**IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse.

De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Para facilitar el manejo y mantenimiento del inventario los activos se pueden distinguir diferentes categorías de los mismos:

* **Datos**: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.
* **Aplicaciones**: El software que se utiliza para la gestión de la información.
* **Personal**: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.
* **Servicios**: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).
* **Tecnología**: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)
* **Instalaciones**: lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)
* **Equipamiento** **auxiliar**: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hayan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.)

Cada uno de los activos que se identifiquen debe contar con un responsable, que será su propietario.

Esta persona se hará cargo de mantener la seguridad del activo, aunque no necesariamente será la que gestione el día a día del mismo.

**INVENTARIO DE LOS ACTIVOS**

El inventario de activos es la base para la gestión de los mismos (ISO 27001), ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre.

Esta información como mínimo es:

* **Identificación del activo**: un código para ordenar y localizar los activos.
* **Tipo de activo**: a qué categoría de las anteriormente mencionadas pertenece el activo.
* **Descripción**: una breve descripción del activo para identificarlo sin ambigüedades.
* **Propietario**: quien es la persona a cargo del activo.
* **Localización**: dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

El inventario de activos no es recomendable que sea demasiado exhaustivo. Desglosar los activos hasta el nivel de registro o de elemento de un equipo informático no es probable que vaya a proporcionar información relevante en cuanto a las amenazas y los riesgos a los que debe hacer frente la organización y además complicará enormemente la realización del análisis de riesgos, ya que cuantos más activos haya más laborioso será el mismo.

El inventario deberá recoger los activos que realmente tengan un peso específico y sean significativos para la organización, agrupando aquellos que, por ser similares, tenga sentido hacerlo. Por ejemplo, si hay treinta PCs de parecidas características técnicas y en la misma ubicación física, pueden agruparse en un único activo, denominado por ejemplo “equipo informático”.

**VALORACIÓN DE LOS ACTIVOS**

Una vez identificados los activos, el siguiente paso a realizar es valorarlos. Es decir, hay que estimar qué valor tienen para la organización, cual es su importancia para la misma.

Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

Esta valoración se hará de acuerdo con una escala que puede ser cuantitativa o cualitativa. Si es posible valorar económicamente los activos, se utiliza la escala cuantitativa. En la mayoría de los casos, no es posible o va a suponer un esfuerzo excesivo, por lo que utilizan escalas cualitativas como por ejemplo: bajo, medio, alto o bien un rango numérico, por ejemplo de 0 a 10

Con independencia de la escala utilizada, los aspectos a considerar pueden ser los daños como resultado de:

* •Violación de legislación aplicable.
* •Reducción del rendimiento de la actividad.
* •Efecto negativo en la reputación.
* •Pérdidas económicas.
* •Trastornos en el negocio.

La valoración debe ser lo más objetiva posible, por lo que en el proceso deben estar involucradas todas las áreas de la organización, aunque no participen en otras partes del proyecto y de esta manera obtener una imagen realista de los activos de la organización.

Es útil definir con anterioridad unos parámetros para que todos los participantes valoren de acuerdo a unos criterios comunes, y se obtengan valores coherentes. Un ejemplo de la definición de estos parámetros podría ser la siguiente:

* **Disponibilidad**. Para valorar este criterio debe responderse a la pregunta de cuál sería la importancia o el trastorno que tendría el que el activo no estuviera disponible. Si consideramos como ejemplo una escala de 0 a 3 se podría valorar como sigue:

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 |

Por ejemplo, la disponibilidad de un servidor central sería de 3, siguiendo estos criterios.

* **Integridad**. Para valorar este criterio la pregunta a responder será qué importancia tendría que el activo fuera alterado sin autorización ni control. Una posible escala es:

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% |

Siguiendo con el ejemplo del servidor central, debe mantenerse en todo momento funcionando correctamente, se le asigna el valor 3.

* **Confidencialidad**. En este caso la pregunta a responder para ponderar adecuadamente este criterio será cuál es la importancia que tendría que al activo se accediera de manera no autorizada. La escala en este caso podría ser:

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 |

Dependiendo de la organización y su contexto, el valor del servidor podría ser incluso 3 si la dependencia de esa máquina es muy grande y el simple acceso físico al servidor sería un trastorno para la organización.

También **debe decidirse cómo se va a calcular el valor total de los activos, bien como una suma de los valores que se han asignado a cada uno de los parámetros valorados, bien el mayor de dichos valores, la media de los mismos, etc.**

**Los criterios para medir el valor del activo deben ser claros, fáciles de comprender por todos los participantes en la valoración y homogéneos, para que se puedan comparar los valores al final del proceso**. De esta manera se sabrá cuales son los principales activos de la organización, y por lo tanto aquellos que necesitan de una particular atención.

El **análisis de riesgos** se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

**REALIZACIÓN DEL ANÁLISIS DE RIESGOS**

**Preparación del análisis de riesgos**

Para realizar un análisis de riesgos se parte del inventario de activos. Si es razonablemente reducido, puede decidirse hacer el análisis sobre todos los activos que contiene. Si el inventario es extenso, es recomendable escoger un grupo relevante y manejable de activos, bien los que tengan más valor, los que se consideren estratégicos o todos aquellos que se considere que se pueden analizar con los recursos disponibles. Se puede tomar cualquier criterio que se estime oportuno para poder abordar el análisis de riesgos en la confianza de que los resultados van a ser útiles.

Hay que tener en cuenta que la realización de un análisis de riesgos es un proceso laborioso. Para cada activo se van a valorar todas las amenazas que pueden afectarle, la vulnerabilidad cada una de las amenaza y el impacto que causaría la amenaza en caso de ocurrir. Con todos esos datos, se calcula el valor del riesgo para ese activo.

Independientemente de la metodología que se utilice, el análisis de riesgos debe ser objetivo y conseguir resultados repetibles en la medida de lo posible. De esta manera quedarán plasmados varios puntos de vista y la subjetividad, que es inevitable, quedará reducida.

**Identificar amenazas**

Como ya se ha visto anteriormente, podríamos denominar amenaza a un evento o incidente provocado por una entidad natural, humana o artificial que, aprovechando una o varias vulnerabilidades de un activo, pone en peligro la confidencialidad, la integridad o la disponibilidad de ese activo. Dicho de otro modo, una amenaza explota la vulnerabilidad del activo.

Las amenazas pueden ser: externas, internas, deliberadas o accidentales

Para valorar las amenazas en su justa medida hay que tener en cuenta cual sería el impacto en caso de que ocurrieran y a cual o cuáles son los parámetros de seguridad que afectaría, si a la confidencialidad, la integridad o la disponibilidad.

**Identificación de vulnerabilidades**

Hay que identificar las debilidades en el entorno de la Organización y valorar cómo de vulnerable es el activo en una escala razonable (alto-medio-bajo, de 1 a 5, etc.).

Algunos ejemplos de vulnerabilidades son:

* La ausencia de copias de seguridad, que compromete la disponibilidad de los activos.
* Tener usuarios sin formación adecuada, que compromete la confidencialidad, la integridad y la disponibilidad de los activos, ya que pueden filtrar información o cometer errores sin ser conscientes del fallo.
* Ausencia de control de cambios, que compromete la integridad y la disponibilidad de los activos.

**Ejecución del análisis**

Con el equipo de trabajo asignado para ello y la metodología escogida, se llevará a cabo el análisis de riesgos. Los participantes tendrán que valorar las amenazas y las vulnerabilidades que afectan a los activos escogidos para el análisis y el impacto que ocasionaría que alguna de las amenazas realmente ocurriera, sobre la base de su conocimiento y experiencia dentro de la organización.

Como ejemplo de metodología de Análisis de Riesgos (muy resumida) utilizaremos como referencia las siguientes tablas:

Estimación de la probabilidad de ocurrencia de una amenaza sobre cada activo:

Tabla 4. PROBABILIDADES

|  |  |
| --- | --- |
| Probabilidad de ocurrencia de la amenaza | Guía  |
| Baja | Una media de una vez cada 5 años |
| Media | Una media de una vez al año |
| Alta | Una media de 3 veces al año |
| Muy alta | Una media de una vez al mes |

Estimación de la vulnerabilidad de cada activo, es decir, la facilidad de las amenazas para causar daños en el mismo.

Tabla 5. VULNERABILIDAD

|  |  |
| --- | --- |
| Vulnerabilidad  | Guía  |
| Baja | Difícil que ocurra el peor escenario posible (Prob.< 33%) |
| Media | Probable que ocurra el peor escenario posible (33% > Prob.< 66%) |
| Alta | Casi seguro que ocurra el peor escenario posible (Prob.> 66%) |

La siguiente tabla se utilizará para calcular el nivel de riesgo, valorando el impacto que tendría en un activo la ocurrencia de una amenaza:

Tabla 6. NIVEL DE RIESGO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Amenaza | Baja | Media | Alta | Muy alta |
| Vulnerabilidad | B | M | A | B | M | A | B | M | A | B | M | A |
| Impacto | 0 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 3 |
|  | 1 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 4 |
| 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 |
| 3 | 2 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 |
| 4 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 5 |
|  5 | 3  | 4  | 4  | 4  | 4  | 5  | 4  | 5  | 5  | 5  | 5  | 6  |
| 6 | 4  | 4  | 5  | 4  | 5  | 5  | 5  | 5  | 6  | 5  | 6  | 6  |
|  | 7 | 4  | 5  | 5  | 5  | 5  | 6  | 5  | 6  | 6  | 6  | 6  | 7  |
|  | 8 | 5  | 5  | 6  | 5  | 6  | 6  | 6  | 7  | 7  | 8  | 8  | 9  |
|  | 9 | 6  | 6  | 7  | 7  | 8  | 8  | 8  | 9  | 9  | 9  | 10  | 10  |

Tomemos como ejemplo un activo, portátiles, cuya valoración ha resultado ser 8 y cuyas principales amenazas se considera que son:

* + - * Robo.
			* Errores de los usuarios.
			* Divulgación de información.
			* Acceso no autorizado.

Por lo que el nivel de riesgo será:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Amenaza | Impacto (Valor del activo) | Probabilidad de la Amenaza | Vulnerabilidad | Nivel de riesgo |
| Fuego | 8 | Baja | Alta | 6 |
| Errores usuarios | de | 8 | Alta | Media | 7 |
| Divulgación información | de | 8 | Media | Media | 6 |
| Acceso autorizado | no | 8 | Muy Alta | Alta | 9 |
|  | Total | 28 |

El valor de riesgo para este activo es la suma de los valores individuales de cada amenaza, por lo que es 28.

De este modo obtendríamos el riesgo de todos los activos que se han incluido en el Análisis de Riesgos y podríamos realizar las medidas oportunas para mitigarlos (o realizar el tratamiento escogido en cada caso).

**Documentar el análisis de riesgos**

Independientemente de la metodología o la herramienta informática que se utilice para la realización del análisis de riesgos, el resultado debería ser una lista de los riesgos correspondientes a los posibles impactos en caso de que se materialicen las amenazas a las que están expuestos los activos.

Esto permite categorizar los riesgos e identificar cuáles deberían ser tratados primero o más exhaustivamente. Se debe escoger, a la vista de los resultados, cual es el nivel de riesgo que la organización está dispuesta a tolerar, de manera que por debajo de ese nivel el riesgo es aceptable y por encima no lo será y se tomará alguna decisión al respecto.

Hay cuatro tipos de decisiones para tratar los riesgos que se consideran no aceptables:

* **Transferirlo**: El riesgo se traspasa a otra organización, por ejemplo mediante un seguro.
* **Eliminarlo**: Se elimina el riesgo, que normalmente sólo se puede hacer eliminando el activo que lo genera, por ello esta opción no suele ser viable.
* **Mitigarlo**: Es decir, reducir el riesgo, normalmente aplicando controles de seguridad. Es una de las opciones más habituales.
* **Asumirlo**: Otra opción común es aceptar que no se puede hacer nada y por lo tanto se asume ese riesgo.

Toda esta información debe quedar documentada para justificar las acciones que se van a tomar para conseguir el nivel de seguridad que la organización quiere alcanzar y como referencia para posteriores análisis.