Módulo 8:
Análisis y valoración de los riesgos. Metodologías

Uno de los puntos clave de todo SGSI es el análisis de riesgos. En este módulo además de explicar detalladamente en qué consiste y cómo debe llevarse a cabo para cumplir con lo establecido por la Norma se describirán las principales metodologías que existen en el mercado.

Los contenidos de este módulo comprenden:

- Conceptos básicos.
- Realización del análisis de riesgos.
- Metodologías.
- Evaluación.

I. Conceptos básicos de un análisis de riesgos:

En primer lugar conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, 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. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

- **Amenaza:** Es la causa potencial de un daño a un activo.
- **Vulnerabilidad:** debilidad de un activo que puede ser aprovechada por una amenaza.
- **Impacto:** consecuencias de que la amenaza ocurra.
- **Riesgo intrínseco:** cálculo del daño probable a un activo si se encontrara desprotegido.
- **Salvaguarda:** Medida técnica u organizativa que ayuda a paliar el riesgo.
- **Riesgo residual:** Riesgo remanente tras la aplicación de salvaguardas.

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

A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuantos recursos se cuenta (económicos, humanos, técnicos…) pero no es tan fácil saber a ciencia cierta cuáles son las necesidades de seguridad.

Es aquí donde se muestra imprescindible la realización de un análisis de riesgos. Hacerlo permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información ya será posible tomar decisiones bien fundamentadas acerca de qué medidas de seguridad deben implantarse.

Por tanto, un aspecto de gran importancia a la hora de realizar la implantación de un SGSI es tener en cuenta que la inversión en seguridad tiene que ser proporcional al riesgo.

La información es generada y tratada por el personal tanto interno como externo, mediante los equipos de tratamiento de la información existentes en la organización y está situada en las instalaciones, por lo hay que considerar todos los riesgos relacionados con estos aspectos.

II. 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, por lo que deberían participar en él todas las áreas de la organización que estén dentro del alcance del SGSI. De esta manera quedarán plasmados varios puntos de vista y la subjetividad, que es inevitable, quedará reducida. Además contar con la colaboración de varias personas ayuda a promover el desarrollo del SGSI como una herramienta útil para toda la organización y no sólo para la dirección o el área que se encarga del proyecto. Se puede abordar el análisis de riesgos con varios enfoques dependiendo del grado de profundidad con el que se quiera o pueda realizar el análisis:

1. Enfoque de Mínimos:

Se escoge un conjunto mínimo de activos y se hace un análisis conjunto, de manera que se emplean una cantidad mínima de recursos, consumiendo poco tiempo y por lo tanto tiene el coste es menor. Este enfoque tienen el inconveniente de que si se escoge un nivel básico de seguridad muy alto, puede requerir recursos excesivos al implantarlo para todos los activos y por el contrario, si es muy bajo, los activos con más riesgos pueden no quedar adecuadamente protegidos. Debido a la falta de detalle en el análisis, puede ser difícil actualizar los controles o añadir otros según vayan cambiando los activos y sistemas.

2. Enfoque informal:

Con este enfoque, no se necesita formación especial para realizarlo ni necesita de tantos recursos de tiempo y personal como el análisis detallado. Las desventajas de este informe son que al no estar basado en métodos estructurados, puede suceder que se pasen por altos áreas de riesgos o amenazas importantes y al depender de las personas que lo realizan, el análisis puede resultar con cierto grado de subjetividad. Si no se argumenta bien la selección de controles, puede ser difícil justificar después el gasto en su implantación.

3. Enfoque detallado:

Con este enfoque se consigue una idea muy exacta y objetiva de los riesgos a los que se enfrenta la organización. Se puede decidir un nivel de seguridad apropiado para cada activo y de esa manera escoger los controles con precisión. Es el enfoque que más recursos necesita en tiempo, personal y dinero para llevarlo a cabo de una manera efectiva.

4. Enfoque combinado:

Con un enfoque de alto nivel al principio, permite determinar cuáles son los activos en los que habrá que invertir más antes de utilizar muchos recursos en el análisis. Por ello ahorra recursos al tratar antes y de manera más exhaustiva los riesgos más importantes mientras que al resto de los riesgos sólo se les aplica un nivel básico de seguridad, con lo que consigue un nivel de seguridad razonable en la organización con recursos ajustados. Es el enfoque más eficaz en cuanto a costes y a adaptabilidad a empresas con recursos limitados. Hay que tener en cuenta que si el análisis de alto nivel es erróneo puede que queden algunos activos críticos a los que no se realice un análisis detallado.

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.

Atendiendo a su origen, existen dos tipos de amenazas:

- **Externas**, que son las causadas por alguien (hackers, proveedores, clientes, etc.) o algo que no pertenece a la organización. Ejemplos de amenazas de este tipo son los virus y las tormentas.
- **Internas**, estas amenazas son causadas por alguien que pertenece a la organización, por ejemplo errores de usuario o errores de configuración.

Las amenazas también pueden dividirse en dos grupos según la intencionalidad del ataque en deliberadas y accidentales:

1. **Deliberadas:** Cuando existe una intención de provocar un daño, por ejemplo un ataque de denegación de servicio o la ingeniería social.

2. **Accidentales:** Cuando no existe tal intención de perjudicar, por ejemplo averías o las derivadas de desastres naturales: terremotos, inundaciones, fuego, etc.

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

Identificación de vulnerabilidades

Tal y como hemos comentado anteriormente, una vulnerabilidad es toda aquella circunstancia o característica de un activo que permite la materialización de ataques que comprometen la confidencialidad, integridad o disponibilidad del mismo. Por ejemplo, un equipo será vulnerable a los virus si no tiene un programa antivirus instalado.

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.).

Hay que tener en cuenta que la presencia de una vulnerabilidad por si misma no causa daño. Para que se produzca este daño debe existir una amenaza que pueda explotarla.

Algunos ejemplos de vulnerabilidades son:

1. La ausencia de copias de seguridad, que compromete la disponibilidad de los activos.
2. 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.
3. 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:

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:

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:

Amenaza		Baja			Media			Alta			Muy alta		
Vulnerabilidad		Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta	Baja	Media	Alta
Impacto	0	1	1	1	1	1	2	1	2	2	2	2	3
	1	1	2	2	2	2	3	2	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:

1. Robo.
2. Errores de los usuarios.
3. Divulgación de información.
4. Acceso no autorizado.

Por lo que el nivel de riesgo será:

NIVEL DE RIESGO

Amenaza	Impacto (Valor del Activo)	Probabilidad de la Amenaza	Vulnerabilidad	Nivel de riesgo
Fuego	8	Baja	Alta	6
Errores de los usuarios	8	Alta	Media	7
Divulgación de información	8	Media	Media	6
Acceso no autorizado	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.

III. Metodologías:

Existen numerosas metodologías disponibles para la realización de análisis de riesgos, ya que es una labor que requiere de bastante dedicación y con una metodología estructurada se facilita la tarea, sobre todo si existe una herramienta que simplifique todo el proceso.

La organización debe escoger aquella que se ajuste a sus necesidades, y si considera varias opciones, inclinarse por la más sencilla. Hay que tener en cuenta que el análisis de riesgos debe revisarse periódicamente, por lo que si se hace con una metodología complicada, esta labor necesitará de una dedicación excesiva.

A continuación se detallarán algunas de las metodologías más reconocidas:

- **Análisis holandés A&K.**

Es método de análisis de riesgos, del que hay publicado un manual, que ha sido desarrollado por el Ministerio de Asuntos Internos de Holanda, y se usa en el gobierno y a menudo en empresas holandesas.

- **CRAMM.**

Es un método de análisis de riesgos desarrollado por el gobierno británico y cuenta con una herramienta, ya que es un método difícil de usar sin ella. Está basado en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas.

- **EBIOS.**

Es un juego de guías mas una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no sólo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de cinco fases:

- *Fase 1.* Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.
- *Fases 2 y 3*, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.
- *Fases 4 y 5*, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

- **IT-GRUNDSCHUTZ (Manual de protección básica de TI)**

Desarrollado en Alemania por la Oficina Federal de la Seguridad de la Información (BSI en sus siglas alemanas). Este manual proporciona un método para establecer un SGSI en cualquier organización, con recomendaciones técnicas para su implantación. El proceso de seguridad de TI propuesto por esta metodología sigue los siguientes pasos:

- Iniciar el proceso.
- Definir los objetivos de seguridad y el contexto de la organización.
- Establecer la organización para la seguridad de TI.
- Proporcionar recursos.
- Crear el concepto de la seguridad de TI.
- Análisis de la estructura de TI.
- Evaluación de los requisitos de protección.
- Modelado.
- Comprobación de la seguridad de TI.
- Planificación e implantación.
- Mantenimiento, seguimiento y mejora del proceso.

La metodología incluye listas de amenazas y controles de seguridad que se pueden ajustar a las necesidades de cada organización.

- **MAGERIT.**

Desarrollado por el Ministerio de Administraciones Públicas español, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de de un análisis y una gestión realmente efectivos. Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas.

- **Manual de Seguridad de TI Austriaco.**

onsta de dos partes, en la primera se describe el proceso de la gestión de la seguridad de TI, incluyendo el análisis de riesgos y la segunda es un compendio de 230 medidas de seguridad. Es conforme con la Norma ISO/IEC IS 13335 y en parte con la ISO 27002.

- **MARION – MEHARI.**

El primigenio MARION (Método de Análisis de Riesgos por Niveles), basado en una metodología de auditoría, permitía estimar el nivel de riesgos de TI de una organización. Sustituido por MEHARI, este Ing. José M. Poveda

método de análisis de riesgo cuenta con un modelo de evaluación de riesgos y módulos de componentes y procesos. Con MEHARI se detectan vulnerabilidades mediante auditorías y se analizan situaciones de riesgo.

- **Métodos ISF para la evaluación y gestión de riesgos.**

El Information Security Forum. (ISF) es una importante asociación internacional. Su Estándar de Buenas Prácticas es un conjunto de principios y objetivos para la seguridad de la información con buenas prácticas asociadas a los mismos. El Estándar cubre la gestión de la seguridad a nivel corporativo, las aplicaciones críticas del negocio, las instalaciones de los sistemas de información, las redes y el desarrollo de sistemas. El Estándar contiene:

  - FIRM, una metodología para el seguimiento y control del riesgo. o Una herramienta para la gestión del riesgo. o SARA, otra metodología para analizar el riesgo en sistemas críticos. o SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.
  - SARA, otra metodología para analizar el riesgo en sistemas críticos.
  - Una herramienta para la gestión del riesgo.
  - SPRINT, una metodología para hacer análisis de impacto en el negocio y analizar el riesgo en sistemas importantes pero no críticos.

- **Norma ISO/IEC IS 27005.**

  La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PDCA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.

- **OCTAVE.**

  (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®), desarrollado en EEUU por el SEI, en un una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.

- **SP800-30 NIST Risk Management Guide for Information Technology Systems.**

  Desarrollado por el NIST estadounidense, es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

Evaluación Módulo 8

1. **Para realizar el análisis de riesgos se parte del inventario de activos completo:**

   - [ ] Verdadero
   - [ ] Falso
   - [ ] Sólo si el inventario es lo bastante reducido
   - [ ] Dejar en blanco

2. **El resultado del análisis de riesgos:**

   - [ ] Es un mapa de los riesgos de la organización
   - [ ] Es un listado de amenazas que acechan a la organización.
   - [ ] Es un informe de puntos fuertes y débiles de la organización
   - [ ] Dejar en blanco

3. **Las amenazas a las que está expuesta cualquier organización son:**

   - [ ] Internas y deliberadas
   - [ ] Externas y deliberadas
   - [ ] Internas, externas, deliberadas y accidentales
   - [ ] Dejar en blanco

4. **¿Qué metodología es mejor?**

   - [ ] Cualquiera de las comerciales
   - [ ] La que se ajuste a las necesidades de la organización
   - [ ] Las que tienen una herramienta asociada
   - [ ] Dejar en blanco