvil y de escritorio, portal web de venta online, contabilidad(Odoo), catálogo de productos, clientes y proveedores, histórico de compras (clientes, proveedores), histórico de precios de productos, usuarios internos, PC.

**Valor de los activos**



**Amenazas producidas por PILAR:**



**Amenazas:**

* Problemas con la distribución del producto (robo, mal estado, pérdida, etc).
* Mala reputación en las redes sociales
* Robo de cuentas en las redes sociales

**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, la empresa dejaría de tener la disponibilidad de dicho activo hasta que la amenaza se subsane, lo que deriva en pérdida de comunicación con los clientes o proveedores, pudiendo derivar en pérdida de dinero.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Problemas en la distribución del producto | 10 | Frecuente | Mensualmente |
| Mala reputación en las redes sociales | 1/10 | Poco frecuente | Cada varios años |
| Robo de cuentas en las redes sociales | 1/10 | Poco frecuente | Cada varios años |

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Distribución de productos | Problemas en la distribución del producto | 70% | MA | MA |
| Redes sociales | Mala reputación en las redes sociales | 90% | A | A |
| Redes sociales | Robo de cuentas en las redes sociales | 100% | M | M |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Distribución de productos | Problemas en la distribución del producto | 10 | MA | MA |
| Redes sociales | Mala reputación en las redes sociales | 1/10 | A | A |
| Redes sociales | Robo de cuentas en las redes sociales | 1/10 | M | M |

**Riesgo potencial:** Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR: no tiene**

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + No tener contenido en las redes sociales
  + La gestión en la distribución de los productos se realice dos veces y encontrar posibles fallos
* No justifica:
  + No tener contenido en las redes sociale ya que sería inútil tenerlas y no usarlas
  + La gestión en la distribución de los productos se realice dos veces ya que supondría un esfuerzo excesivo
* Aplican y justifican:
  + Interacción con los clientes en las redes sociales
  + Subir contenido en función de los gustos de los clientes en base a estadísticas
  + Asegurar productos
  + Envíos certificados

#### **2.2 Servicios Internos**

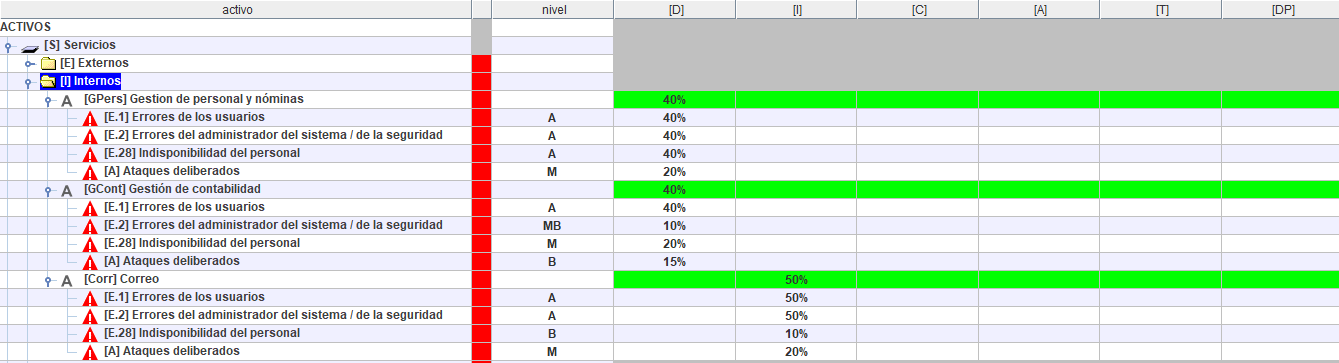
**Activos:** Gestión de personal y nóminas, gestión de contabilidad y correo.

**Dependencias entre activos:** Usuarios internos, personal y nóminas, empleados, proveedores, administración, contabilidad, pedidos, histórico de compras (clientes, proveedores), histórico de precios de productos, clientes, usuarios registrados, usuarios externos registrados, empleados.

**Valor de los activos**

### 

**Amenazas producidas por PILAR:**

****

**Amenazas:**

* Phishing, spam,
* Indisponibilidad del personal
* Fallo en la contabilidad

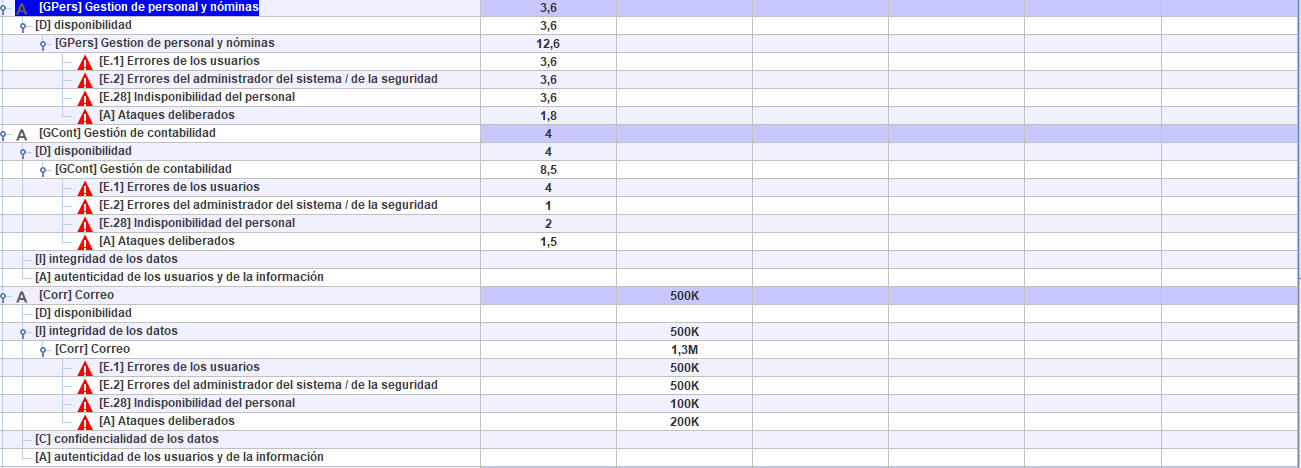
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, los impactos en la empresa podrían ser graves porque afectan a la estructura interna de la empresa, su organización y su contabilidad, resumiendo en costes económicos muy elevados.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Phising,spam | 10 | Frecuente | Mensualmente |
| Indisponibilidad | 1 | Normal | Una vez al año |
| Fallo en la contabilidad | 1/10 | Poco frecuente | Cada varios años |

**Impactos según PILAR:**

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Gestión personal y nóminas | Indisponibilidad | 20% | B | MB |
| Gestión de contabilidad | Fallo en la contabilidad | 10% | A | M |
| Correo | Phishing, spam | 80% | MA | MA |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

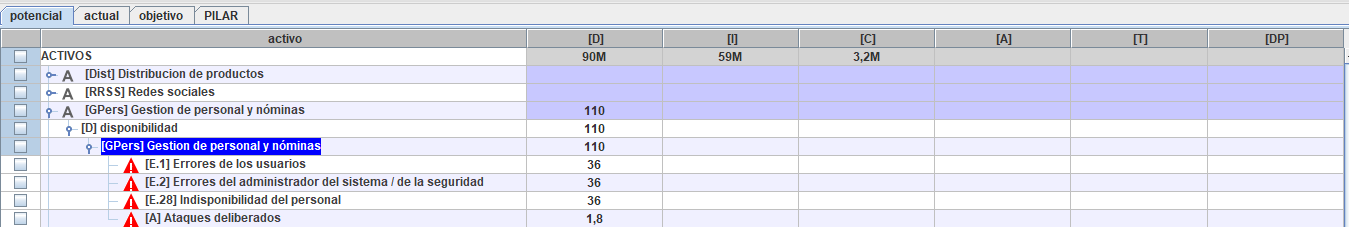
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

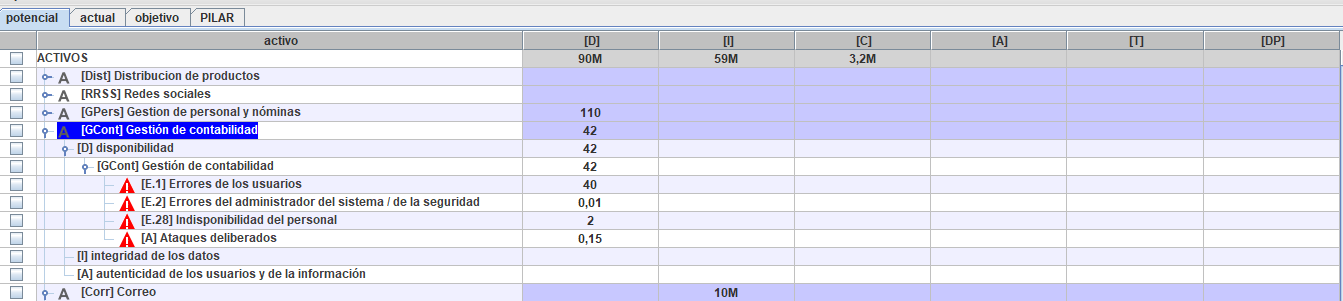
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Gestión personal y nóminas | Indisponibilidad | 10 | MB | B |
| Gestión de contabilidad | Fallo en la contabilidad | 1 | M | M |
| Correo | Phishing, spam | 1/10 | MA | MA |

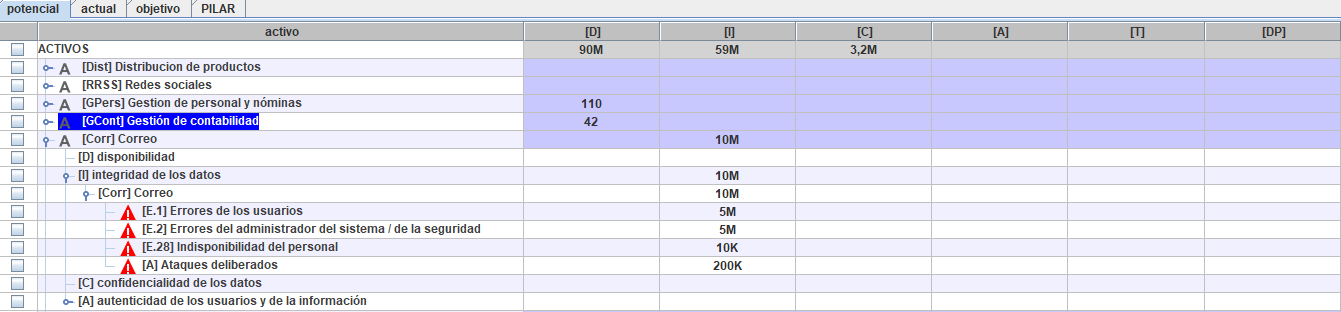
**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

****

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Analizar todos los correos enviados personalmente para comprobar que no hay nada fuera de lo normal.
  + Que la gestión de nóminas se realice dos veces para poder comparar y encontrar posibles fallos.
  + Contratar a alguien que esté permanentemente buscando fallos en la aplicación de gestión de nóminas.
  + Ceder a cualquier petición de las empresas interesadas en un acuerdo.
* No justifica:
  + Analizar personalmente todos los correos ya que sería un esfuerzo excesivo.
  + Realizar la gestión de nóminas dos veces ya que habría que dedicar unos recursos excesivos y necesitaría de una mayor inversión económica.
  + Contratar a alguien que tan solo se dedique a probar la aplicación de nóminas ya que sería excesivo.
  + Ceder a las peticiones de una empresa que perjudique a los productos de las demás empresas.
* Aplican y justifican:

○ Añadir a los contratos cláusulas de confidencialidad.

○ Obligar a los trabajadores a modificar la contraseña periódicamente por si esta hubiese sido hackeada.

○ Realizar charlas y seminarios de concienciación con la seguridad de la información.

○ Añadir alguna medida de verificación de datos a la aplicación de gestión de nóminas.

○ Guardar copias de seguridad de las nóminas.

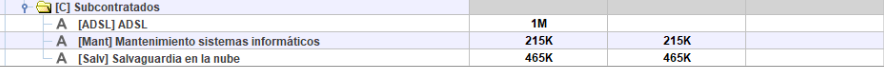
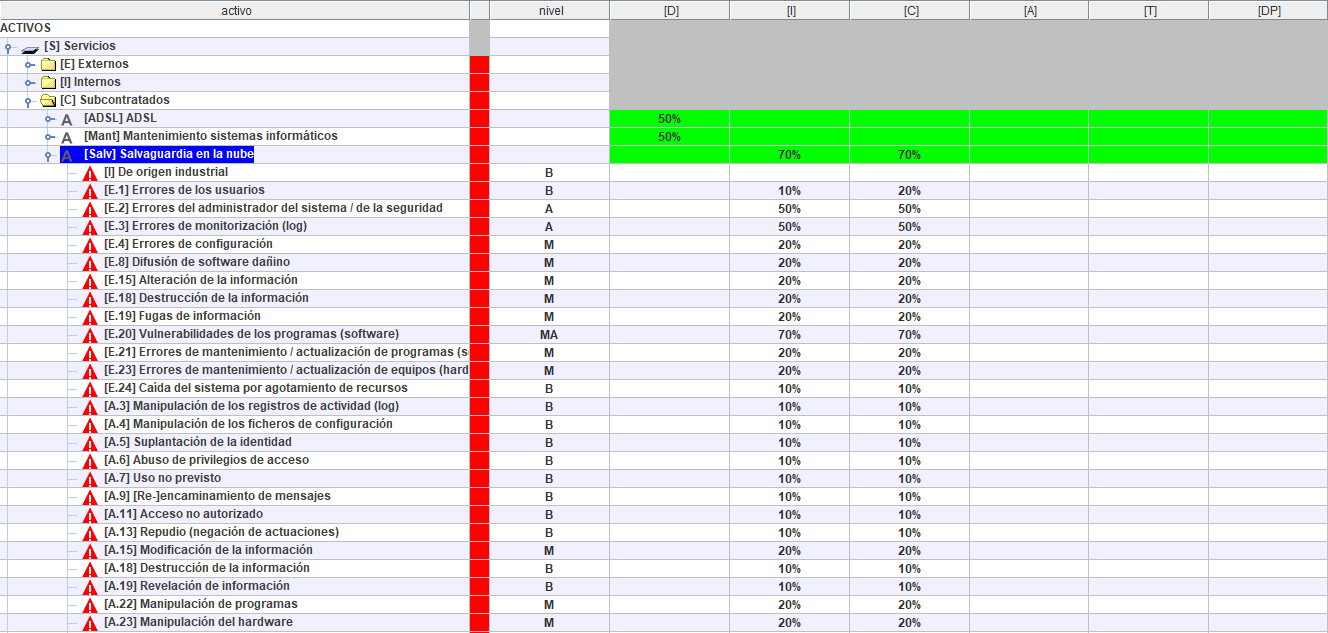
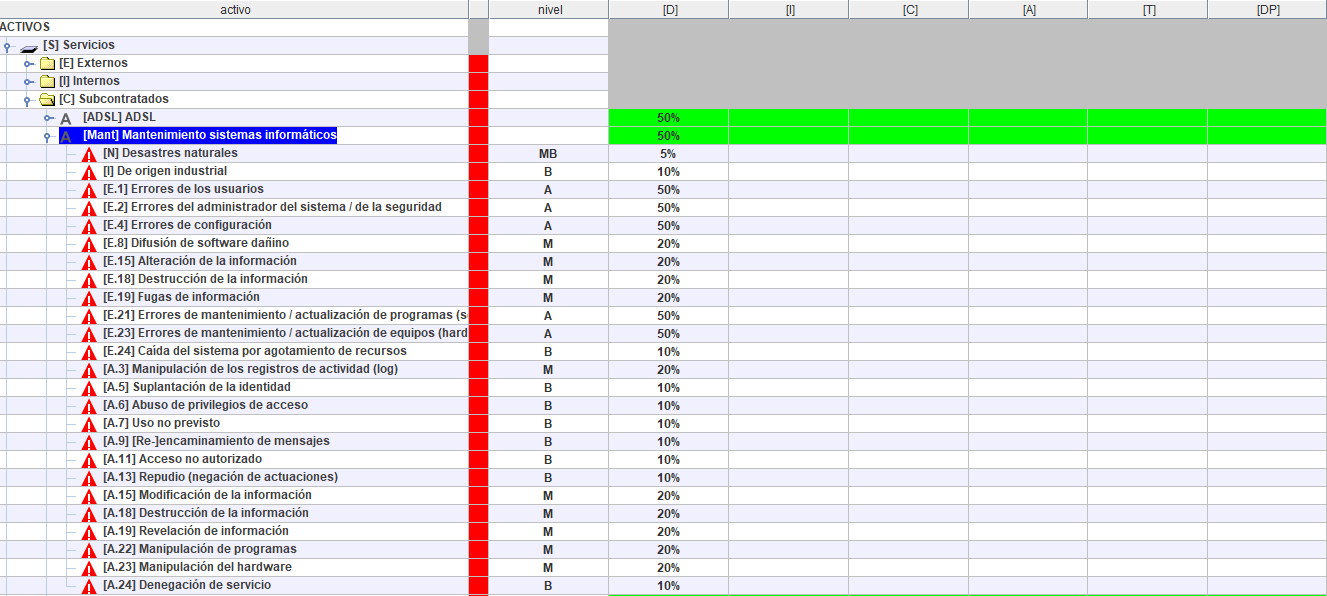
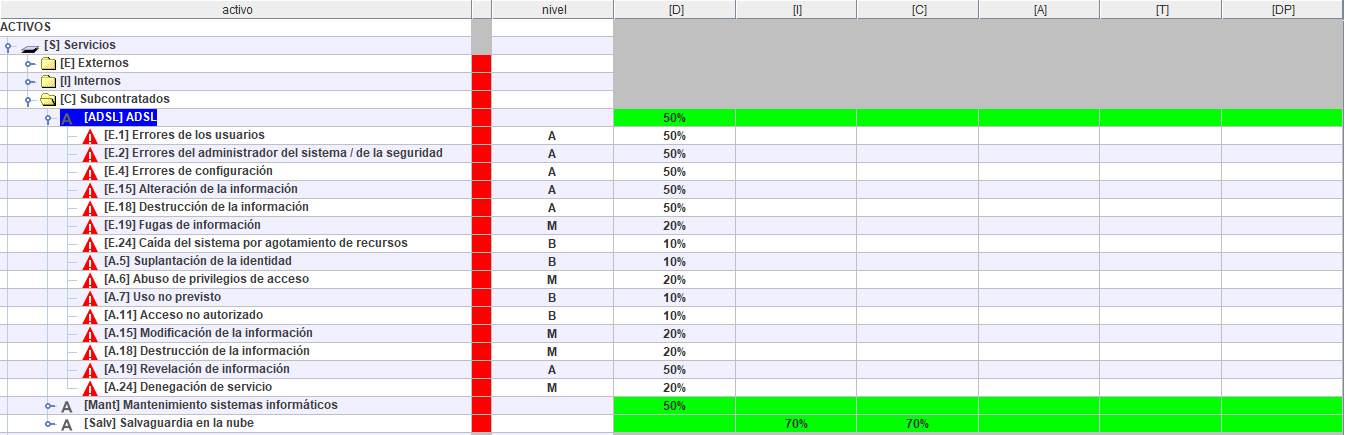
○ Priorizar las peticiones de las empresas más importantes.

#### **2.3 Servicios subcontratados**

**Activos:** ADSL, mantenimiento sistemas informáticos y salvaguardia en la nube.

**Dependencias entre activos:** Red LAN para usuarios, conexión ADSL para Internet, PC, cortafuegos, bases de datos, servidores WEB.

### **Valor de los activos**

**Amenazas producidas por PILAR:**

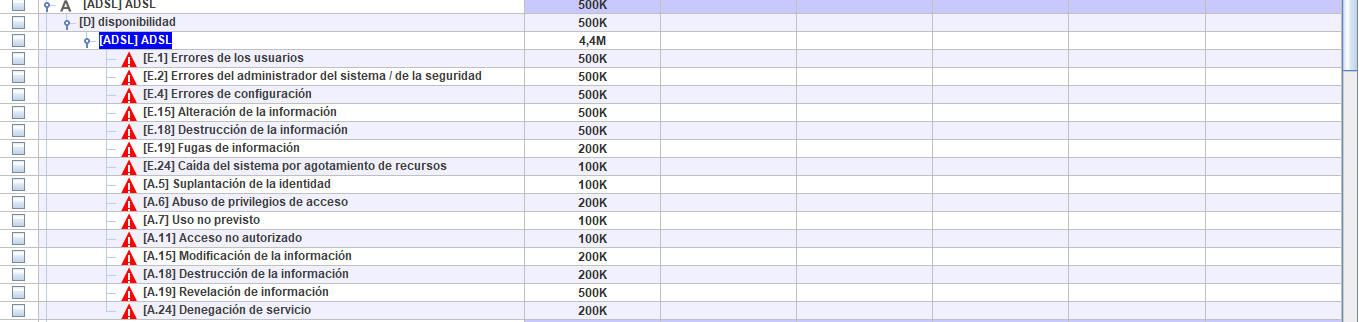
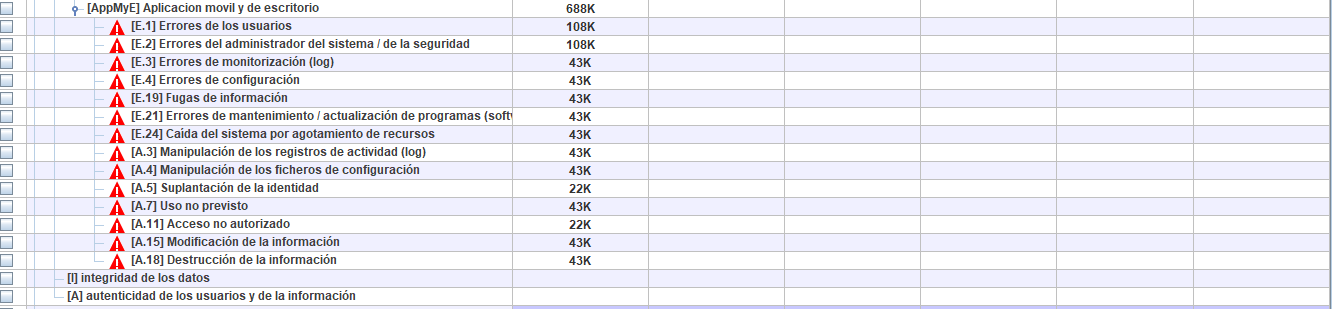
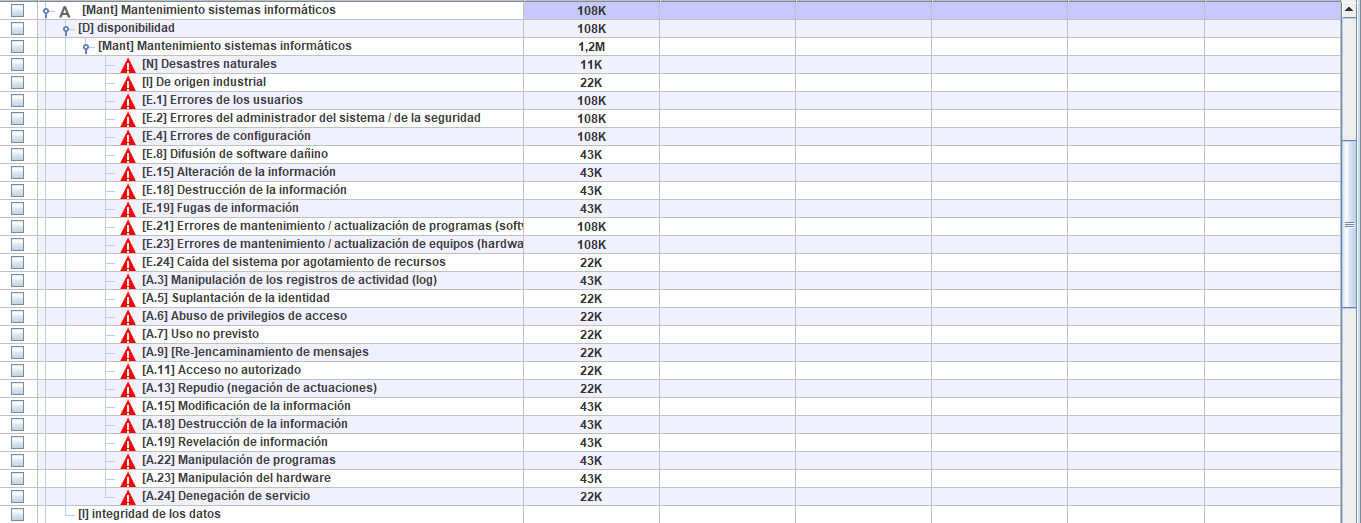
**Amenazas:**

* Interrupción del suministro
* Ataques deliberados a la red
* Caída del sistema
* Fuga de información

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Fuga de información | 1/10 | Poco frecuente | Cada varios años |
| Interrupción del suministro | 1/10 | Poco frecuente | Cada varios años |
| Ataques deliberados a la red | 10 | Frecuente | Mensualmente |
| Caída del sistema | 1 | Normal | Una vez al año |

**Impactos según PILAR:**

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| ADSL | Caída de la red | 100% | M | M |
| ADSL | Interrupción del suministro | 100% | B | B |
| ADSL | Ataques deliberados a la red | 50% | A | M |
| Mantenimiento de sistemas informáticos | Ataques deliberados a la red | 50% | A | M |
| Mantenimiento de sistemas informáticos | Caída del sistema | 70% | A | A |
| Salvaguardias en la nube | Caída del sistema | 1% | MB | MB |
| Salvaguardias en la nube | Fuga de información | 70% | MA | MA |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

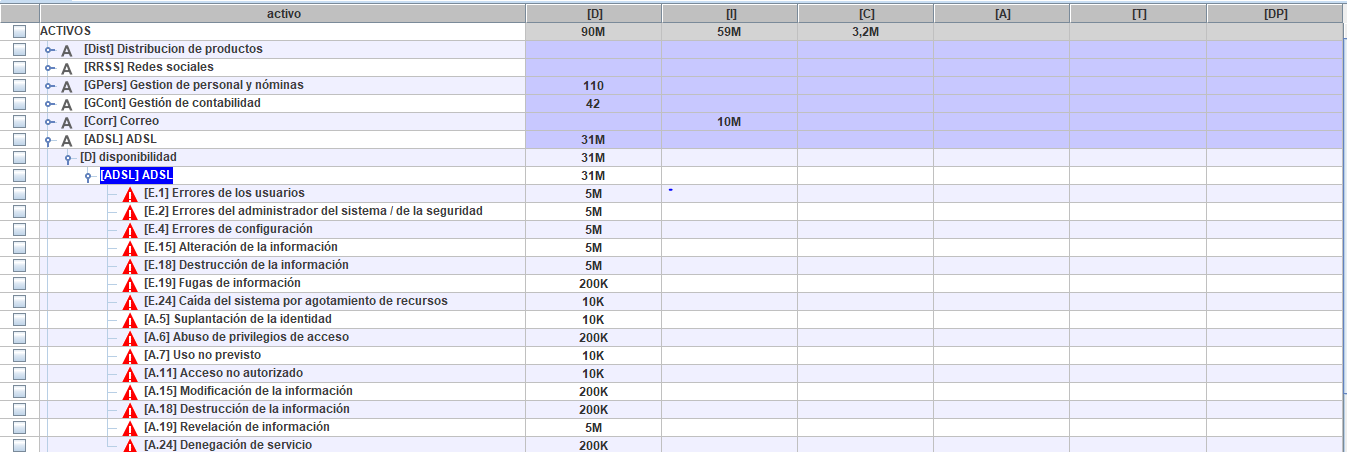
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

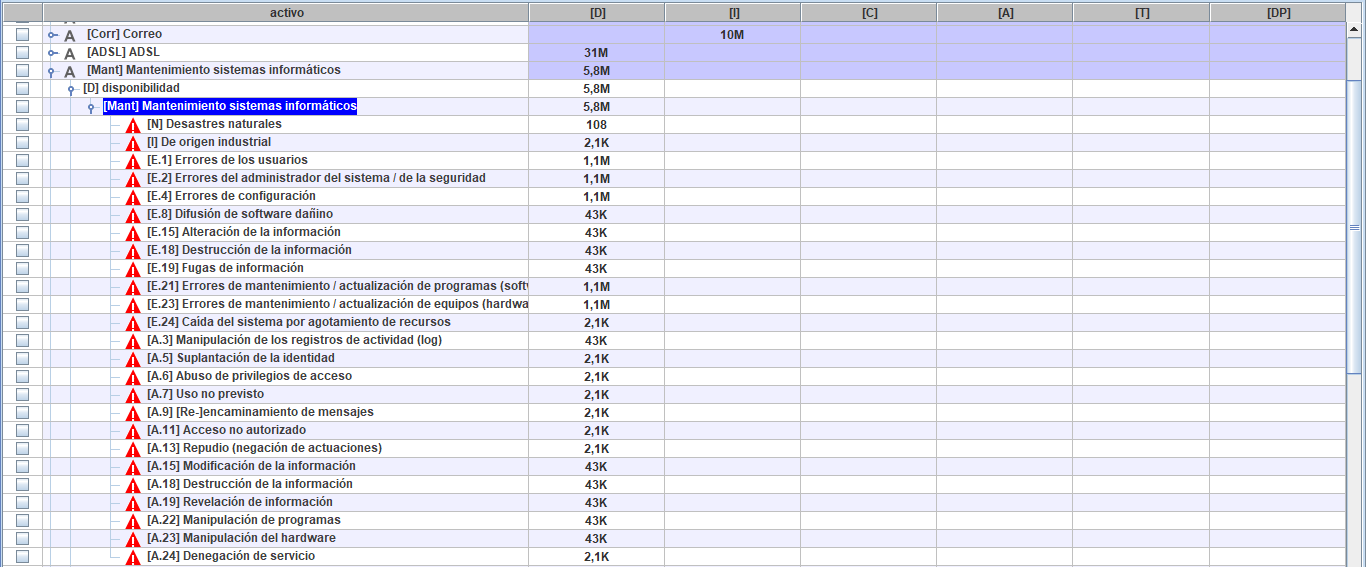
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| ADSL | Caída de la red | 1 | M | M |
| ADSL | Interrupción del suministro | 1/10 | B | B |
| ADSL | Ataques deliberados a la red | 10 | M | A |
| Mantenimiento de sistemas informáticos | Ataques deliberados a la red | 10 | M | A |
| Mantenimiento de sistemas informáticos | Caída del sistema | 1 | A | A |
| Salvaguardias en la nube | Caída del sistema | 1 | MB | MB |
| Salvaguardias en la nube | Fuga de información | 1/10 | MA | MA |

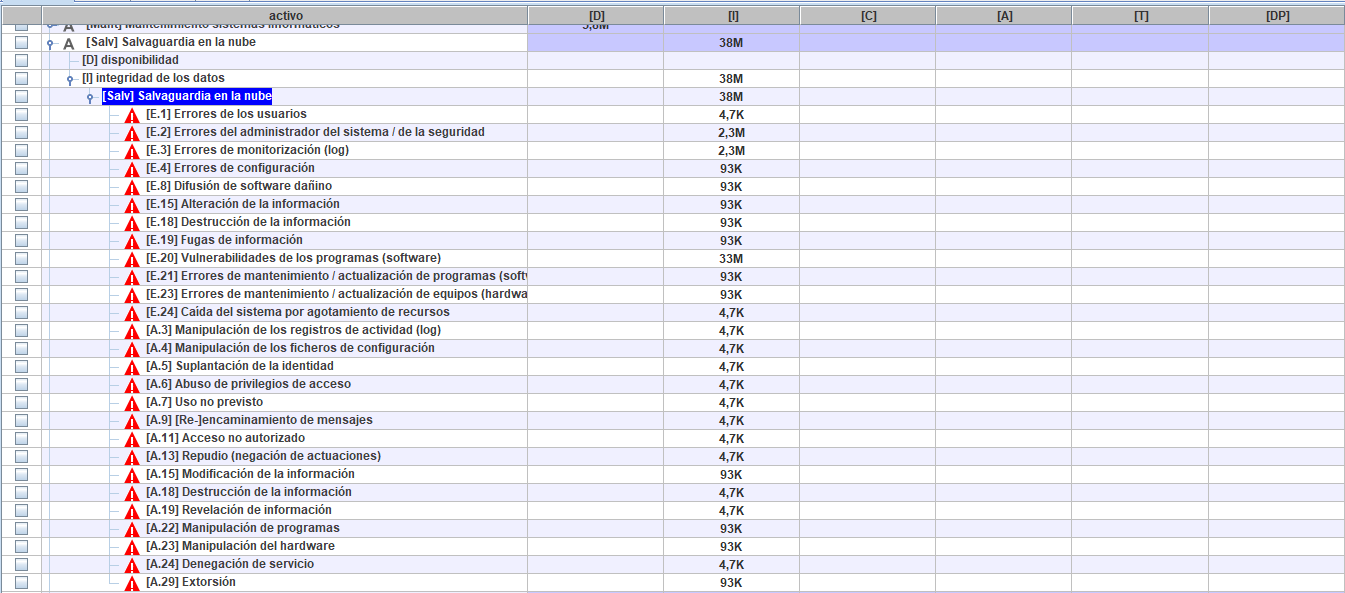
**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

****

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Varias empresas de distribución
  + Contratar un servicio externo para comprobar el correcto funcionamiento de la empresa
  + Ceder a cualquier petición de las empresas interesadas en un acuerdo.
* No justifica:
  + Al tener un único contrato en la empresa podemos abaratar costes en la empresas
  + Contratar un servicio externo para comprobar el correcto funcionamiento de la empresa ya que tenemos en la empresa personal cualificado para realizar esas funciones
  + Ceder a las peticiones de una empresa que perjudique a los productos de las demás empresas. ya que pueden ser peticiones que no beneficien a nuestra propia empresas
* Aplican y justifican:

○ Revisar periódicamente los contratos con los distribuidores

○ Tener cierto control con el personal externo de la empresa

○ Realizar charlas y seminarios de concienciación con la seguridad de la información.

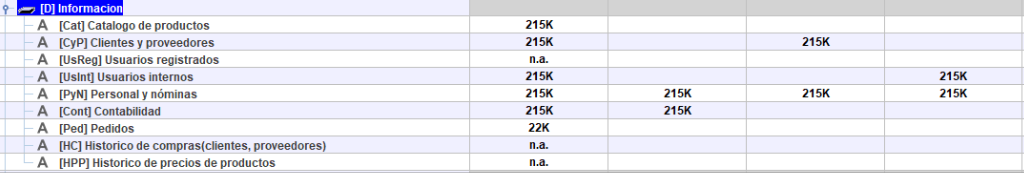
○ Conseguir que el personal externo subcontratado tenga la mejor formación posible

#### **3.D Información**

**Activos:** Catálogo de productos, clientes y proveedores, usuarios registrados, usuarios internos, personal y nóminas, contabilidad, pedidos, histórico de compras (clientes, proveedores), e histórico de precios de productos.

**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**



**Amenazas:**

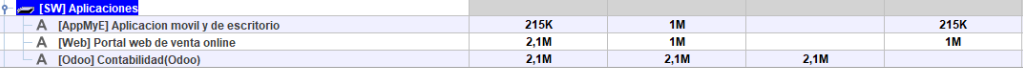
Este activo no tiene ninguna amenaza asociada

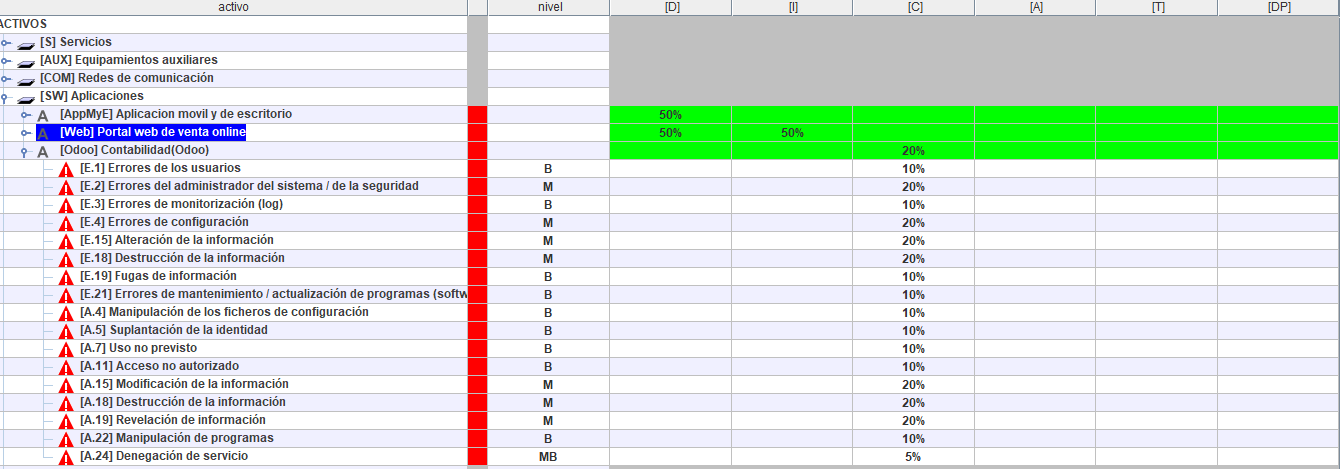
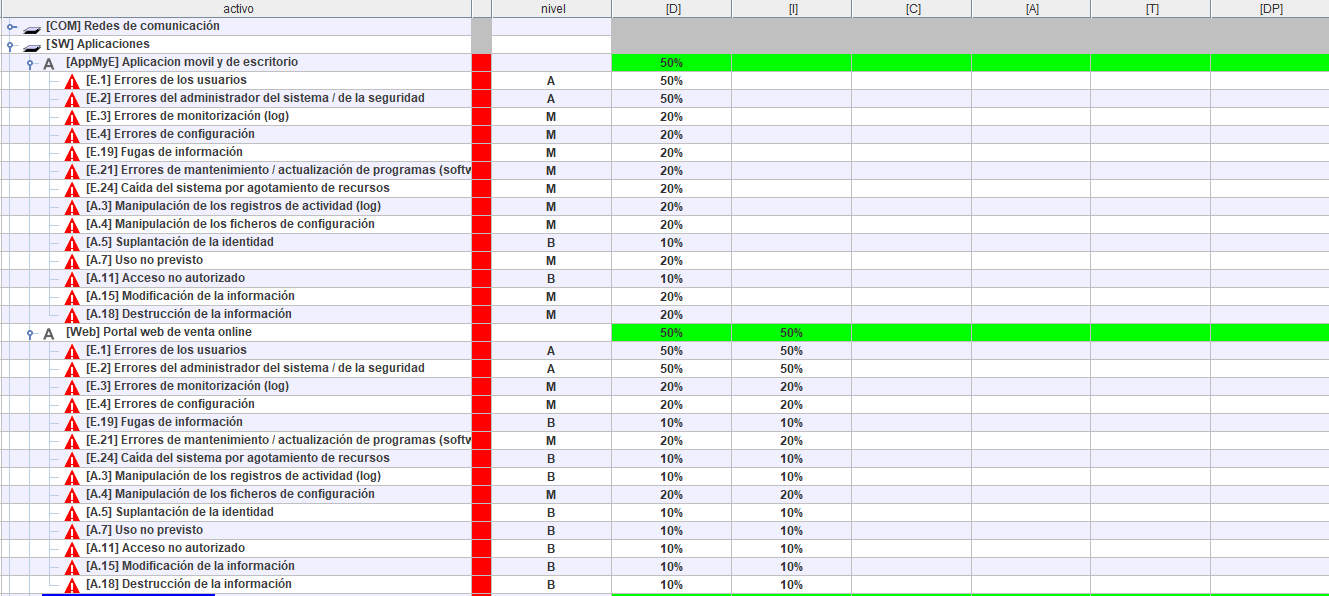
#### **4.SW Aplicaciones**

**Activos:** Aplicación móvil y de escritorio, portal web de venta online y contabilidad (Odoo).

**Dependencias entre activos:** Servidores WEB, PC, bases de datos, usuarios externos registrados, clientes, empleados, proveedores, administración

### **Valor de los activos**



**Amenazas producidas por PILAR:** 

**Amenazas:**

* Mala implementación
* Seguridad escasa
* Software no actualizado y poco mantenible
* Suplantación de la identidad

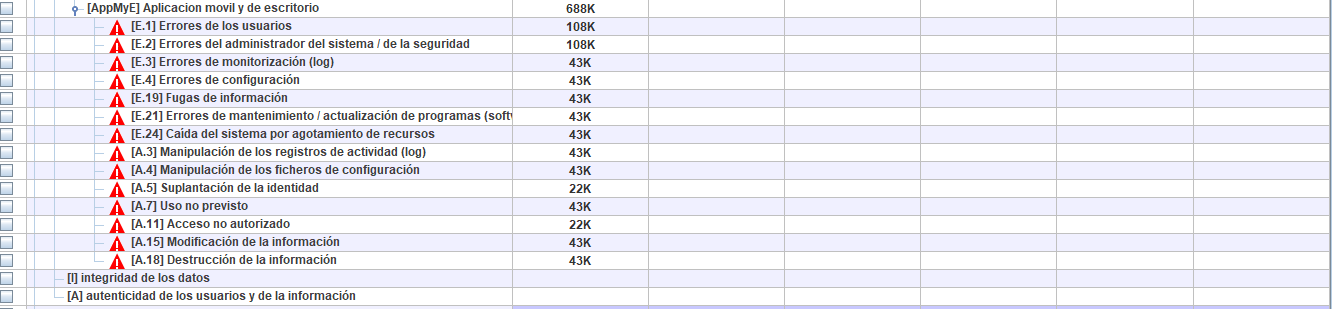
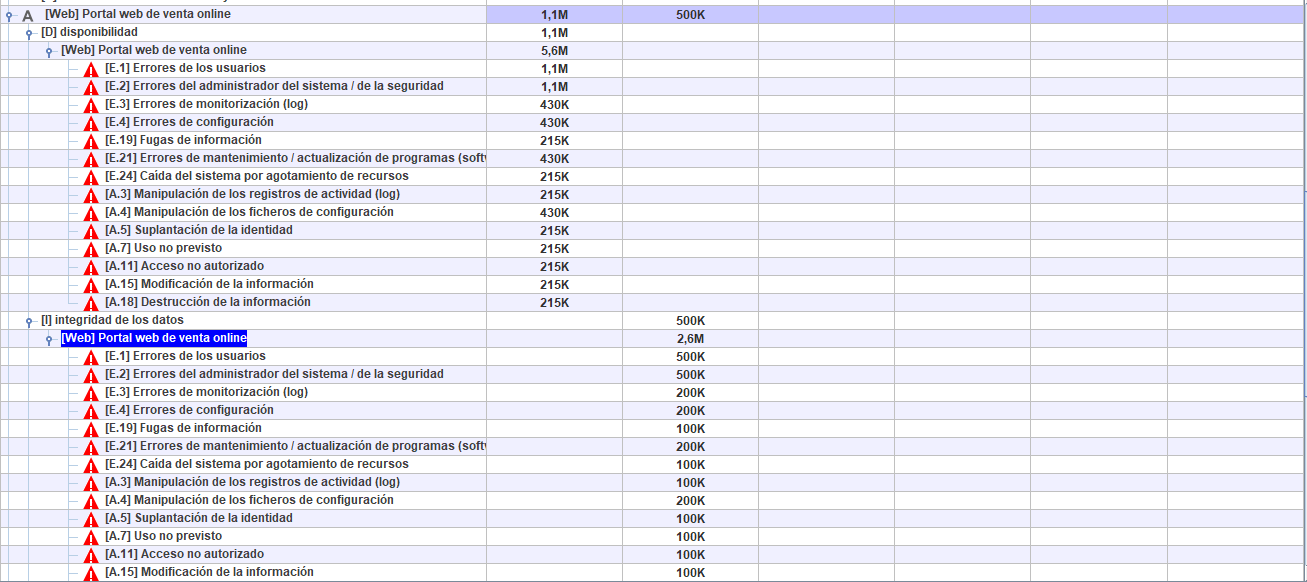
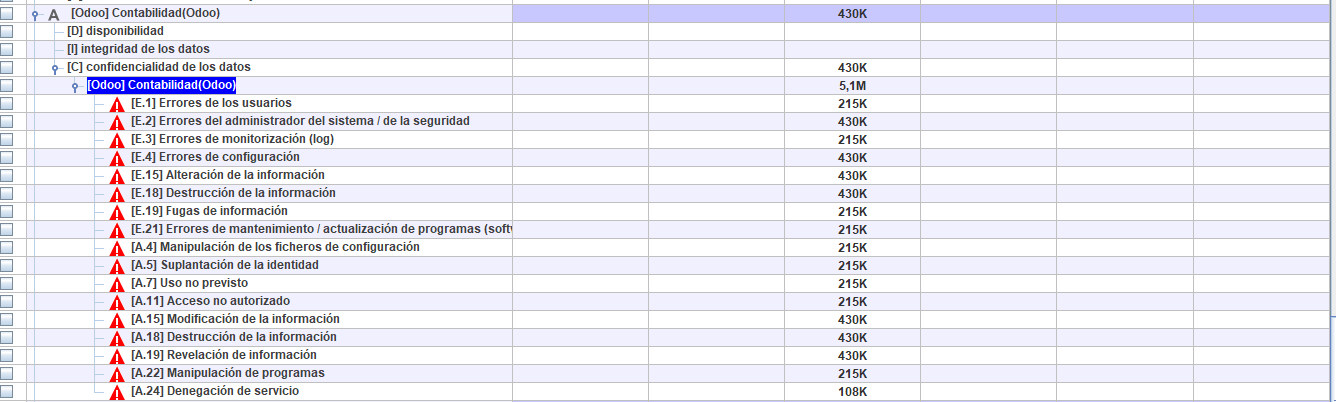
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, la empresa dejaría de tener la disponibilidad de dicho activo hasta que la amenaza se subsane, lo que deriva en la imposibilidad de trabajar y, por tanto, perder dinero.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Mala implementación | 1 | Normal | Una vez al año |
| Seguridad escasa | 1 | Normal | Una vez al año |
| Software no actualizado y poco mantenible | 1 | Normal | Una vez al año |
| Suplantación de la identidad | 100 | Muy frecuente | A diario |

**Impactos según PILAR:**



**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Aplicación móvil y de escritorio | Mala implementación | 100% | MA | MA |
| Aplicación móvil y de escritorio | Seguridad escasa | 100% | A | A |
| Aplicación móvil y de escritorio | Software no actualizado y poco mantenible | 50% | B | MB |
| Portal web de venta online | Mala implementación | 100% | MA | MA |
| Portal web de venta online | Seguridad escasa | 80% | A | A |
| Porta web de venta online | Software no actualizado y poco mantenible | 50% | M | B |
| Contabilidad (Odoo) | Suplantación de la identidad | 50% | B | MB |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

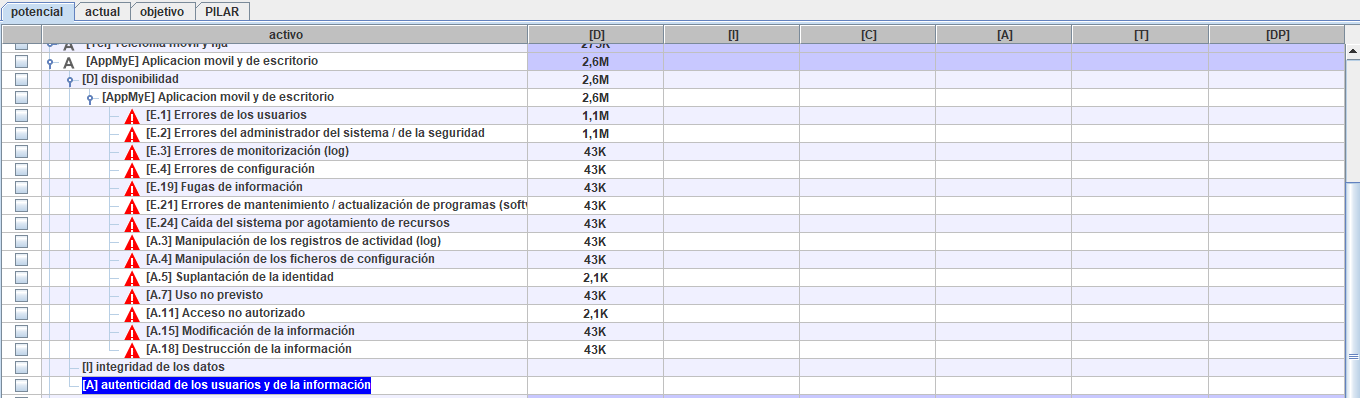
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

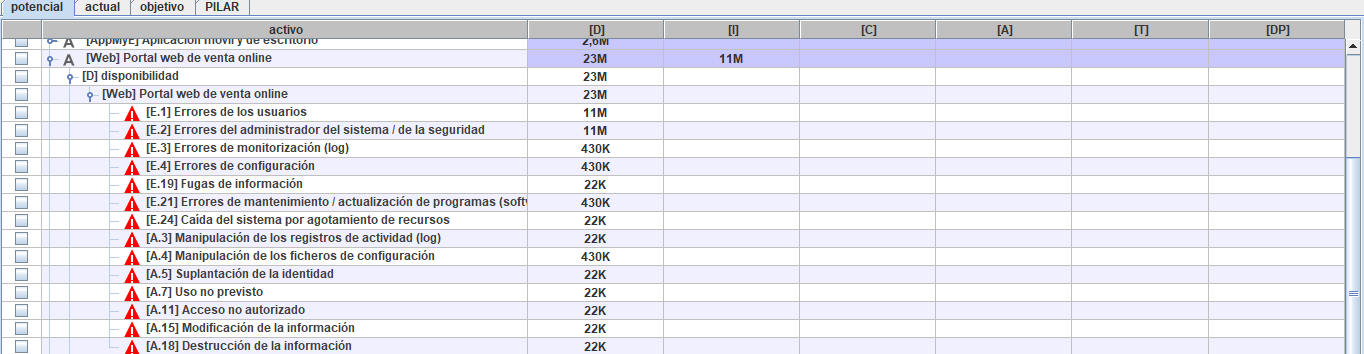
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Aplicación móvil y de escritorio | Mala implementación | 1 | MA | MA |
| Aplicación móvil y de escritorio | Seguridad escasa | 1 | A | A |
| Aplicación móvil y de escritorio | Software no actualizado y poco mantenible | 1 | MB | MB |
| Portal web de venta online | Mala implementación | 1 | MA | MA |
| Portal web de venta online | Seguridad escasa | 1 | A | A |
| Porta web de venta online | Software no actualizado y poco mantenible | 1 | M | B |
| Contabilidad (Odoo) | Suplantación de la identidad | 100 | B | M |

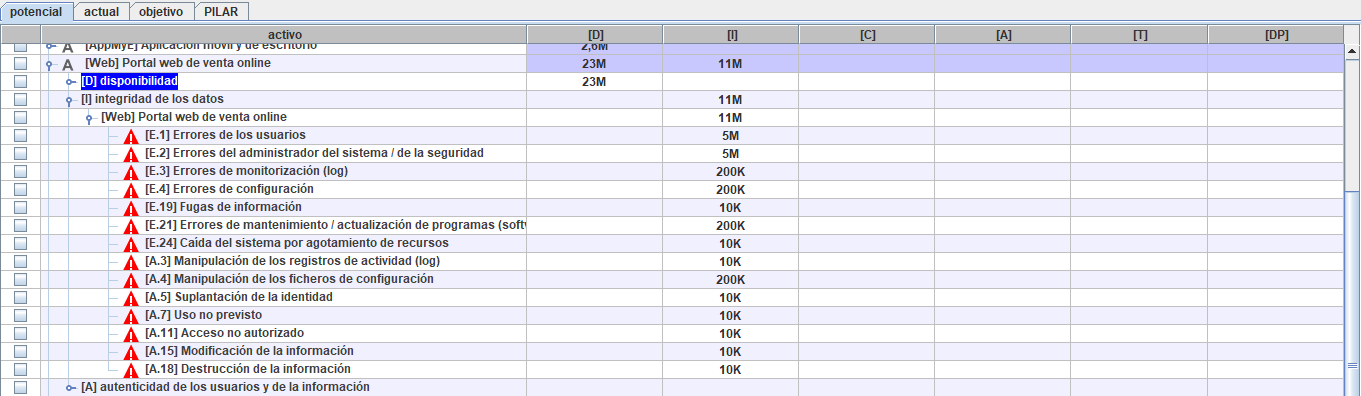
**Riesgo potencial:**

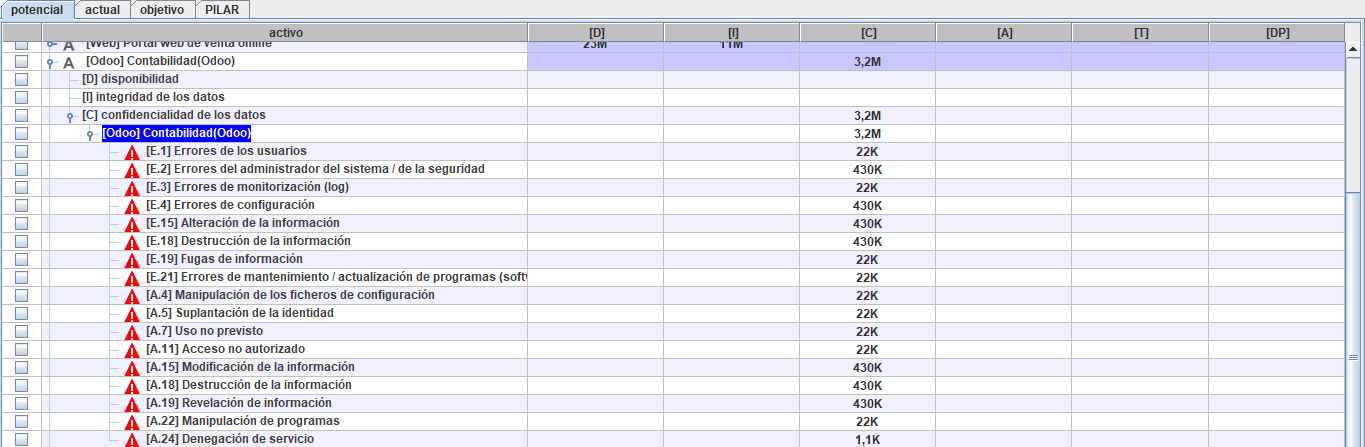
Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

****

****

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Tener las aplicaciones móviles para una única plataforma
  + Tener las aplicaciones de escritorio para un único sistema operativo
  + Desaprovechar los medios disponibles para llevar a cabo la contabilidad
* No justifica:
  + Tener una aplicación para un único sistema operativo ya que no podríamos tener la mayor cantidad de clientes
  + Existen muchos medios actualmente para facilitar la gestión de la contabilidad
* Aplican y justifican:

○ Diseñar nuestras aplicaciones para distintos sistemas operativos

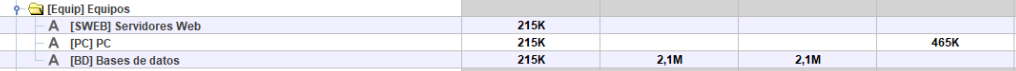
○ Utilizar las herramientas adecuada para la gestión de la contabilidad

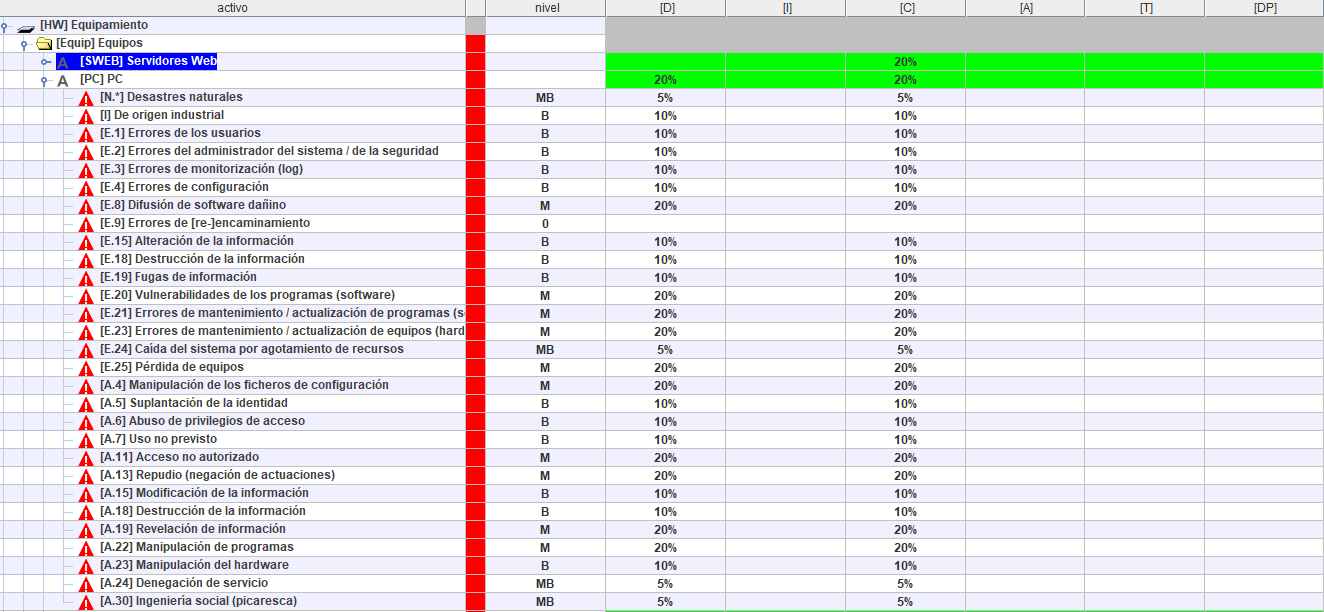
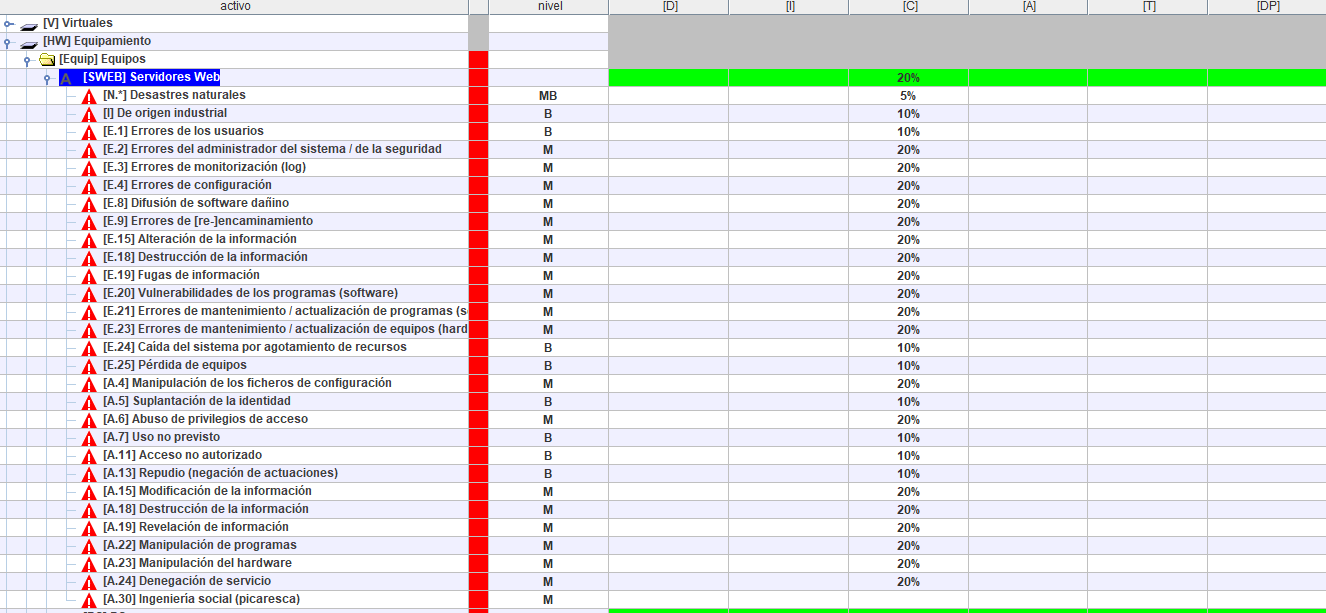
#### **5.1 Equipos**

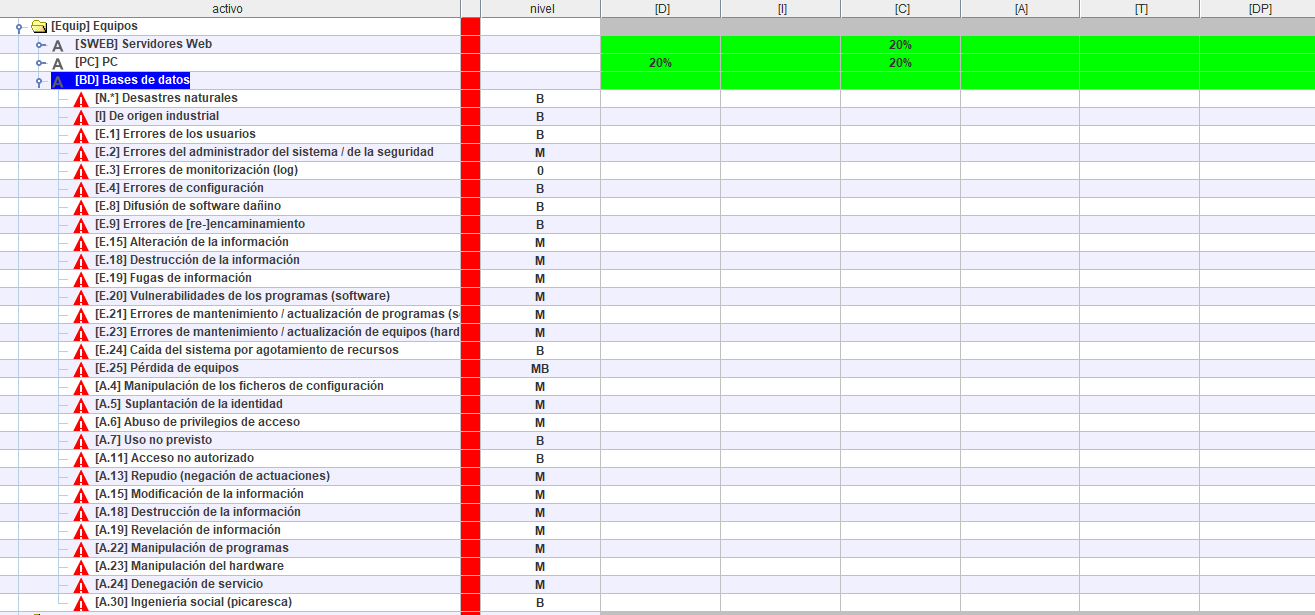
**Activos:** Servidores web, PC y bases de datos.

**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**

**Amenazas producidas por PILAR**

****



**Amenazas:**

* Gestión errónea de los equipos
* Fuga de información
* Ataques deliberados
* Robo o pérdida de equipos

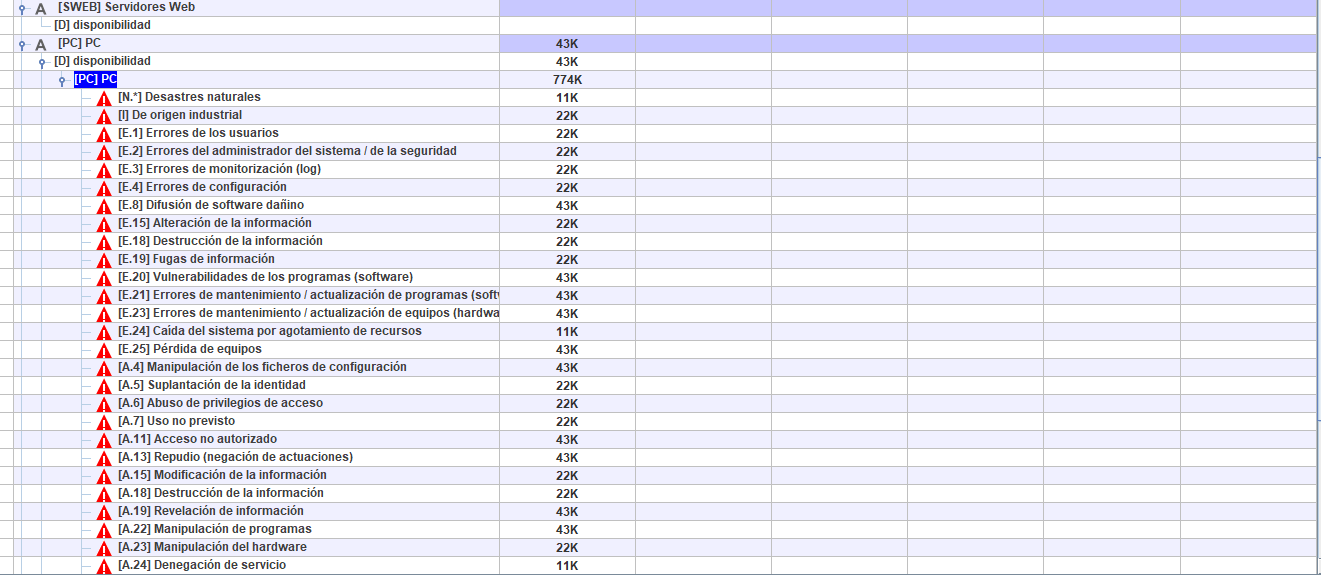
**Degradación:**

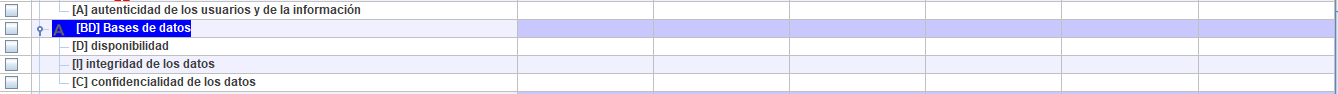
En caso de materializarse alguna de las amenazas anteriores, la empresa dejaría de tener la disponibilidad de dicho activo hasta que la amenaza se subsane, lo que deriva en la imposibilidad de trabajar y, por tanto, perder dinero. También puede derivar esta materialización de las amenazas en problemas legales, al haber una brecha en la seguridad de la información.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Gestión errónea de los equipos | 1 | Normal | Una vez al año |
| Fuga de información | 1/10 | Poco frecuente | Cada varios años |
| Ataques deliberados | 10 | Frecuente | Mensualmente |
| Robo o pérdida de equipos | 1 | Normal | Una vez al año |

**Impactos según PILAR:**





**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Servidores web | Fuga de información | 1% | B | MB |
| Servidores web | Ataques deliberados | 95% | A | A |
| PC | Gestión errónea de los equipos | 90% | M | M |
| PC | Fuga de información | 1% | B | MB |
| PC | Ataques deliberados | 80% | A | A |
| PC | Robo o pérdida de equipos | 100% | MA | MA |
| Bases de datos | Fuga de información | 1% | B | MB |
| Bases de datos | Ataques deliberados | 80% | A | A |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

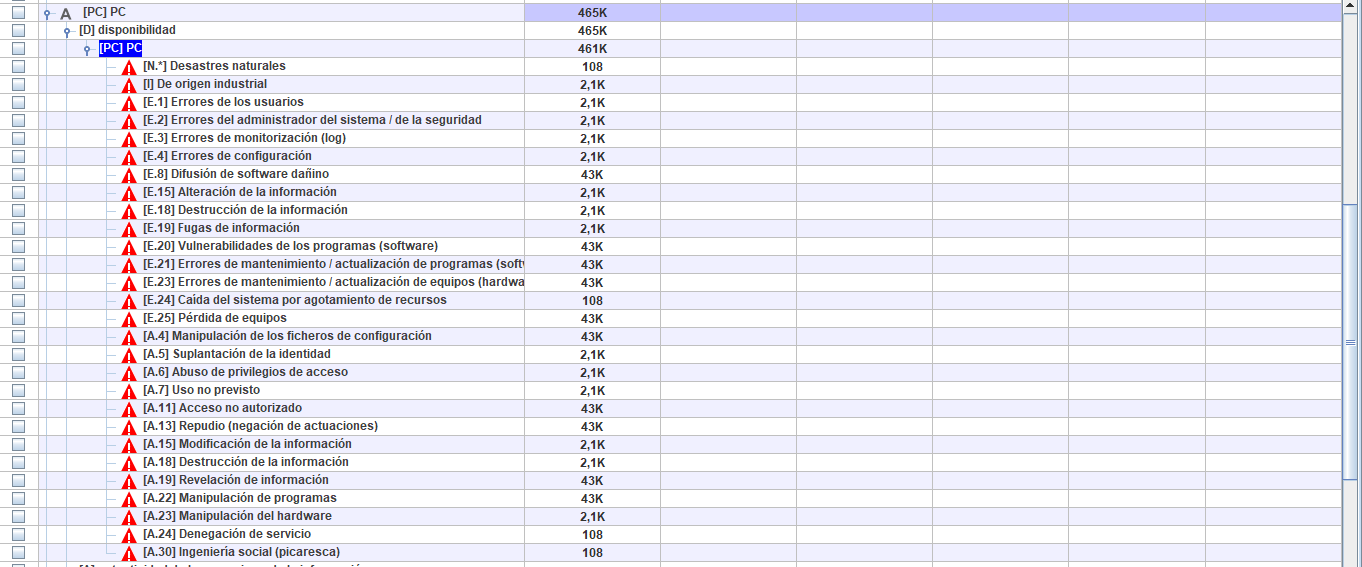
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Servidores web | Fuga de información | 1/10 | MB | MB |
| Servidores web | Ataques deliberados | 10 | A | MA |
| PC | Gestión errónea de los equipos | 1 | M | M |
| PC | Fuga de información | 1/10 | MB | MB |
| PC | Ataques deliberados | 10 | A | MA |
| PC | Robo o pérdida de equipos | 1 | MA | A |
| Bases de datos | Fuga de información | 1/10 | MB | MB |
| Bases de datos | Ataques deliberados | 10 | A | MA |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Tener equipos desactualizados
  + Renovar los equipos con demasiada frecuencia ej: 1 mes
* No justifica:
  + Tener equipos desactualizados porque puede haber problemas con las vulnerabilidades
  + Renovar los equipos con demasiada frecuencia ya que puede suponer un coste muy alto para la empresa
* Aplican y justifican:

○ Tener actualizadas las versiones de los equipos

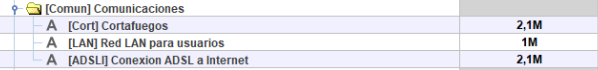
○ Utilizar las herramientas adecuada para la gestión de la contabilidad

#### **5.2 Comunicaciones**

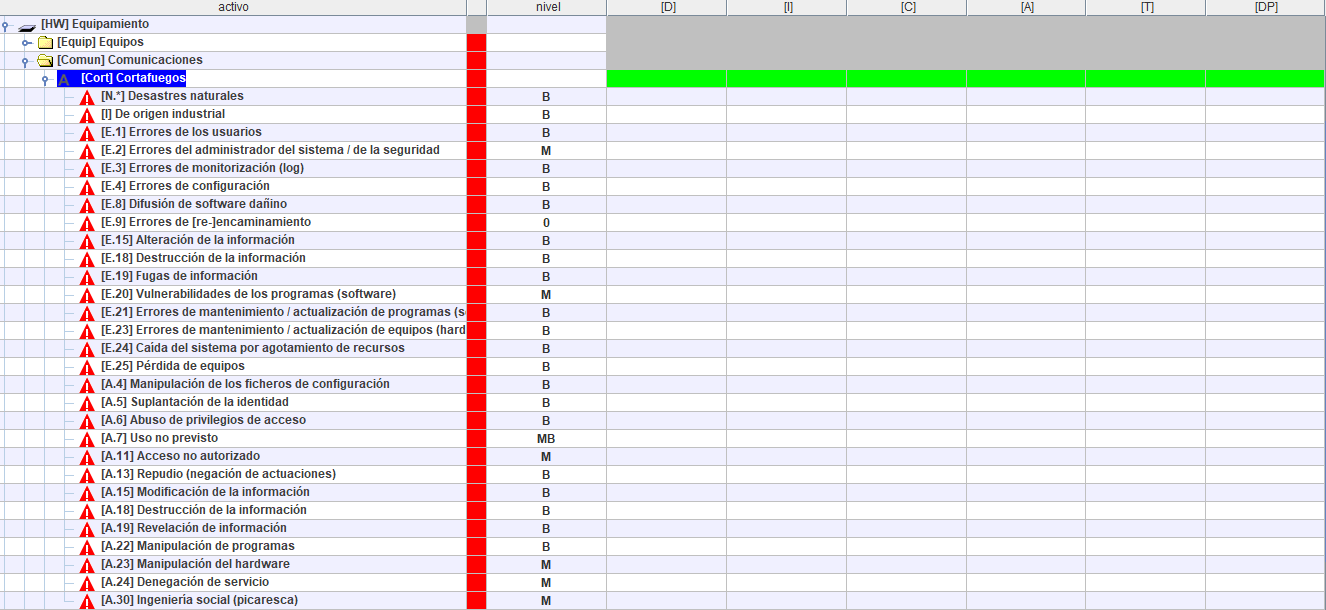
**Activos:** Cortafuegos, red LAN para usuarios y conexión ADSL a Internet.

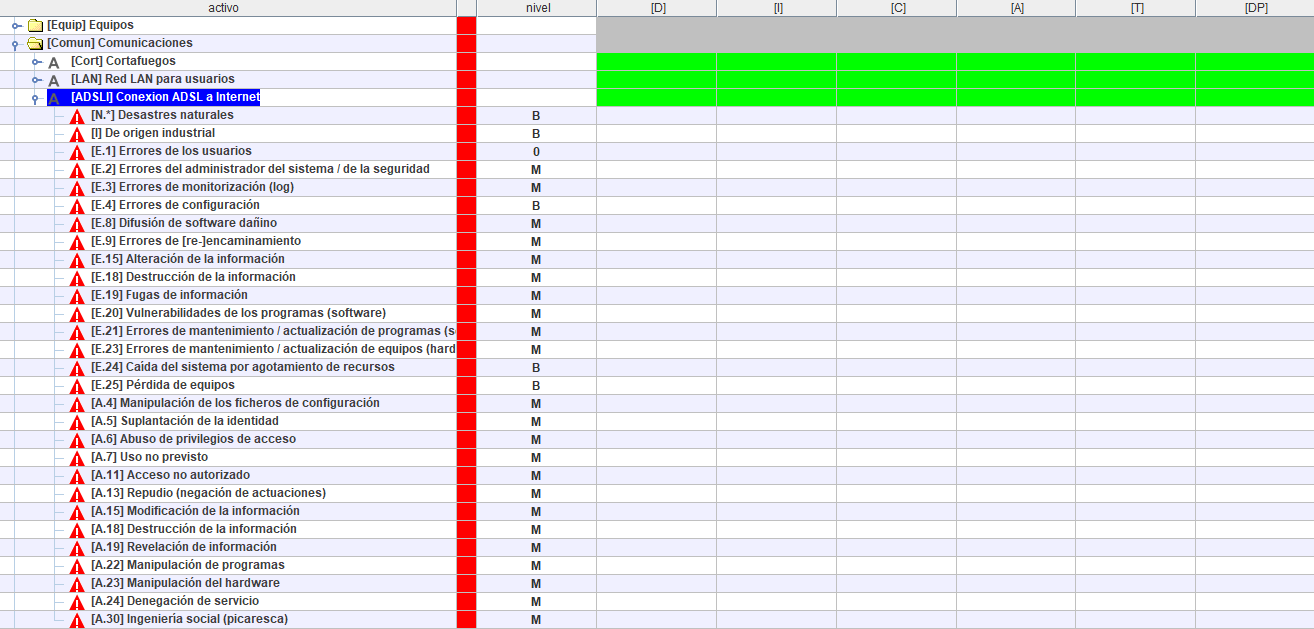
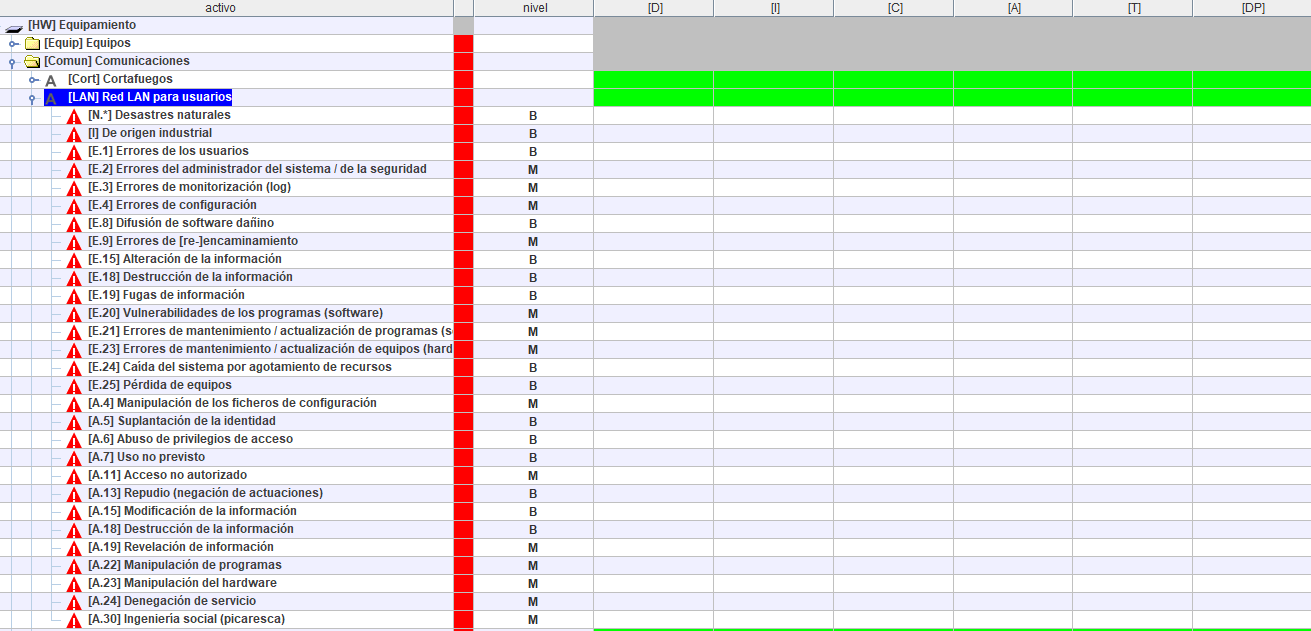
**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**



**Amenazas producidas por PILAR:**





**Amenazas:**

* Corte de suministro
* Ataques a la red

**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, retrasaría la producción de la empresa y podría suponer una brecha en la seguridad, derivando en una pérdida de dinero y problemas legales.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Corte de suministro | 1 | Normal | Una vez al año |
| Ataques a la red | 10 | Frecuente | Mensualmente |

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Cortafuegos | Corte de suministro | 50% | MB | MB |
| Red LAN | Corte de suministro | 1% | A | B |
| Red LAN | Ataques a la red | 100% | MA | MA |
| Conexión ADSL a Internet | Corte de suministro | 1% | A | B |
| Conexión ADSL a Internet | Ataques a la red | 100% | MA | MA |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Cortafuegos | Corte de suministro | 1 | MB | MB |
| Red LAN | Corte de suministro | 1 | B | B |
| Red LAN | Ataques a la red | 10 | MA | MA |
| Conexión ADSL a Internet | Corte de suministro | 1 | B | B |
| Conexión ADSL a Internet | Ataques a la red | 10 | MA | MA |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR:** no tiene.

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Poner unas reglas muy estrictas en firewall que solo permiten acceder a los servicios si se accede desde un ISP conocido
  + Vigilar a diario el sitio en el que se encuentran los switches, routers y dispositivos NAS para que nadie choque con ellos y se produzca una caída o pisotón de dichos activos.
* No justifica:
  + Solamente permitir el acceso a los servicios a los usuarios que se encuentren registrados con datos personales verificados.
  + Prohibir acercarse a los switches, routers y dispositivos NAS.
* Aplican y justifican:
  + Configurar el firewall correctamente y valorar la implantación de herramientas que logren mitigar ataque de denegación de servicio o que detecten comportamiento anómalo
  + Situar los routers, switches y dispositivos NAS en un lugar seguro, fuera del alcance de los trabajadores.
  + Controlar el número de peticiones que realiza cada usuario y corregir las vulnerabilidades del servicio para prevenir un ataque DDoS.

#### **5.3 Equipos auxiliares**

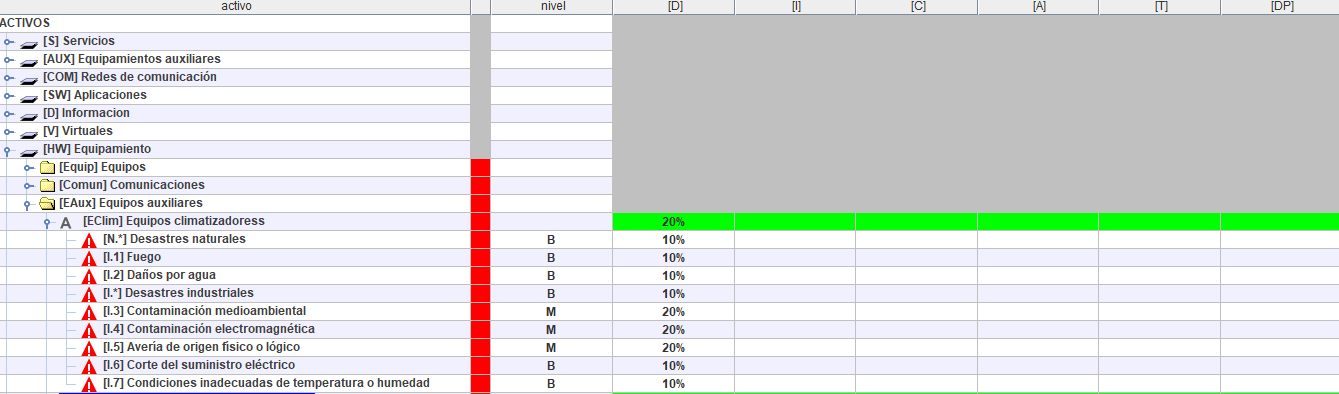
**Activos:** Equipos climatizadores y detección y extinción de incendios.

**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**



**Amenazas producidas por PILAR:**



**Amenazas:**

* Fallo en el funcionamiento en los equipos

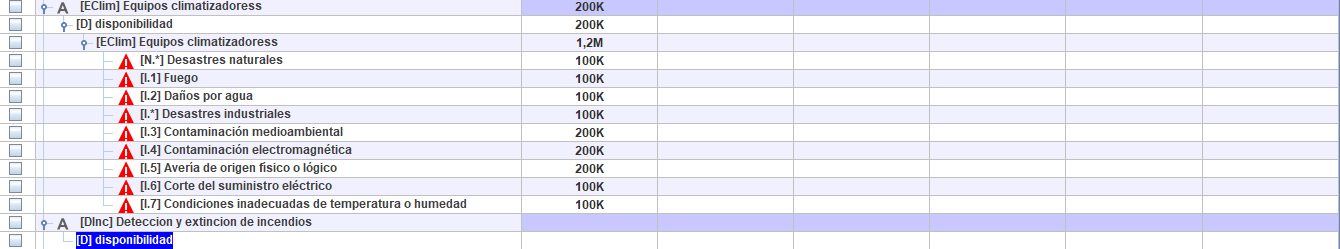
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, pueden devastar totalmente muchos de los otros activos de la empresa, derivando en una gran pérdida del capital.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Fallo en el funcionamiento en los equipos | 10 | Frecuente | Mensualmente |

**Impactos según PILAR:**



**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Equipos climatizadores | Fallo en el funcionamiento en los equipos | 100% | A | A |
| Detección y extinción de incendios | Fallo en el funcionamiento en los equipos | 100% | A | A |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

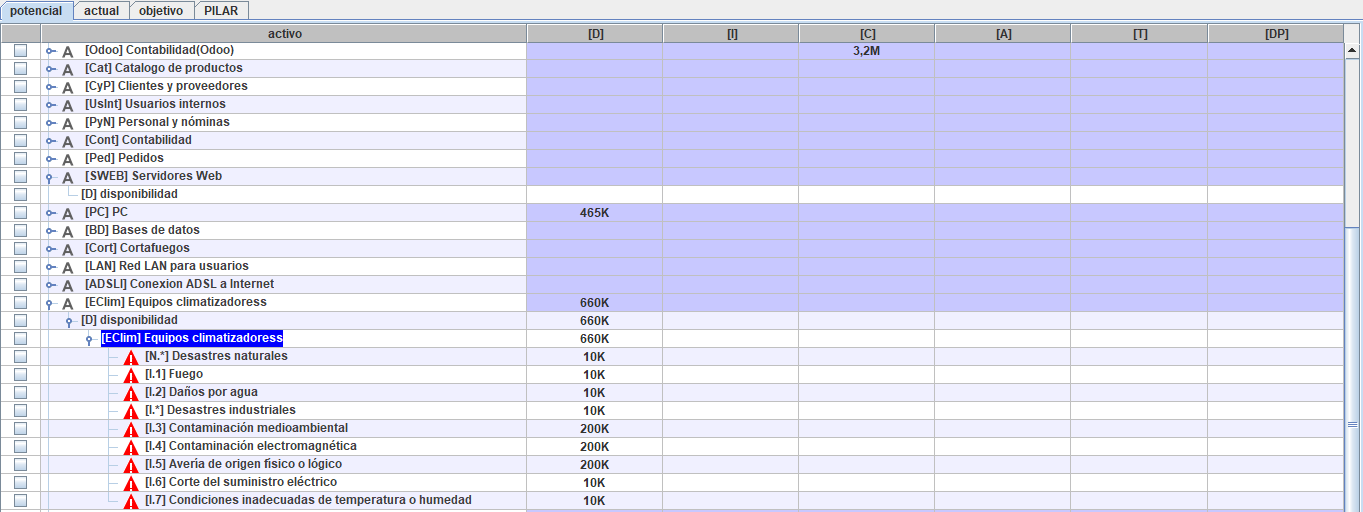
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Equipos climatizadores | Fallo en el funcionamiento en los equipos | 10 | A | MA |
| Detección y extinción de incendios | Fallo en el funcionamiento en los equipos | 10 | A | MA |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Tener varios técnicos que realicen las mismas funciones en cuanto a los equipos climatizadores y de detección de incendios
* No justifica:
  + No tener personal de más, pues sería innecesario, y que sea altamente cualificado.
* Aplican y justifican:
  + Tener equipos de climatización de repuesto

#### **6. Redes de comunicación**

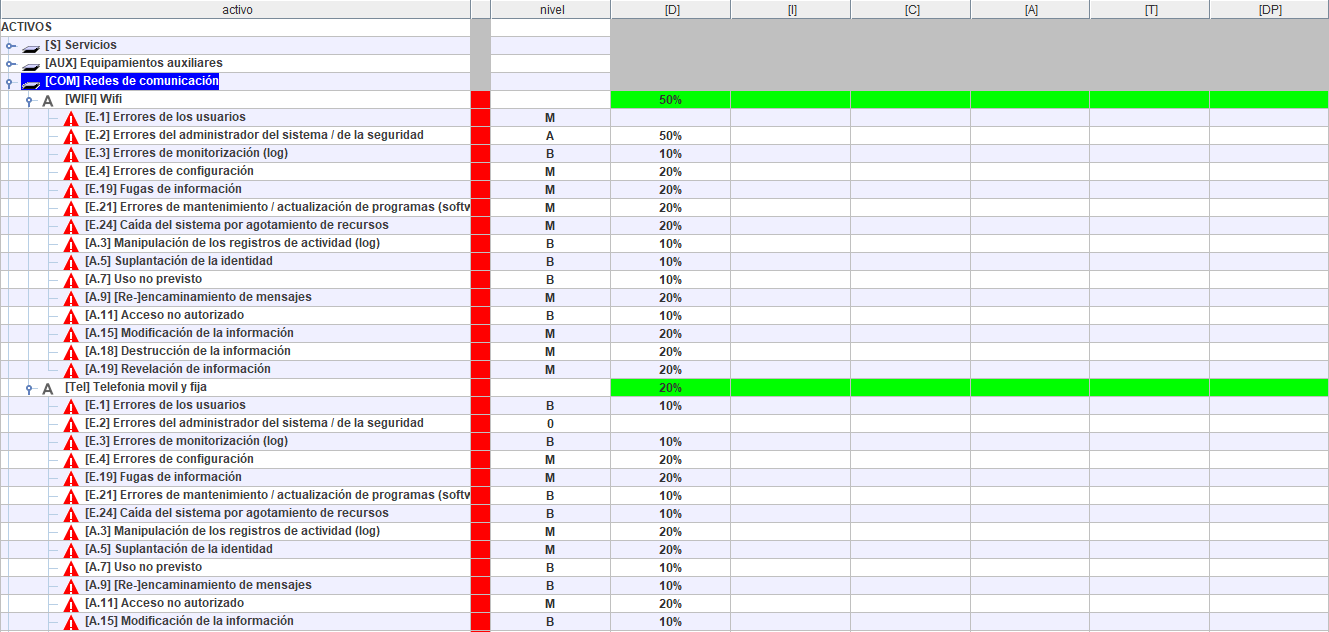
**Activos:** Wifi y telefonía móvil y fija.

**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**

****

**Amenazas producidas por PILAR:**

****

**Amenazas:**

* Corte en el suministro
* Errores de configuración
* Fugas de información
* Ataques deliberados

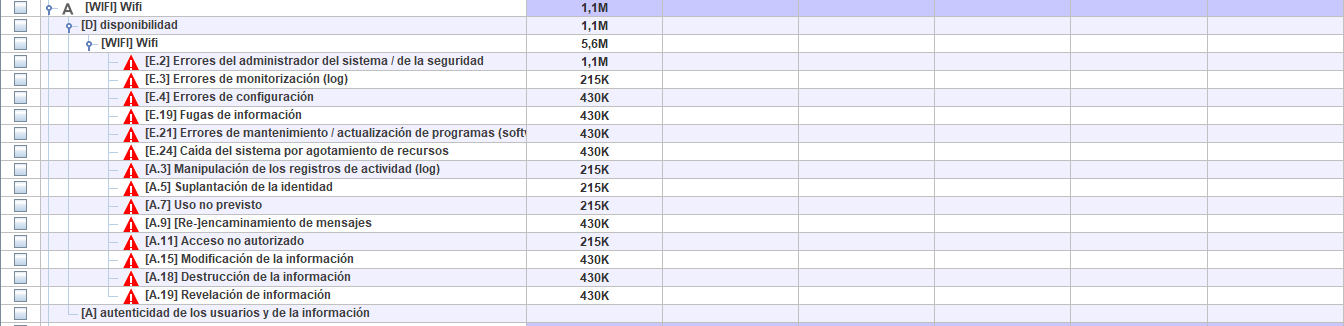
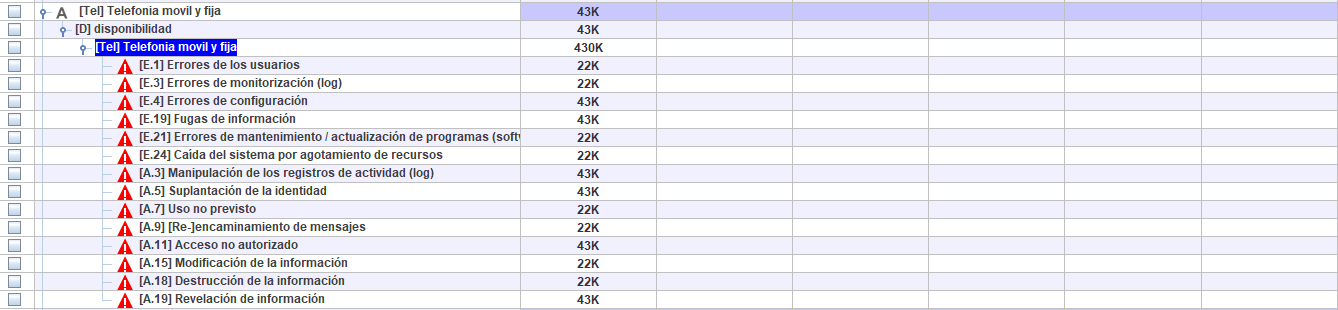
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, retrasaría la producción de la empresa y, por tanto, pérdida de dinero.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Corte en el suministro | 1 | Normal | Una vez al año |
| Errores de configuración | 1 | Normal | Una vez al año |
| Fugas de información | 1 | Normal | Una vez al año |
| Ataques deliberados | 10 | Frecuente | Mensualmente |

**Impactos según PILAR:**

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Wifi | Corte en el suministro | 1% | M | MB |
| Wifi | Errores de configuración | 50% | B | MB |
| Wifi | Ataques deliberados | 100% | A | MA |
| Telefonía móvil y fija | Corte en el suministro | 100% | M | M |
| Telefonía móvil y fija | Fugas de información | 1% | MB | MB |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

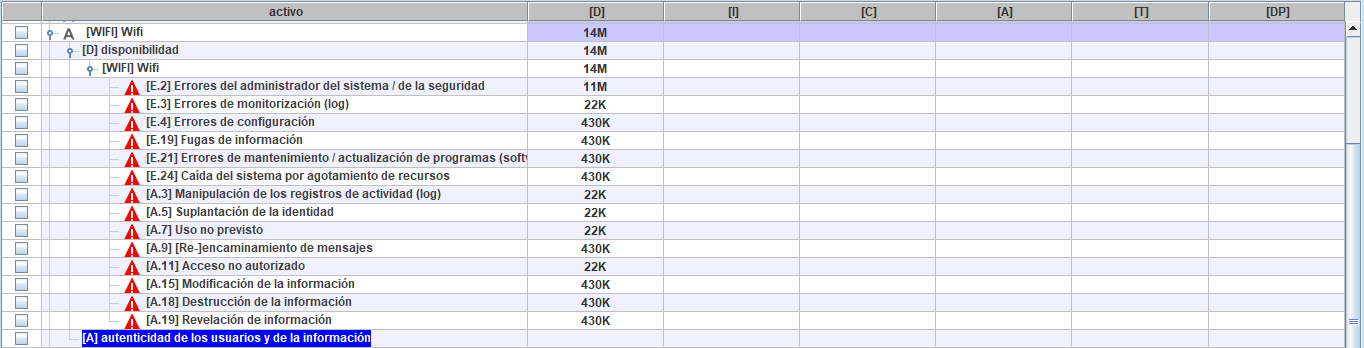
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

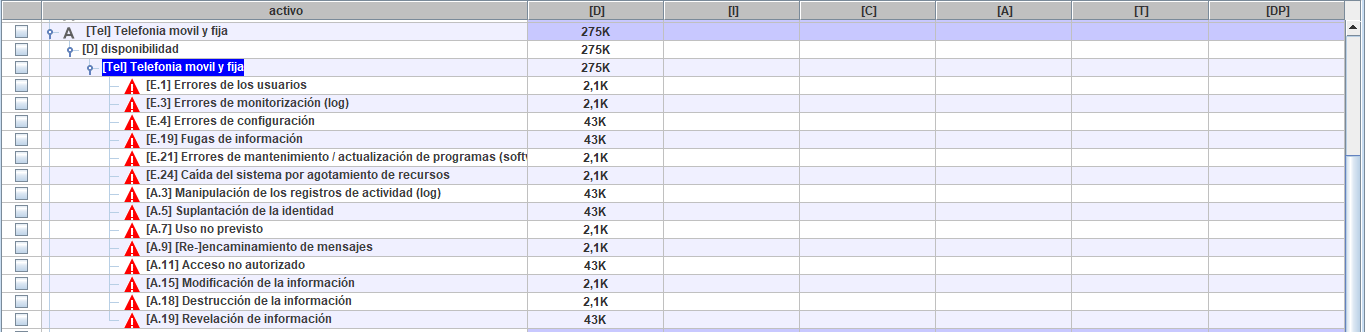
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Wifi | Corte en el suministro | 1 | MB | MB |
| Wifi | Errores de configuración | 1 | MB | MB |
| Wifi | Ataques deliberados | 10 | MA | MA |
| Telefonía móvil y fija | Corte en el suministro | 1 | M | M |
| Telefonía móvil y fija | Fugas de información | 1 | MB | MB |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR:** no tiene





**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

* No aplica:
  + Tener un algoritmo sofisticado que actualice la contraseña del wifi cada poco tiempo, por ejemplo, cada día.
  + Cambiar el teléfono móvil de cada miembro de la empresa en el momento en el que salga un nuevo terminal.
* No justifica:
  + Conseguir ese algoritmo sería muy caro y resultaría inutil
  + Cambiar el terminal de cada empleado supondría un coste muy elevado e innecesario.
* Aplican y justifican:
  + Tener revisiones periódicas y comprobar que la red es segura
  + Limitar los terminales de los empleados para que su única utilidad pueda ser en torno a funciones de la empresa y mejorar su vida útil.

#### **7 Equipamientos auxiliares**

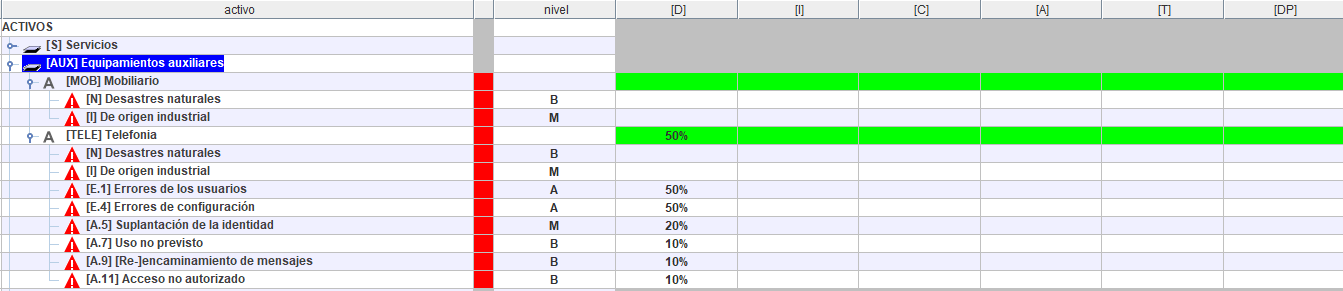
**Activos:** Mobiliario y telefonía.

**Dependencias entre activos:** no tiene activos que dependan.

### **Valor de los activos**



**Amenazas producidas por PILAR:**



**Amenazas:**

* Pérdida del equipamiento

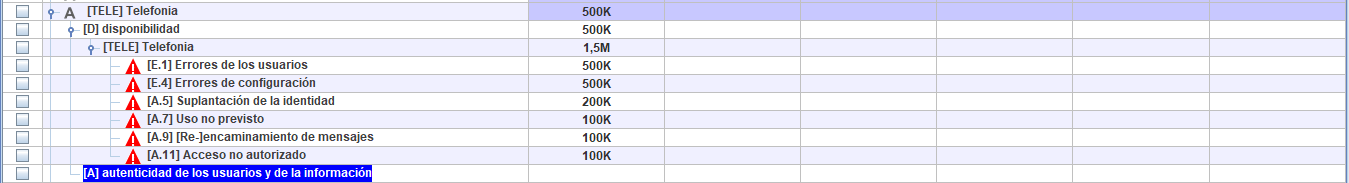
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, supondría restaurar el equipamiento.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Pérdida del equipamiento | 10 | Frecuente | Mensualmente |

**Impactos según PILAR:**

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Mobiliario | Pérdida del equipamiento | 100% | M | M |
| Telefonía | Pérdida del equipamiento | 100% | A | A |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

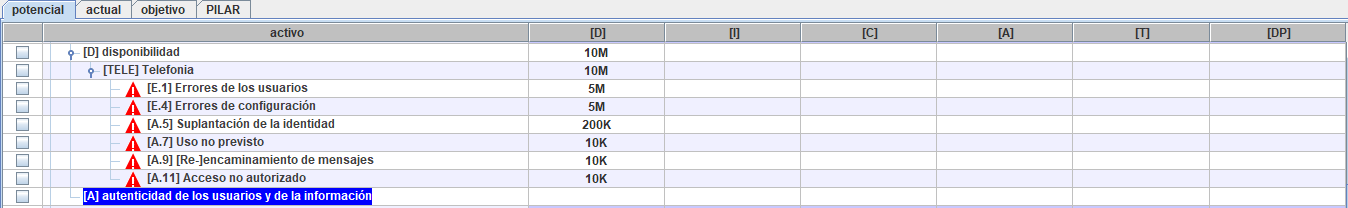
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Mobiliario | Pérdida del equipamiento | 10 | M | A |
| Telefonía | Pérdida del equipamiento | 10 | A | MA |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

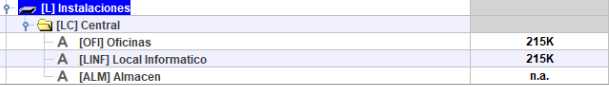
* No aplica:
  + Reemplazar de manera innecesaria el mobiliario por el hecho de reemplazar el mobiliario y punto
* No justifica:
  + Sería un gasto muy innecesario de dinero
* Aplican y justifican:
  + Reemplazar el mobiliario cuando deje de estar disponible y concienciar a los empleados de su buen uso y cuidado.

#### **8.1 Instalaciones**

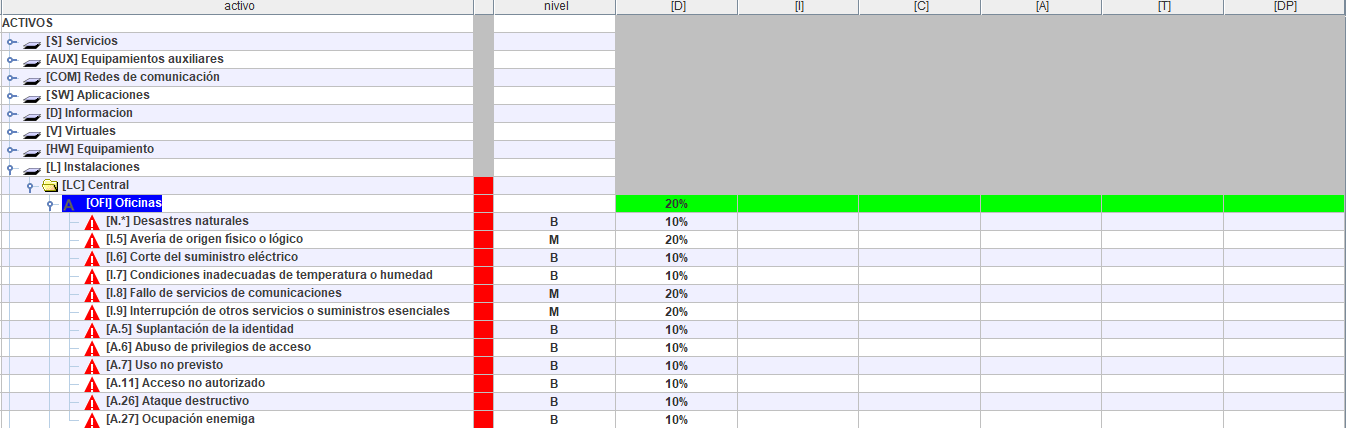
**Activos:** Oficinas, local informático y almacén.

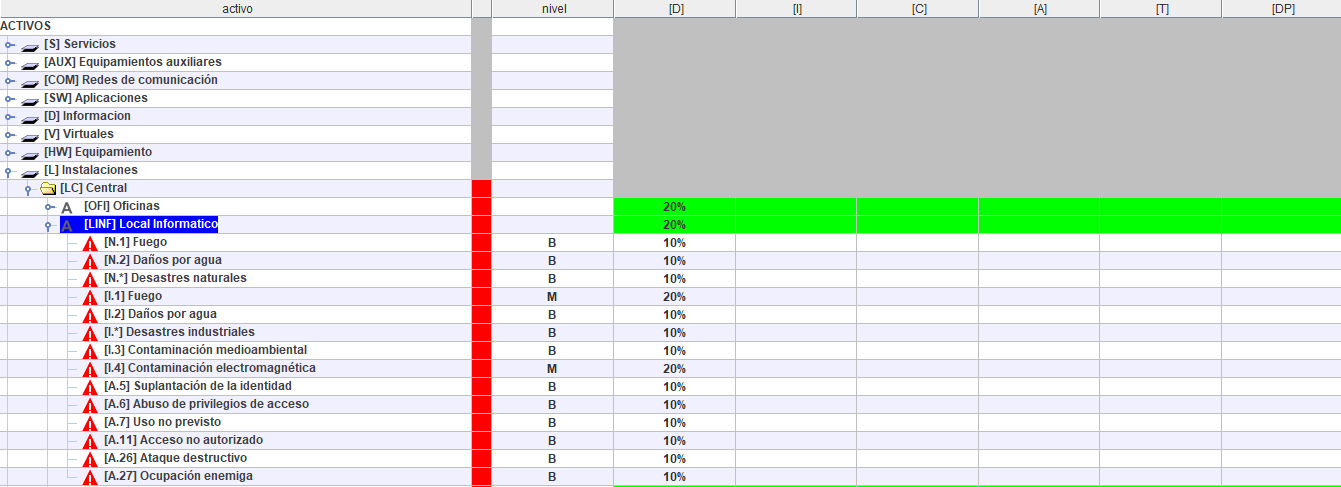
**Dependencias entre activos:** Equipos, comunicaciones, equipos auxiliares, empleados, administración.

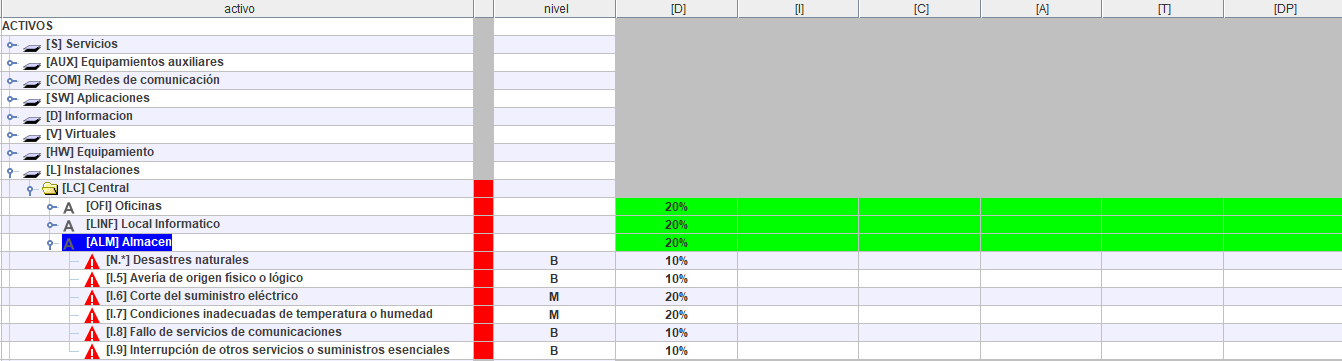
### **Valor de los activos**



**Amenazas producidas por PILAR:**







**Amenazas:**

* Ocupación enemiga
* Cortes en los suministros
* Acceso no autorizado

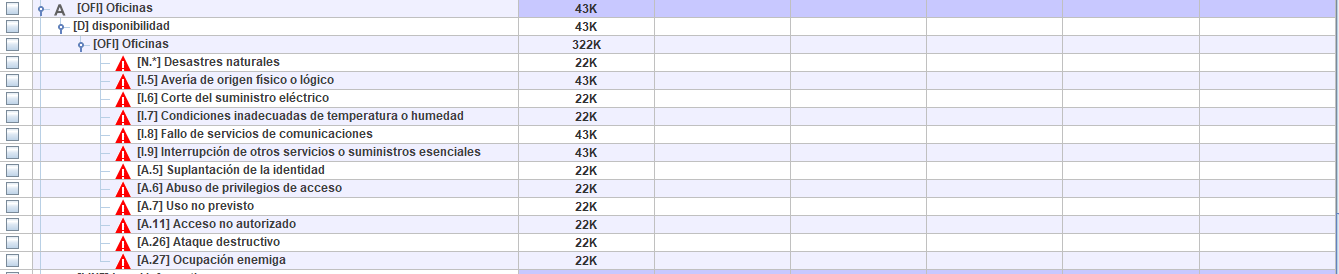
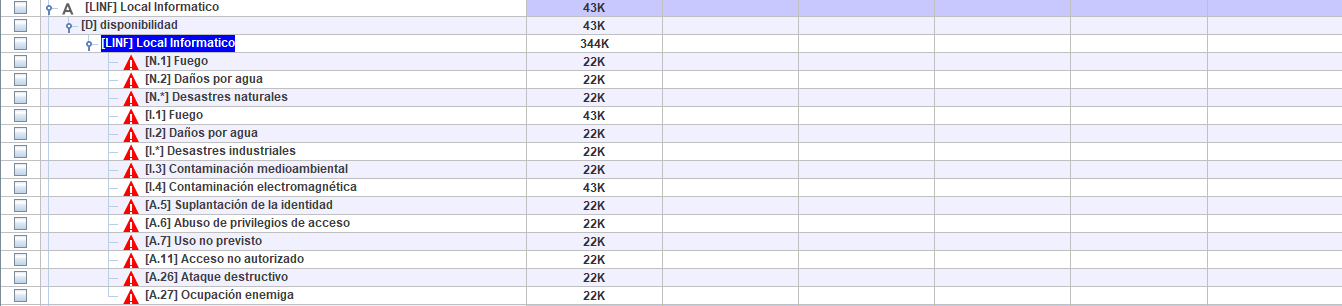
**Degradación:**

En caso de materializarse alguna de las amenazas anteriores, podría derivar en daños materiales y personales muy graves, comprometiendo a integridad de la empresa.

**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Ocupación enemiga | 1 | Normal | Una vez al año |
| Cortes en los suministros | 10 | Frecuente | Mensualmente |
| Acceso no autorizado | 10 | Frecuente | Mensualmente |

**Impactos según PILAR:**

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Oficina | Ocupación enemiga | 1% | M | MB |
| Oficina | Corte en los suministros | 10% | B | MB |
| Oficina | Acceso no autorizado | 80% | A | A |
| Local informático | Ocupación enemiga | 1% | M | MB |
| Local informático | Cortes en los suministros | 10% | B | MB |
| Local informático | Acceso no autorizado | 80% | A | A |
| Almacén | Ocupación enemiga | 1% | M | MB |
| Almacén | Corte en los suministros | 10% | B | MB |
| Almacén | Acceso no autorizado | 80% | A | A |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

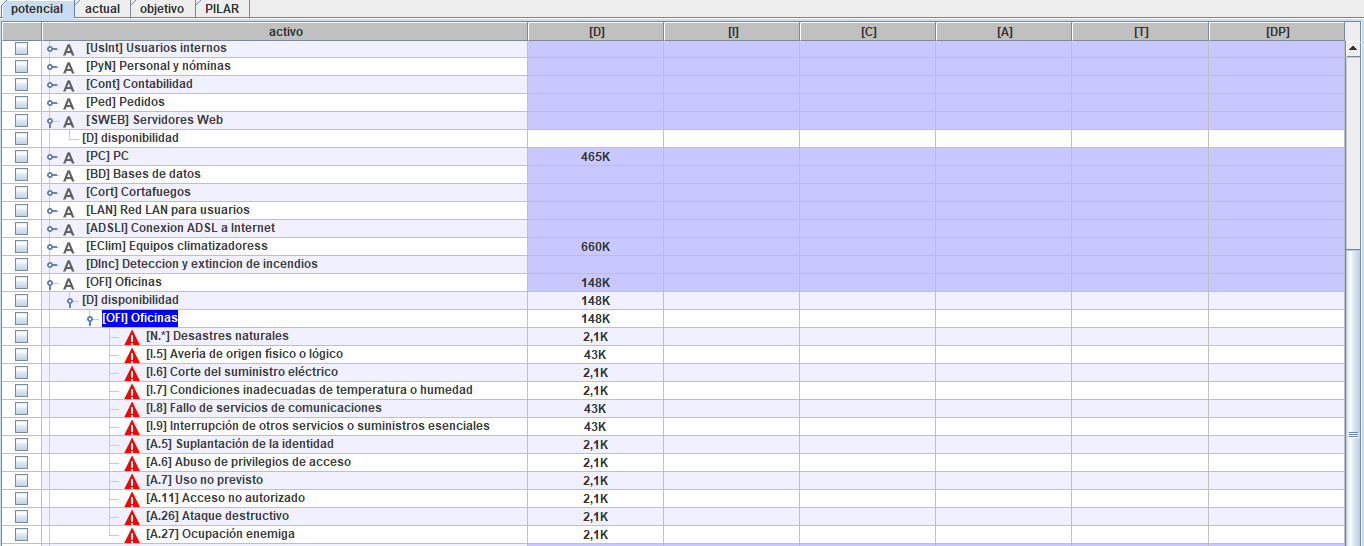
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

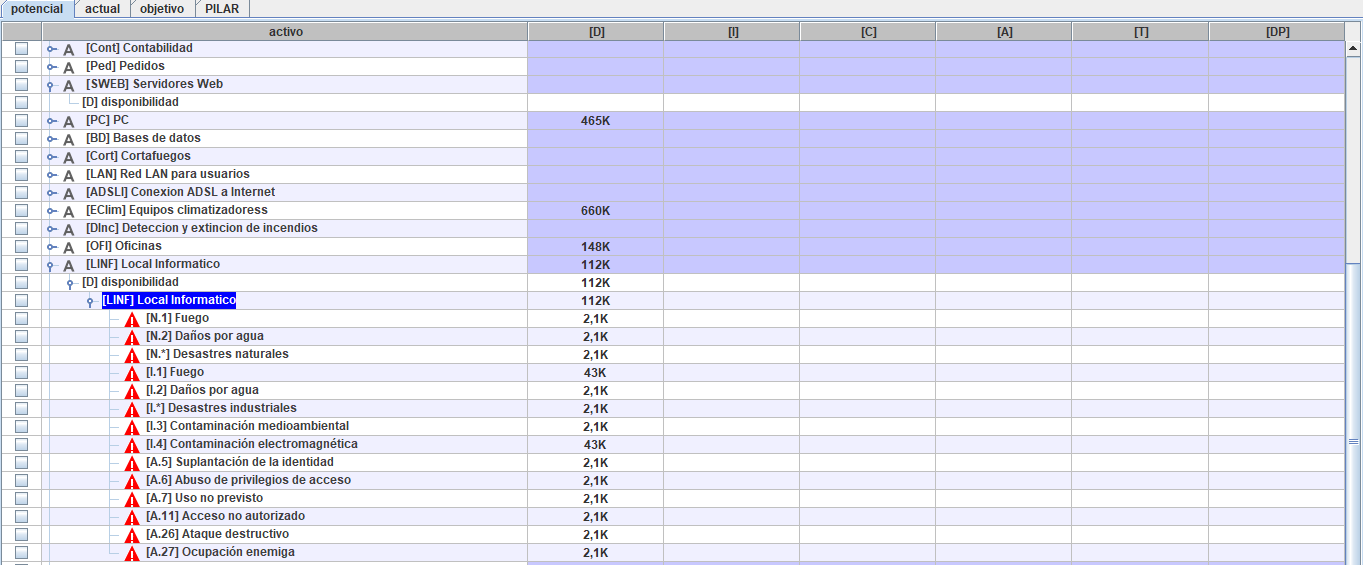
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Oficina | Ocupación enemiga | 1 | MB | MB |
| Oficina | Corte en los suministros | 10 | MB | B |
| Oficina | Acceso no autorizado | 10 | A | MA |
| Local informático | Ocupación enemiga | 1 | MB | MB |
| Local informático | Cortes en los suministros | 10 | MB | B |
| Local informático | Acceso no autorizado | 10 | A | MA |
| Almacén | Ocupación enemiga | 1 | MB | MB |
| Almacén | Corte en los suministros | 10 | MB | B |
| Almacén | Acceso no autorizado | 10 | A | MA |

**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

****

**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

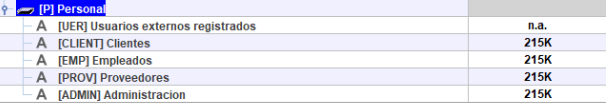
* No aplica:
  + Tener equipos de seguridad específica en cada sector
  + Controlar la entrada de personas a los edficios con escáneres
* No justifica:
  + Sería tener contratado personal innecesario ya que con pocas personas encargándose de la seguridad sería suficiente.
  + Sería tener equipos demasiado sofisticados.
* Aplican y justifican:
  + Tener medidas de seguridad como cámaras de vigilancia y personas encargadas en ello
  + Tener los equipos de detección pertinentes para la oficina/local/almacén en cuestión.

#### **9 Personal**

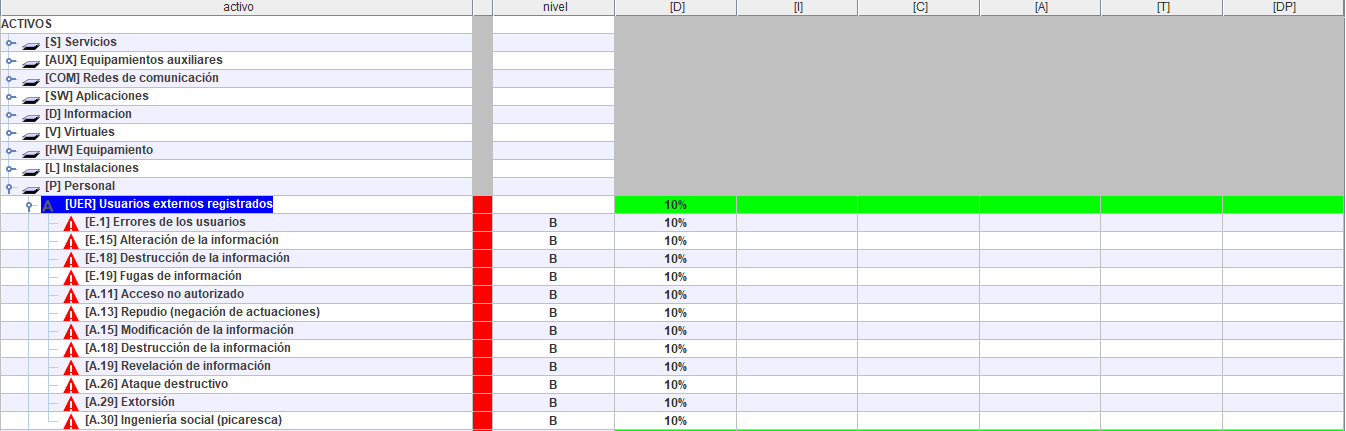
**Activos:** Usuarios externos registrados, clientes, empleados, proveedores y administración.

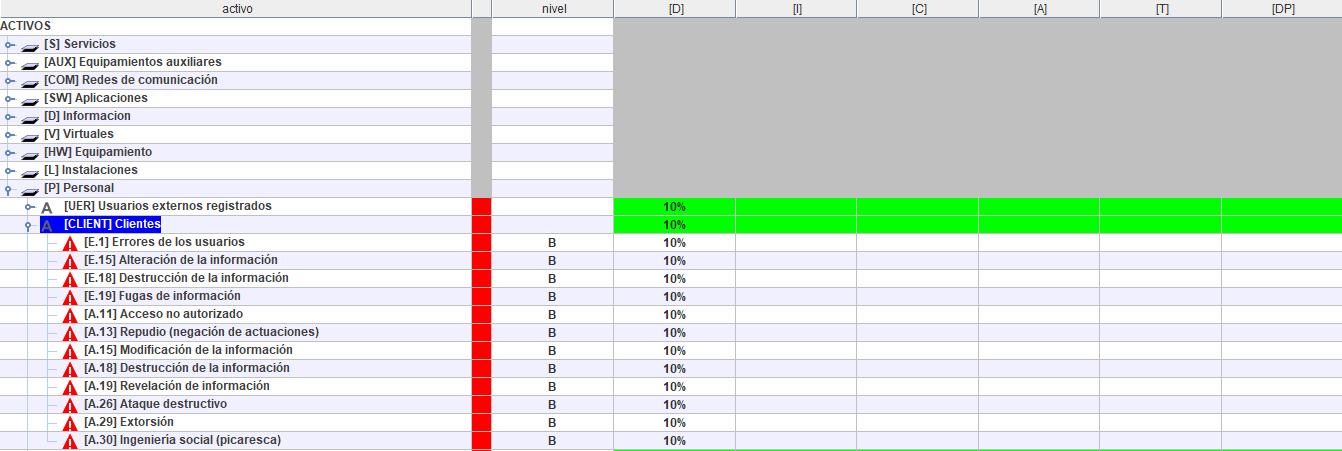
**Dependencias entre activos:** Usuarios registrados, reputación de la empresa, pedidos, histórico de compras (clientes, proveedores), histórico de precios de productos, imagen de la empresa, catálogo de productos, usuarios internos, personal y nóminas.

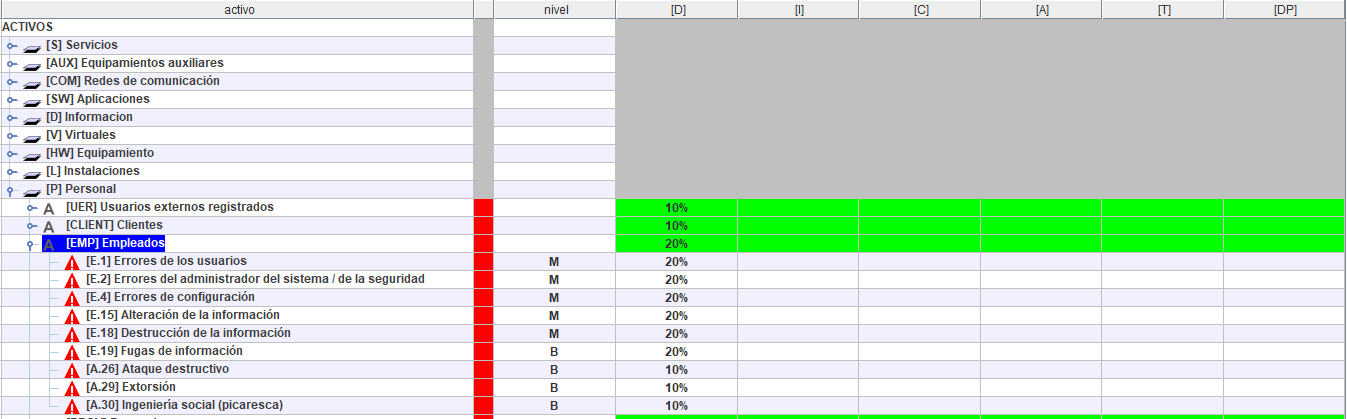
### **Valor de los activos**

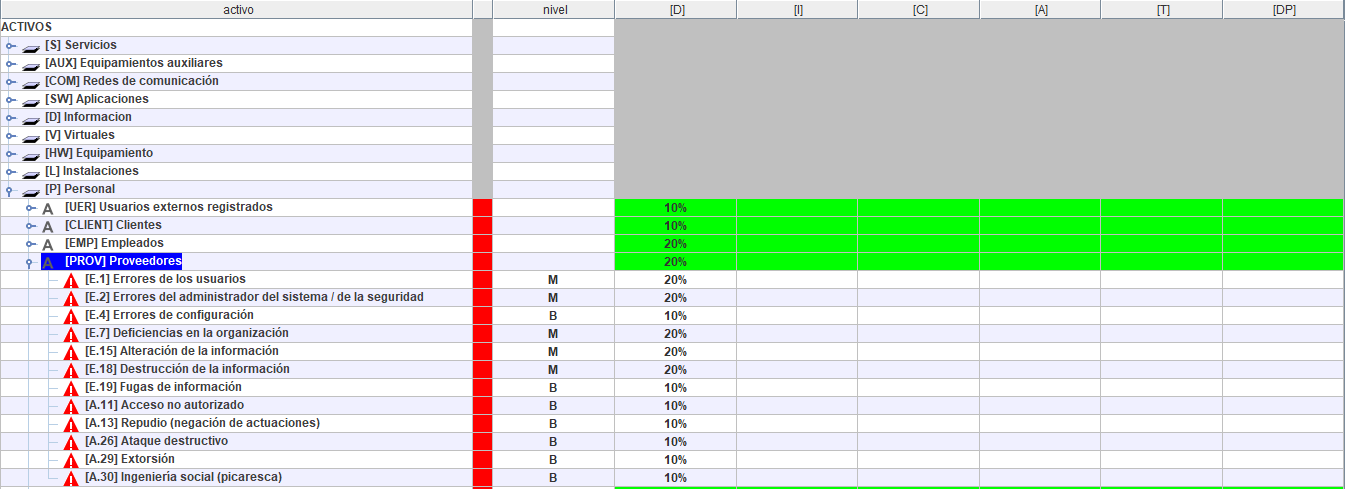
****

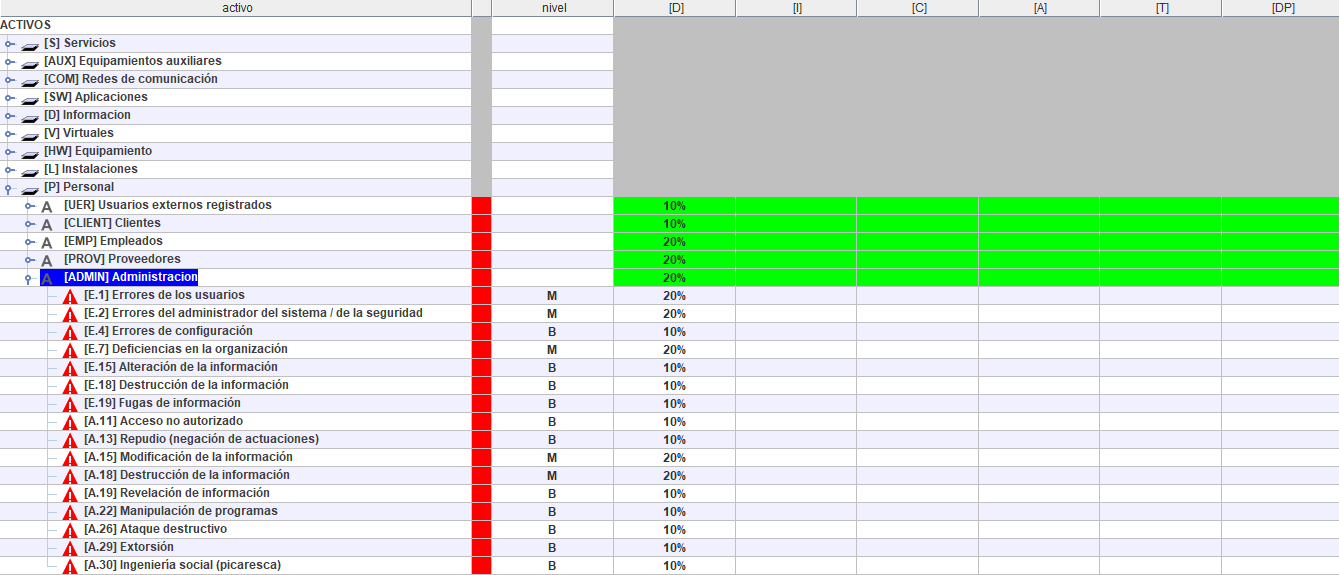
**Amenazas producidas por PILAR:**

****

****

****

****

****

**Amenazas:**

* Suplantación de la identidad
* Errores de usuario
* Extorsión
* Ingeniería social picaresca

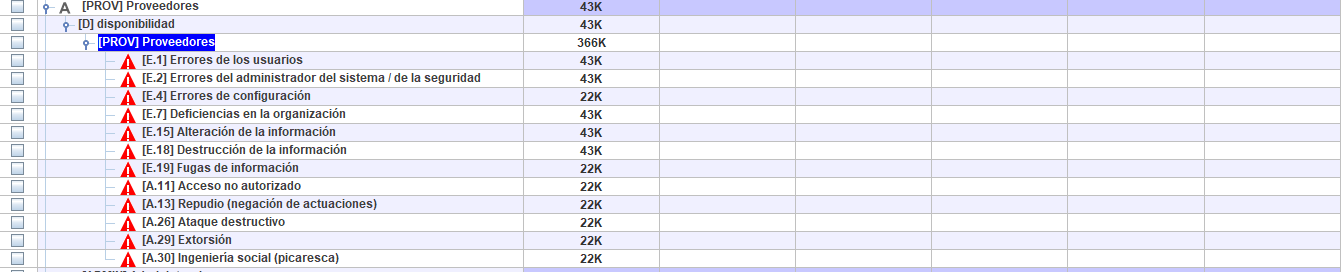
**Degradación:**

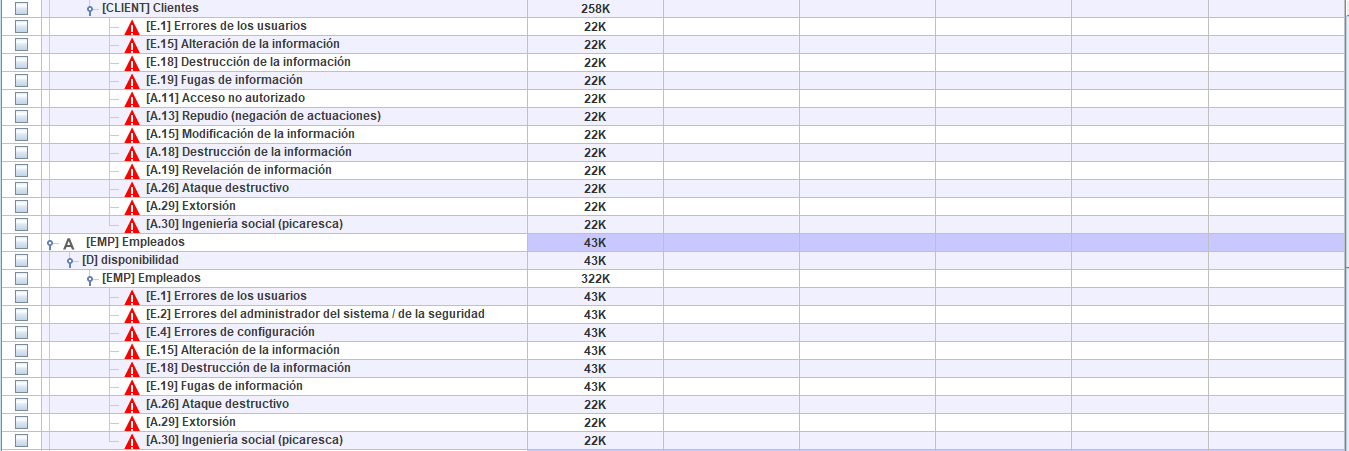
En caso de materializarse alguna de las amenazas anteriores, derivaría en daños materiales y/o personales que comprometerían en menor o mayor medida la empresa.

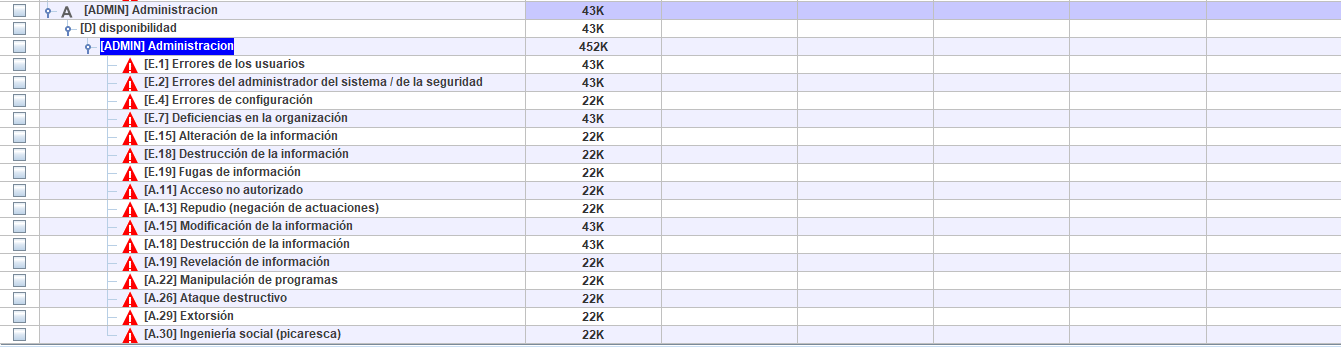
**Probabilidad:**

|  |  |  |  |
| --- | --- | --- | --- |
| Amenaza | Probabilidad | Frecuencia | Temporalidad |
| Suplantación de la identidad | 10 | Frecuente | Mensualmente |
| Errores de usuario | 100 | Muy frecuente | A diario |
| Extorsión | 1 | Normal | Una vez al año |
| Ingeniería social picaresca | 1 | Normal | Una vez al año |

**Impactos según PILAR:**

****

****

****

**Impactos:**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Degradación | Valoración | Impacto |
| Usuarios externos registrados | Errores de usuario | 1% | MB | MB |
| Clientes | Suplantación de la identidad | 10% | B | MB |
| Empleados | Suplantación de la identidad | 100% | A | A |
| Empleados | Extorsión | 100% | A | A |
| Empleados | Ingeniería social picaresca | 100% | A | A |
| Administración | Suplantación de la identidad | 100% | A | **A** |
| Administración | Extorsión | 100% | A | A |
| Administración | Ingeniería social picaresca | 100% | MA | MA |
| Proveedores | Suplantación de la identidad | 10% | B | MB |

**Impacto potencial**:

Si se materializase alguna de estas amenazas el impacto sería bastante alto en más de la mitad de las ocasiones. Por lo que es importante analizar bien los riesgos que se pueden derivar de las amenazas que tienen un mayor nivel de impacto. Sobre todo, los relacionados con los acuerdos con empresas.

**Riesgo**:

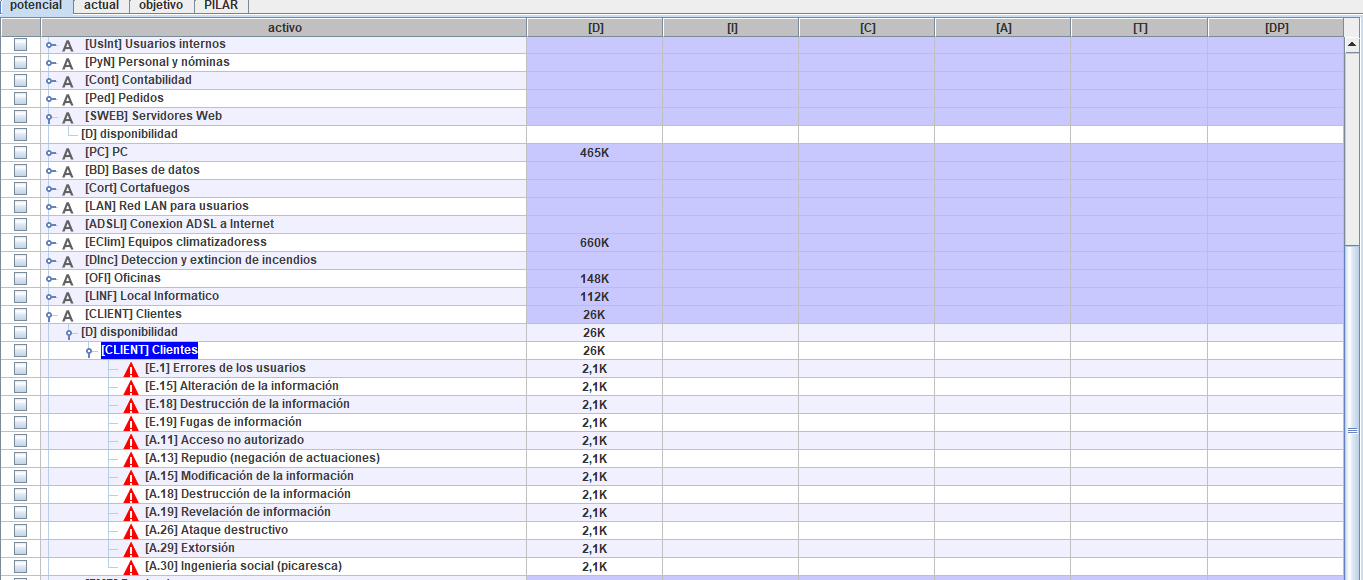
Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

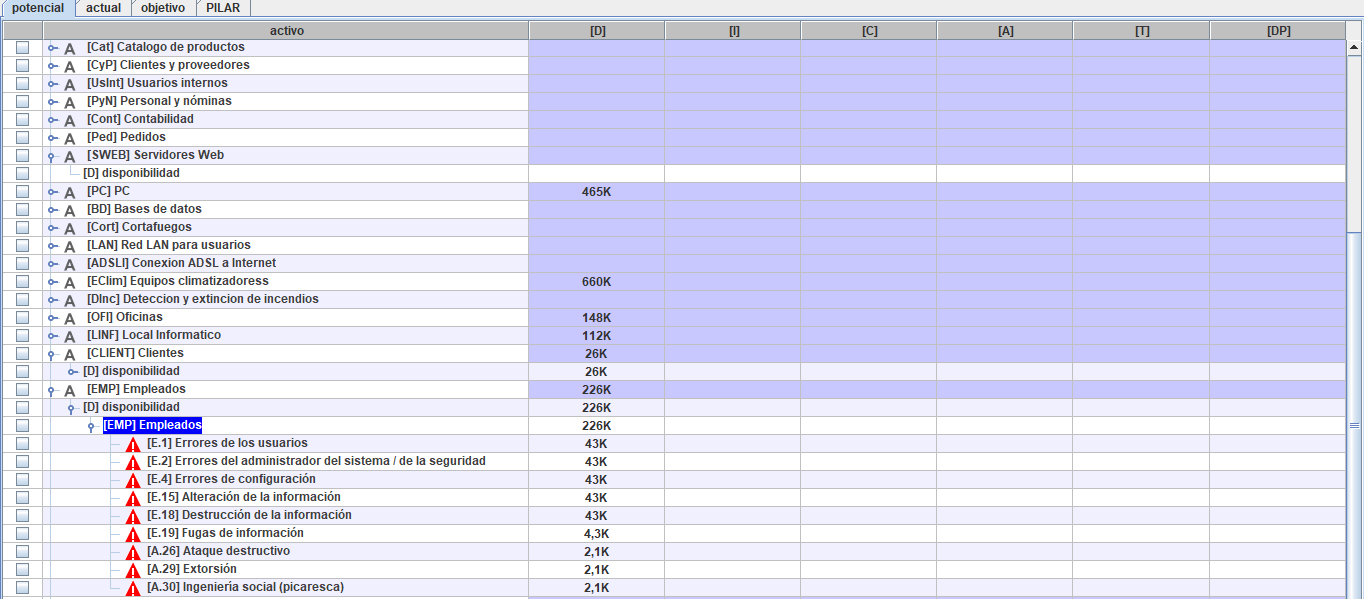
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Activo | Amenaza | Probabilidad | Impacto | Riesgo |
| Usuarios externos registrados | Errores de usuario | 100 | MB | B |
| Clientes | Suplantación de la identidad | 10 | MB | B |
| Empleados | Suplantación de la identidad | 10 | A | MA |
| Empleados | Extorsión | 1 | A | A |
| Empleados | Ingeniería social picaresca | 1 | A | A |
| Administración | Suplantación de la identidad | 10 | **A** | MA |
| Administración | Extorsión | 1 | A | A |
| Administración | Ingeniería social picaresca | 1 | MA | MA |
| Proveedores | Suplantación de la identidad | 10 | MB | B |

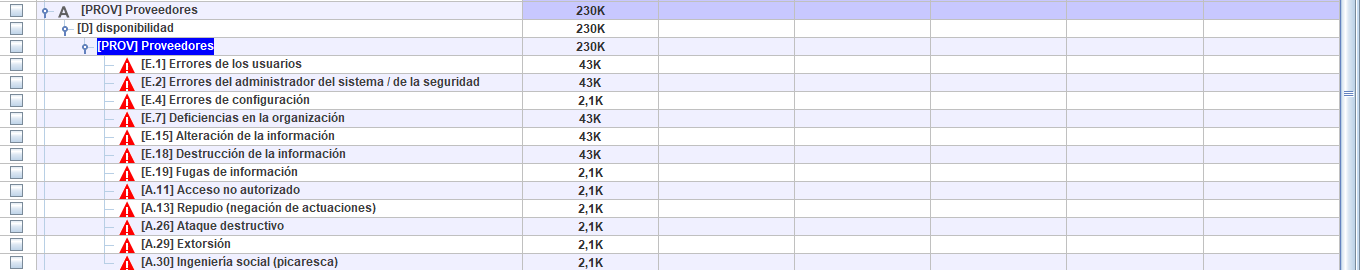
**Riesgo potencial:**

Si se materializase alguna de las amenazas anteriores el riesgo podría ser muy grande por lo que es necesario estudiar en profundidad las amenazas con un riesgo mayor para evitar éste en la medida de lo posible.

**Riesgo con PILAR**

****

****

****

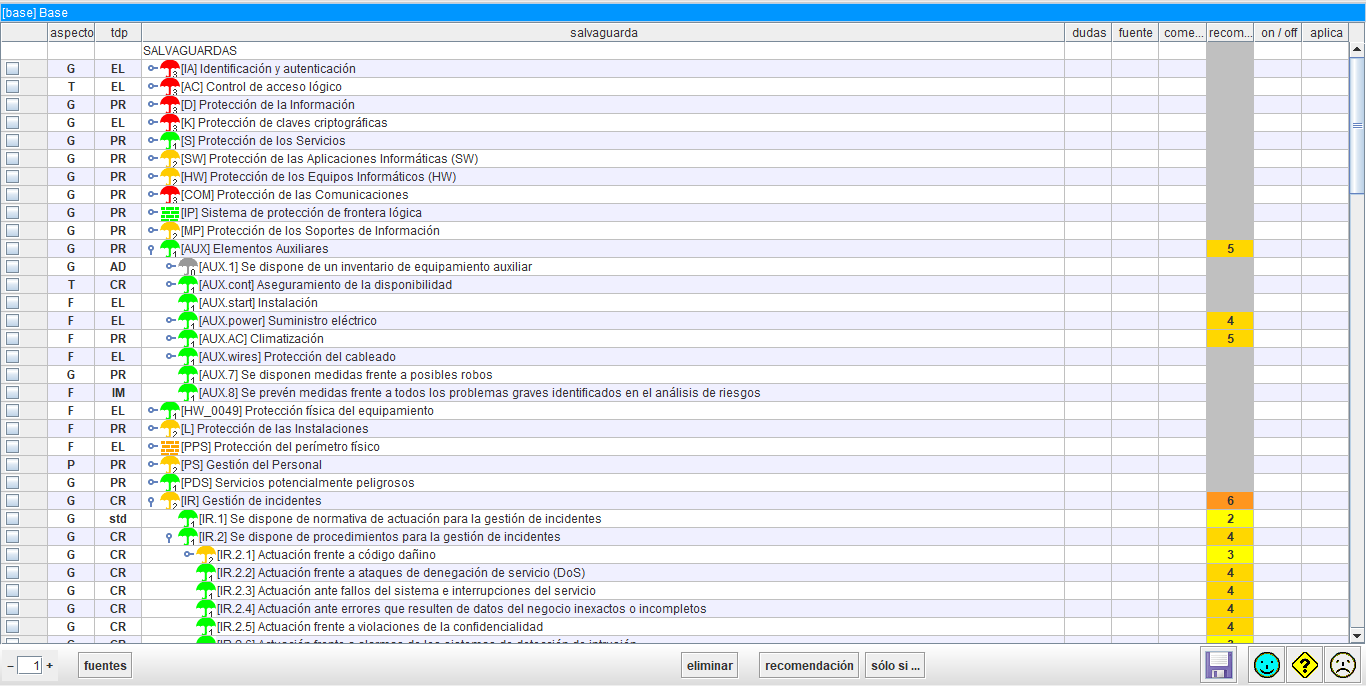
**Salvaguardas:**En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

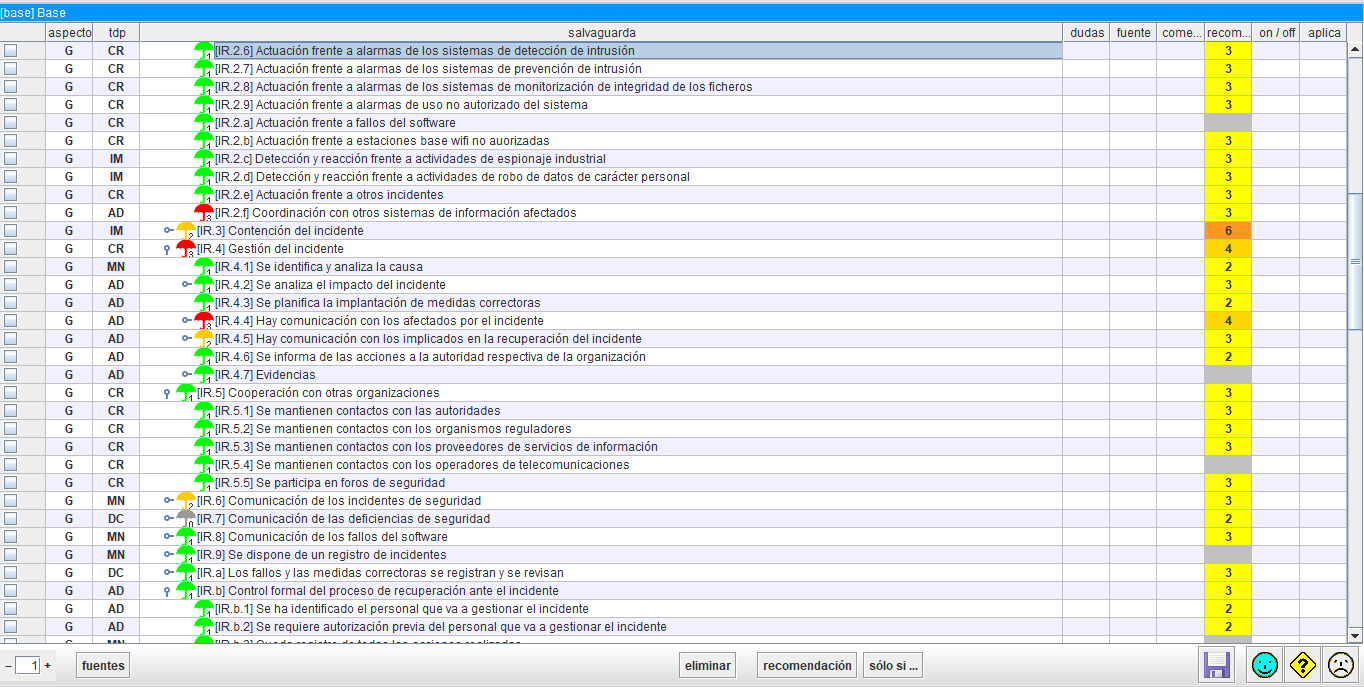
En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

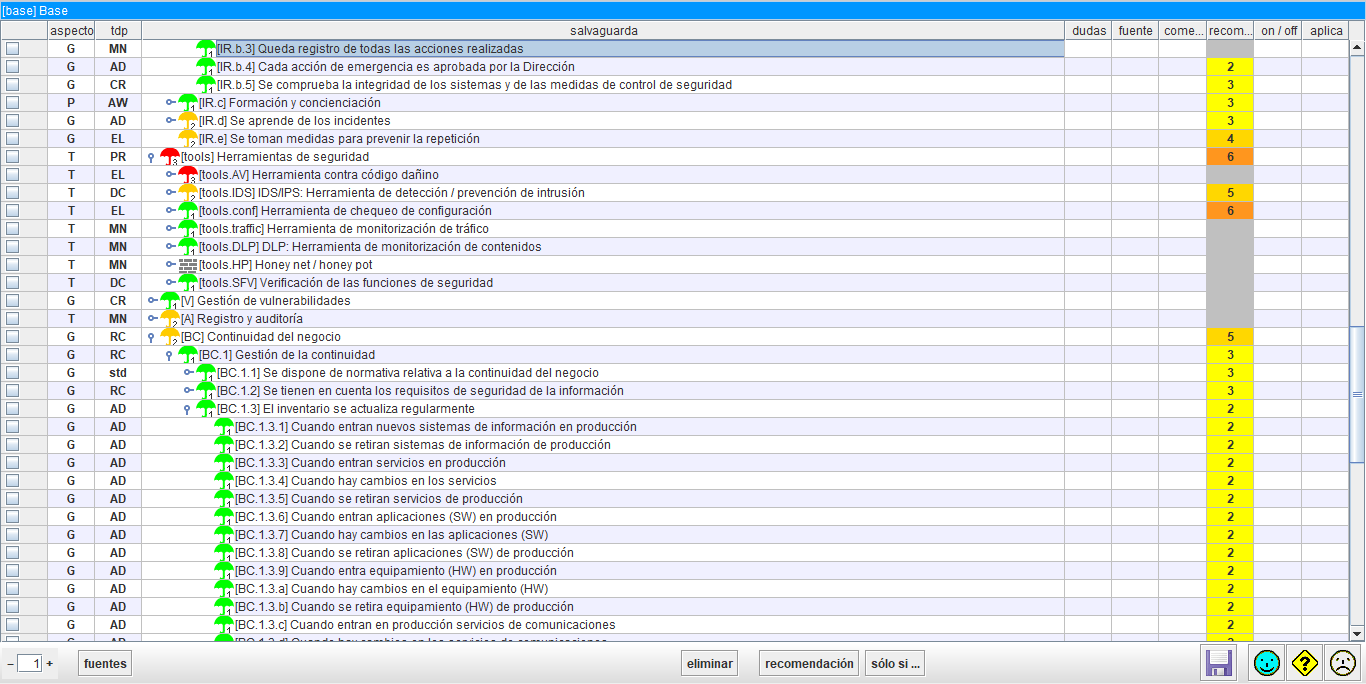
Se definen las salvaguardas o contramedidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

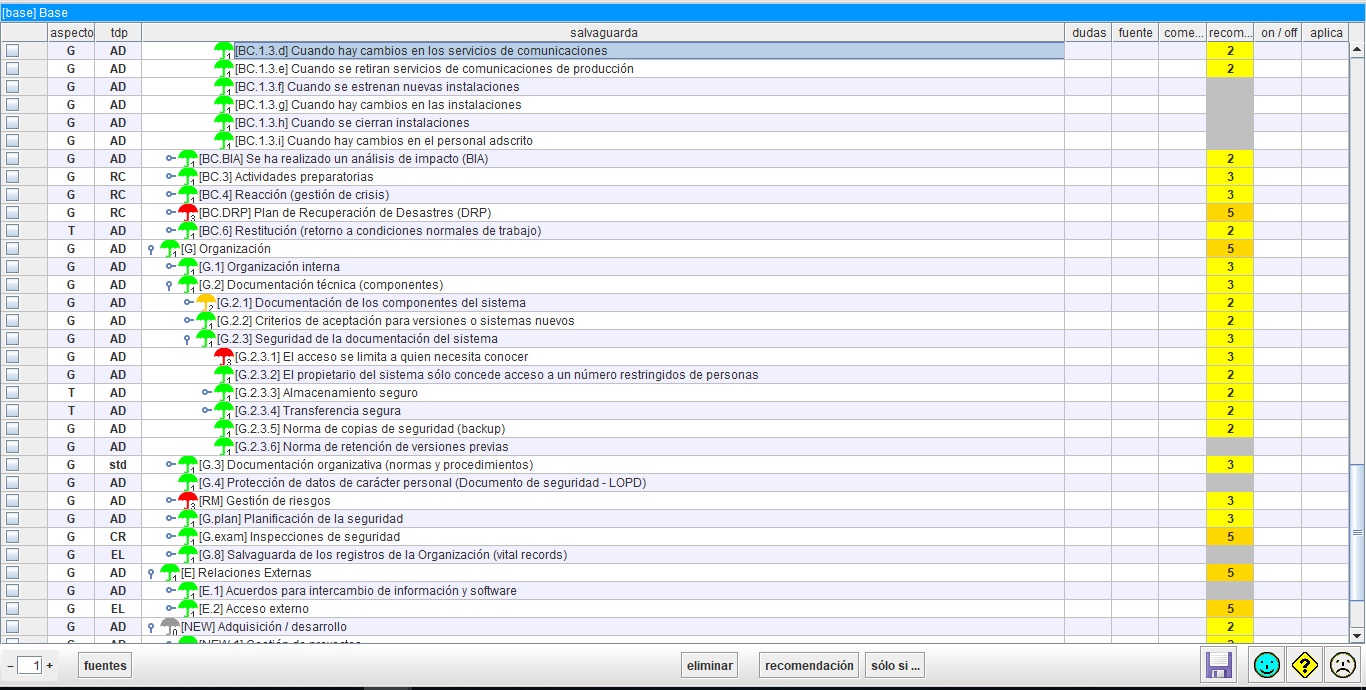
* No aplica:
  + Tener varias personas encargándose de lo misma función.
  + Realizar cursos de formación que no estén relacionados con las actividades de la empresa.
  + Fomentar la competitividad “sucia” entre los empleados para motivar a realizar y coneguir los objetivos pro`puestos por la empresa.
* No justifica:
  + Sería tener personal de más de manera innecesaria.
  + Ya que no servirán de nada más que perder dinero y tiempo.
  + Ya que ,seguramente pueda ocasionar problemas en la realización de las funciones de las empresas por conflictos entre el personal.
* Aplican y justifican:
  + Tener personal de RRHH competente para llevar a cabo una gestión correcta del personal de la empresa.
  + Realizar solo los cursos pertinentes, continuamente, para el mayor desempeño de los empleados
  + Fomentar el trabajo en equipo y la competencia sana con actividades lúdicas a cargo de la empresa para promover un buen ambiente de trabajo.

#### **10 Salvaguardas según PILAR**









#### **11 Dependencias entre activos**

#### 

