Módulo 7:
Los activos de Seguridad de la Información

Se explica en este tema cómo deben abordarse la elaboración de un inventario de activos que recoja los principales activos de información de la organización, y cómo deben valorarse esos activos en función de su relevancia para la misma y del impacto que ocasionaría un fallo de seguridad en ellos.

El contenido de este módulo es:

- Identificación de los activos de información.
- Inventario de activos.
- Valoración de los activos.
- Evaluación.

I. 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 hallan 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.

Por ejemplo, puede existir un activo que sea la base de clientes, cuyo propietario sea el Director Comercial, sin embargo serán los comerciales de la organización los usuarios del mismo y el responsable de sistemas el encargado del mantenimiento de la base de datos.

Pero el propietario decide quién accede y quién no a la información, si es necesario aplicarle alguna medida de seguridad o existe algún riesgo que deba ser tenido en cuenta, si le aplica la LOPD y por tanto deben implantarse las medidas de seguridad exigidas por la Ley, etc.

II. Inventario de activos:

El inventario de activos que se va a utilizar para la gestión de la seguridad no debería duplicar otros inventarios, pero sí que debe recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.

El inventario de activos es la base para la gestión de los mismos, 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”.

En el caso de que hubiera veinte PCs y diez portátiles, si los portátiles no salieran nunca y los treinta equipos permanecieran siempre en la misma ubicación, también se podría asumir que constituyen un único activo pero si los portátiles se utilizan fuera de las instalaciones de la organización, ya no se podrían agrupar los treinta equipos, ya que las circunstancias en las que se utilizarían los equipos son distintas, por lo que habría que distinguir dos activos, por ejemplo “Equipo informático fijo” para los PCs y “Equipo informático móvil” para los portátiles.

En algunos casos, la complejidad de la organización, de sus procesos o de su contexto, puede hacer necesario el desarrollar un árbol de dependencias entre activos. El concepto es que algunos activos dependen de otros, en uno o más parámetros de seguridad.

Identificar y documentar estas dependencias constituye un árbol de dependencias, que dará una idea más exacta del valor de cada activo. Por ejemplo, una aplicación alojada en un servidor, depende este servidor para ejecutarse, para estar disponible. Si el servidor tiene una avería o un error de configuración, la aplicación podría ver afectada su disponibilidad. Por lo tanto el valor del servidor puede considerarse que sea no sólo el que tiene en sí mismo, sino también el que tiene por permitir el correcto funcionamiento de la aplicación.

III. 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:

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 con 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:

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%

  Por ejemplo, que en el servidor central fueran modificadas, por personal no autorizado, las cuentas de usuario de los demás departamentos. En este caso el valor sería 3.

- **Confidencialidad:**

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

VALOR	CRITERIO
0	No aplica / No es relevante
1	Daños muy bajos, el incidente no trascendería del área afectada
2	Serían relevantes, el incidente implicaría a otras áreas
3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas

Por ejemplo, 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.

La valoración de los activos deben realizarla un grupo de personas que sean lo suficientemente representativas como para aportar entre todos una visión razonablemente objetiva de la organización. Por supuesto deben ser personas que conozcan bien la organización. Si se van a hacer las valoraciones mediante reuniones de trabajo, el grupo no debería ser excesivamente numeroso para que las reuniones no se alarguen demasiado. Si se van a utilizar cuestionarios o entrevistas, se puede involucrar a más personas, siempre teniendo en cuenta el coste asociado a ello.

Evaluación Módulo 7

1. Son activos de información:

   - [ ] Expedientes de proyectos, libros de contabilidad y facturas
   - [ ] Equipos informáticos, incluyendo periféricos y software
   - [ ] Todos ellos
   - [ ] Dejar en blanco

2. El propietario de un activo se encarga de:

   - [ ] Su adquisición y puesta en marcha
   - [ ] Su seguridad
   - [ ] Gestionarlo
   - [ ] Dejar en blanco

3. Para valorar un activo hay que calcular su valor económico:

   - [ ] Verdadero
   - [ ] Falso
   - [ ] Sólo si se quiere hacer una valoración cuantitativa
   - [ ] Dejar en blanco

4. Es mejor que en la valoración de los activos participen:

   - [ ] Representantes de las áreas dentro del alcance del SGSI
   - [ ] Todos los empleados
   - [ ] Sólo el responsable de seguridad
   - [ ] Dejar en blanco