ISOTools EXCELLENCE

Las claves del Éxito
para la Gestión de Riesgos de Seguridad de la Información

ISO 27005. Identificar, calcular, controlar y mejorar la eficacia

ISOTools EXCELLENCE

RIESGOS Y SEGURIDAD

Las claves del Éxito para la Gestión de Riesgos

Identifique, calcule, controle y mejore la eficacia y eficiencia en la Gestión de Riesgos.

La ISO 27001 establece un Sistema de Gestión de Seguridad de la Información, cuyo elemento más importante es la Gestión de los Riesgos.

¿Qué significa Gestionar Riesgos?

Significa que, en primer lugar es necesario identificar los riesgos que afectan a la Organización, y en segundo lugar, es necesario establecer medidas de seguridad para reducir estos riesgos.

Por tanto dentro de la Gestión de riesgos podemos diferenciar principalmente 2 etapas: **Análisis y Tratamiento**.

Para desarrollar todo el proceso de análisis y tratamiento de los riesgos, es imprescindible establecer una Metodología, la cual definirá los pasos que se tienen que seguir para llevar a cabo la Gestión de Riesgos.

Actualmente existen muchas metodologías en el mercado pero todas tienen una serie de puntos en común, los cuales veremos a continuación.

1. Identificación de activos

Podemos considerar como activos: Impresoras, dispositivos de almacenamiento (discos duros externos, pendrives), aplicaciones, ordenadores, servidores, personas, etc.)

Todos estos elementos tienen información:

- **Impresora:** Hojas que se imprimen
- **Pendrives:** Información digital
- **Aplicaciones:** Información digital
- **Servidores:** Información digital
- **Empleados:** Conocimiento, e información de la Organización

No obstante también podemos identificar como activo elementos que no contienen información, pero que son imprescindibles para otros activos que sí la tienen. Por ejemplo: Una consola de aire acondicionado no contiene información, pero su funcionamiento implica que los servidores, que sí contienen información, no se sobrecalienten y se averíen.

También es importante identificar la dependencia que puede existir entre activos: Una aplicación funciona en un servidor, por tanto, si el servidor deja de funcionar, la aplicación también lo hará.

Por último, además de identificar los activos, también puede ser necesario y/o interesante valorarlos con respecto las 3 dimensiones de seguridad: Confidencialidad, Integridad y Disponibilidad.

Podemos categorizar los activos y definir diferentes tipos. Ejemplo: Hardware, Software, Personas, Información, etc

2. Identificación de amenazas y vulnerabilidades

Todos los activos de la Organización están expuestos a amenazas, y estas son explotadas por vulnerabilidades.

¿Qué es una amenaza? Cualquier problema que pueda afectar al negocio: Ingeniería social, catástrofe natural, troyanos, virus, etc.

¿Qué es una vulnerabilidad? Situación que provoca que una amenaza pueda producirse. Por ejemplo, imaginemos que en una Organización existe poca concienciación en seguridad de la información, esto (la vulnerabilidad) ocasionará que exista más probabilidad de que alguno de sus empleados se descargue un correo electrónico con un troyano o un virus (amenaza).

Lo recomendable suele ser identificar amenazas/vulnerabilidades por tipo de activo, lo cual nos ahorrará mucho trabajo, ya que todos los activos que estén bajo el paraguas de una misma categoría podrán compartir amenazas/vulnerabilidades. No obstante hay que hacer un análisis por cada activo y comprobar si las amenazas/vulnerabilidades que le corresponden por su categoría son adecuadas.

Casi todas las metodologías de gestión de riesgos, o al menos las más importantes, incluyen un catalogo de amenazas de donde se pueden seleccionar las que apliquen a cada activo.

3. Cálculo del nivel de riesgo

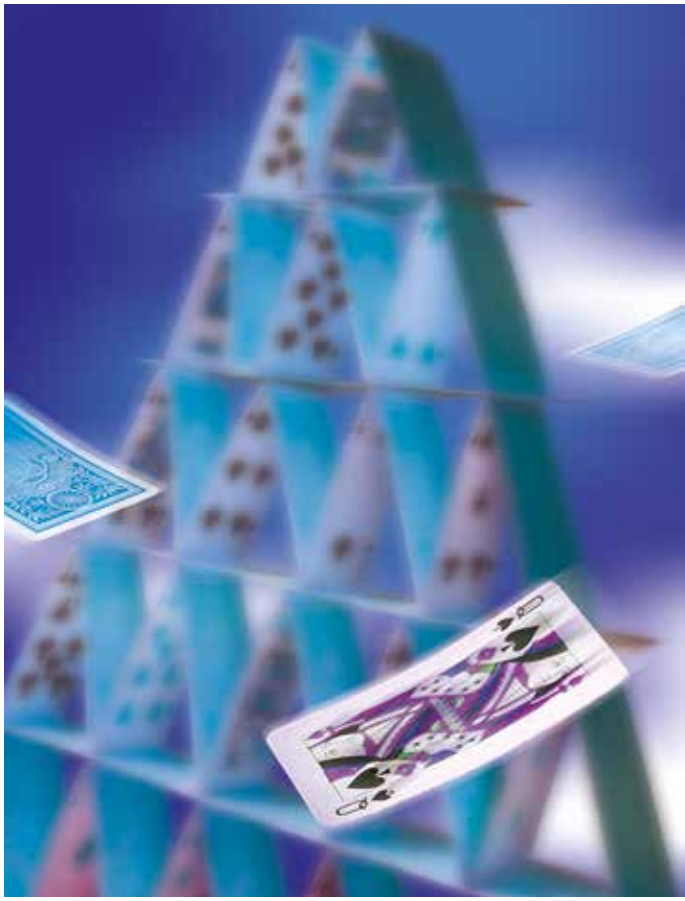
El cálculo del nivel de riesgo se realiza de manera distinta dependiendo de la metodología que se considere, ya que cada una utiliza una fórmula de cálculo distinta (probablemente esto sea lo que haga más distinta unas metodologías de otras). No obstante aquí veremos una fórmula sencilla y rápida de entender, basada en 2 parámetros fundamentales en gestión de riesgos:

- Probabilidad de que una amenaza se materialice.
- Impacto en la Organización resultante de la materialización de una amenaza.

En algunos casos también se considerará la valoración del activo (basada en las 3 dimensiones: Confidencialidad, Integridad y Disponibilidad).

Tanto el Impacto como la Probabilidad se pueden medir en valores porcentuales, lo cual nos resultará más sencillo a la hora de calcular el nivel de riesgo.

Una situación de **vulnerabilidad** en la Organización favorece que las **amenazas** se materialicen



Cálculo del nivel de riesgo

Impacto

- 0% — La amenaza no produce ningún daño
- 50% — La amenaza produce un daño considerable
- 100% — La amenaza produce un daño crítico

Probabilidad

- 0% — Poco probable que se materialice la amenaza
- 50% — Probabilidad considerable de que se materialice
- 100% — Probabilidad muy alta de que se materialice

- **Impacto:** Por ejemplo 0% si la amenaza no produce ningún daño, 50% si el daño es considerable y 100% si el daño es muy crítico para la Organización.
- **Probabilidad:** Por ejemplo 0% si la probabilidad de que la amenaza se materialice es muy baja, 50% si la probabilidad es considerable y 100% si la probabilidad es muy alta.

Al final, obtendremos un valor numérico para el riesgo, el cual representará lo siguiente:

- **Probabilidad de que una amenaza se materialice e impacto en la Organización en caso de que se materialice.**

El siguiente paso será determinar si este nivel de riesgo es aceptable para la Organización, es decir, si el nivel de riesgo detectado está por encima del nivel de riesgo aceptable.

¿Qué es el nivel de riesgo aceptable? Es el nivel de riesgo que establece la Organización como permitido, es decir, si el nivel de riesgo aceptable por ejemplo es medio, únicamente supondrá un peligro para la Organización aquellos riesgos que estén por encima: Alto.

Por tanto, si el nivel de riesgo está por encima del aceptable, tendremos que hacer un tratamiento del mismo con el objetivo de reducirlo (a un nivel aceptable).

Los controles de seguridad son fundamentales, ya que sin ellos los riesgos que están por encima del nivel aceptable supondrán un gran peligro para el negocio y la Organización.

4. Establecimiento de controles

Para aquellos riesgos que superen el nivel aceptable tendremos que aplicar controles. Para hacer esta implantación de controles de manera ordenada, estructurada y planificada, estableceremos un Plan de Tratamiento.

El definir un Plan para la implantación de los controles también es fundamental, ya que existirán muchos e implantarlos todos puede convertirse en un verdadero caos si no existe un orden, una estructura y una planificación.

El Plan de Tratamiento de Riesgos tiene que contener una serie de información básica:

- **Responsable del control:** Persona que se responsabiliza de la correcta implantación del control
- **Recursos:** Personas, técnicos, empresas externas o materiales que se utilizarán para la implantación del control
- **Acciones a llevar a cabo:** Acciones que serán necesarias para la implantación del control
- **Prioridad:** Todos los controles no tienen la misma prioridad, ya que por una parte el nivel de riesgo no será el mismo, ni tampoco el valor de cada activo para la Organización. Por tanto es necesario establecer prioridades. Esta prioridad puede venir determinada por la fecha de implantación de cada control.

Después de implantar todos los controles de seguridad, tenemos que calcular el riesgo residual.

¿Qué es el riesgo residual? Es el riesgo que sigue quedando después de implantar los controles de seguridad.

Cuando implantamos los controles reducimos el riesgo, pero este no dejará de existir, siempre quedará un nivel, aunque sea mínimo.

¿Qué ocurre si el nivel de riesgo, reducido por la implantación de los controles de seguridad, sigue estando por encima del nivel de riesgo aceptable?

Tendremos que tomar una decisión en cuanto al tratamiento, y deberá quedar formalmente establecido en nuestra metodología de análisis y tratamiento de riesgos.

Esta decisión se puede resumir en las siguientes posibilidades:

- **Asumir el riesgo:** La Organización conoce el riesgo y no puede establecer más recursos de los ya establecidos para reducirlo.
- **Transferirlo a otra parte:** Una compañía de seguros, una compañía externa, etc.

Metodologías existentes

1

MAGERIT

Se utiliza mucho en España, sobre todo en Administraciones Públicas, ya que fue desarrollada por el Consejo Superior de Administración Electrónica. Esta metodología no es muy conocida a nivel Internacional, aunque su utilización puede ser interesante en cualquier tipo de empresa.

2

CRAMM

Tuvo su origen en Reino Unido, ya que fue desarrollada por el CCTA (Central Computer and Telecommunications Agency). Tiene reconocimiento a nivel Internacional, y su desarrollo es de los más simples: Identificación y valoración de activos, valoración de amenazas y vulnerabilidades y selección de contramedidas.

3

OCTAVE

Fue desarrollada por el SEI (Software Engineering Institute) en Estados Unidos, y también tiene un gran reconocimiento internacional. Tiene una buena aceptación a nivel mundial, aunque las fases que la componen son un poco diferentes de las metodologías habituales, lo cual suele implicar mayor dificultad a la hora de utilizarla.

4

NIST 800-30

Fue desarrollada por el NIST (National Institute of Standards and Technology) en EEUU, y aunque tiene reconocimiento Internacional, su uso se limita sobre todo a EEUU (Administraciones Públicas). Aunque se compone de un mayor número de fases que las anteriores metodologías, es muy intuitiva, sencilla de utilizar.

5

ISO 27005

Es una norma ISO Internacional que no especifica ningún método de análisis de riesgo concreto sino que, contiene recomendaciones y directrices generales para la gestión de riesgos, por tanto, puede utilizarse como guía para elaborar una Metodología de gestión de riesgos propia.

6

ISO 31000

Al igual que la anterior, es una ISO Internacional que contiene una serie de buenas prácticas para gestionar riesgos, aunque la diferencia con respecto la ISO 27005, es que esta no aplica solamente a la Seguridad de la Información, sino que aplica a cualquier tipo de riesgo.

Conclusiones

- Todos los activos de una Organización (sea grande o pequeña) están expuestos a riesgos, los cuales si no se reducen pueden provocar un problema importante al negocio. Para reducir estos riesgos podemos implantar controles utilizando una metodología de análisis de riesgos.
- Una metodología de análisis de riesgos nos ayuda a identificar activos, las amenazas/vulnerabilidades que les afectan, y calcular el nivel de riesgo, el cual tiene que estar por debajo de un nivel aceptable para la Organización.
- Si el nivel de riesgo es superior al aceptable, la Organización tiene que implantar controles de seguridad para reducirlo.
- Existen muchas metodologías, pero todas tienen el mismo objetivo: calcular el riesgo asociado a los activos de la Organización y establecer medidas para reducirlo.

La Plataforma Tecnológica ISOTools le ayuda a automatizar la Gestión de Riesgos

ISOTools el la Plataforma Tecnológica idónea para facilitar la implementación y mantenimiento de su sistema de gestión de Riesgos, sea cual sea el tamaño y tipo de organización.

ISOTools permite la automatización del Sistema de Gestión del Riesgo, para la detección y control de amenazas de las organizaciones, mejorando la eficacia y eficiencia en la gestión, reduciendo riesgos y controlando incidencias.

Todo ello, gracias a una herramienta de fácil uso y amigable que permite la gestión y distribución práctica de tareas y responsabilidades con sistema de avisos y alarmas escalable.

ISOTools Excellence
www.isotools.org

Eventos ISOTools | **Próximos webinars** | **Contacte con ISOTools**