¡Fácil y sencillo! Análisis de riesgos en 6 pasos

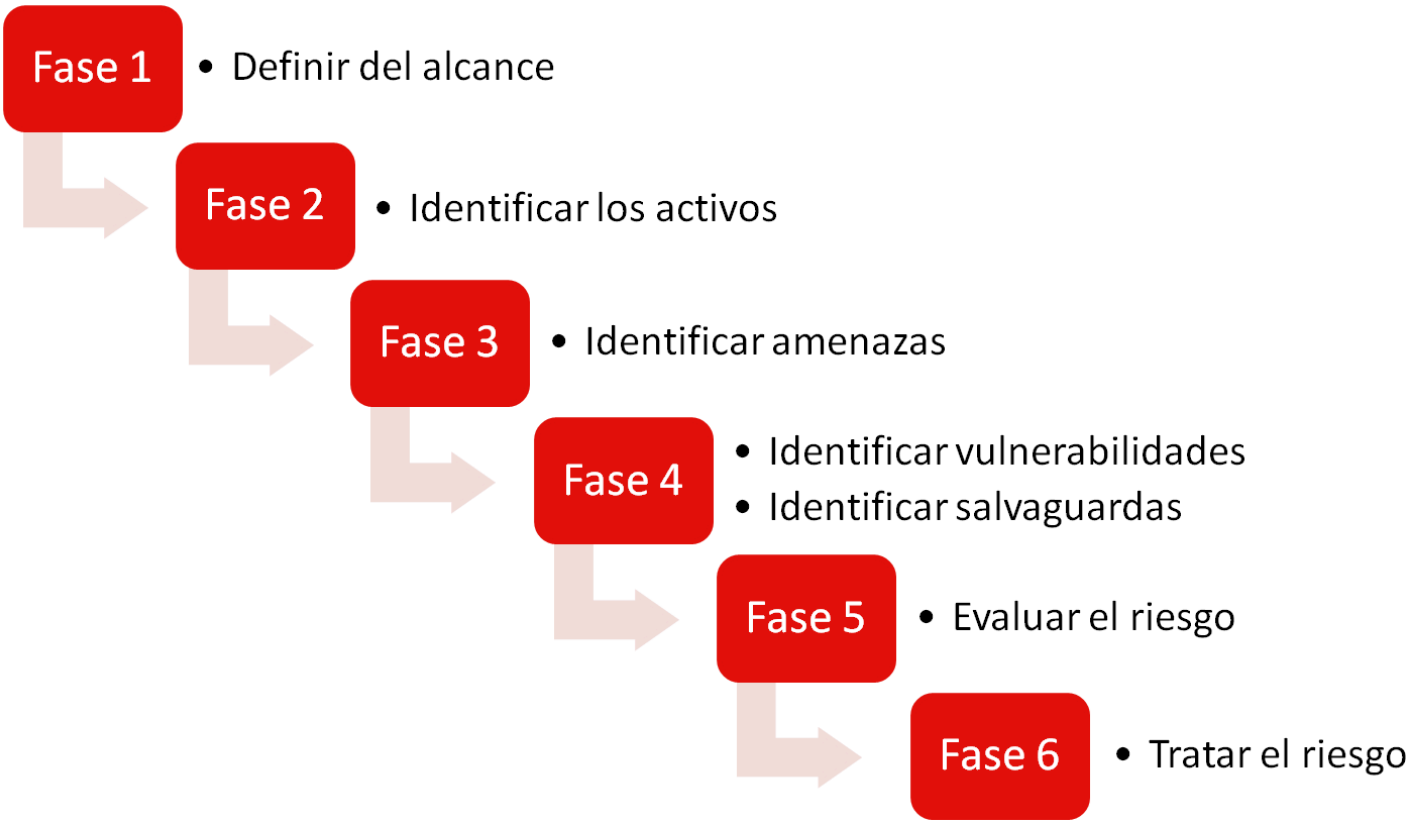
Fecha de publicación 16/01/2017

Autor
INCIBE (INCIBE)

Sin duda alguna, si queremos «empezar por el principio» en materia de ciberseguridad en nuestra empresa, el análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información. Si consideramos que las herramientas tecnológicas y la información que manejamos son de gran valor para nuestra organización debemos empezar a pensar en poner en práctica un **Plan Director de Seguridad**.

El Plan Director de Seguridad (PDS) se puede simplificar como la definición y priorización de un conjunto de proyectos en materia de seguridad de la información, dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables a partir de un análisis de la situación inicial. Llevar a cabo un buen análisis nos permitirá centrar nuestro foco de atención en los riesgos asociados a los sistemas, procesos y elementos dentro del alcance del PDS. De esta forma mitigaremos la posibilidad de tener algún **tipo de incidente de ciberseguridad**. Por otra parte, también podemos obtener beneficios si realizamos un análisis de riesgos de forma aislada en lugar de llevarlo a cabo dentro de un contexto mayor como es el del desarrollo de un PDS.

A continuación veremos de forma sencilla las principales tareas del análisis de riesgos, aportando recomendaciones prácticas sobre **cómo llevarlo a cabo**, y considerando algunas particularidades a tener en cuenta para que aporte el máximo valor al PDS. Cabe señalar que las fases o etapas que componen un análisis de riesgos dependen de la metodología escogida. En el caso que nos ocupa, hemos seleccionado un conjunto de fases que son comunes en la mayor parte de las metodologías para el análisis de riesgos.



Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. *Por ejemplo*, análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa, etc. En este caso práctico consideramos que el alcance escogido para el análisis de riesgos es “Los servicios y sistemas del Departamento Informática”.

Fase 2. Identificar los activos

Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla como la que se muestra a continuación a modo de ejemplo:

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Fase 3. Identificar / seleccionar las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado. *Por ejemplo*, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una cañería) o los daños por fuego, en lugar de plantearnos el riesgo de que el CPD sea destruido por un meteorito.

A la hora de identificar las amenazas, puede ser útil tomar como punto de partida el catálogo de amenazas que incluye la **metodología MAGERIT v3**.

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. *Por ejemplo,* una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.

Por otra parte, también analizaremos y documentaremos las medidas de seguridad implantadas en nuestra organización. *Por ejemplo*, es posible que hayamos instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) o un grupo electrógeno para abastecer de electricidad a los equipos del CPD. Ambas medidas de seguridad (también conocidas como salvaguardas) contribuyen a reducir el riesgo de las amenazas relacionadas con el corte de suministro eléctrico.

Estas consideraciones (vulnerabilidades y salvaguardas) debemos tenerlas en cuenta cuando vayamos a estimar la probabilidad y el impacto como veremos en la siguiente fase.

Fase 5. Evaluar el riesgo

Llegado a este punto disponemos de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Conjunto de medidas de seguridad implantadas

Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos. Pero para entenderlo mejor, veremos a modo de *ejemplo* las tablas para estimar los factores probabilidad e impacto.

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Cálculo del riesgo

A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO.

Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Tal y como indicábamos en el apartado anterior, cuando vayamos a estimar la probabilidad y el impacto debemos tener en cuenta las vulnerabilidades y salvaguardas existentes. *Por ejemplo,* la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (*Ej.* Servidores redundados), podemos considerar que el impacto será medio ya que estas medidas de seguridad harán que los procesos de negocio no se vean gravemente afectados por la caída del servidor. Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto. *Por ejemplo*, si los equipos de climatización del CPD no han recibido el mantenimiento recomendado por el fabricante, incrementaremos el impacto de amenazas como “condiciones ambientales inadecuadas” o “malfuncionamiento de los equipos debido a altas temperaturas”.

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. *Por ejemplo,* trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

- Transferir el riesgo a un tercero. *Por ejemplo*, contratando un **seguro** que cubra los daños a terceros ocasionados por fugas de información.
- Eliminar el riesgo. *Por ejemplo,* eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- Asumir el riesgo, siempre justificadamente. *Por ejemplo,* el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- Implantar medidas para mitigarlo. *Por ejemplo,* contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

Por último, cabe señalar que como realizamos este análisis de riesgos en el contexto de un **PDS**, las acciones e iniciativas para tratar los riesgos pasarán a formar parte del mismo. Por lo tanto, deberemos clasificarlas y priorizarlas considerando el resto de proyectos que forman parte del PDS. Asimismo, tal y como indicábamos en la introducción, llevar a cabo un análisis de riesgos nos proporciona información de gran valor y contribuye en gran medida a mejorar la seguridad de nuestra organización. Dada esta situación, animamos a nuestros lectores a llevar a cabo este tipo de proyectos ya bien sea de forma aislada o dentro del contexto de un proyecto mayor como es el caso del Plan Director de Seguridad.