THE BRIDGE

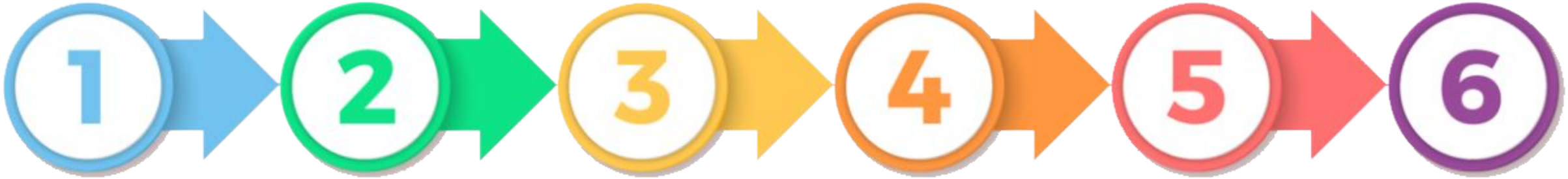
CYBER SECURITY

Análisis de Riesgo

Riesgo en ciberseguridad

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo



FASE 1:

DEFINIR EL ALCANCE DEL ANÁLISIS DE RIESGOS, es decir, dónde vamos a analizar los riesgos. Pueden ser todos los servicios, departamentos y actividades o centrarse en algunos en concreto.

FASE 2:

IDENTIFICAR Y VALORAR LOS ACTIVOS DE INFORMACIÓN del departamento, proceso o sistema objeto del estudio.

FASE 3:

IDENTIFICAR LAS AMENAZAS a las que están expuestos estos activos.

FASE 4:

ESTUDIO Y ANÁLISIS DE LAS CARACTERÍSTICAS DE NUESTROS ACTIVOS para identificar los puntos débiles o vulnerabilidades y las salvaguardas existentes.

FASE 5:

PARA CADA PAR ACTIVO-AMENAZA, estimaremos la **PROBABILIDAD** de que la amenaza se materialice y el **IMPACTO** sobre el negocio que esto produciría.

FASE 6:

Una vez calculado el riesgo, debemos **TRATAR AQUELLOS RIESGOS QUE SUPEREN UN LÍMITE** que nosotros mismos hayamos establecido.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

FASE 1:

DEFINIR EL ALCANCE DEL ANÁLISIS DE RIESGOS, es decir, dónde vamos a analizar los riesgos. Pueden ser todos los servicios, departamentos y actividades o centrarse en algunos en concreto.

- 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.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

FASE 2:

IDENTIFICAR Y VALORAR LOS ACTIVOS DE INFORMACIÓN del departamento, proceso o sistema objeto del estudio.

- 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
...						

- O pueden usarme **herramientas** como MS System Center, SIEM, Nagios, Zabbix, etc.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

FASE 3:

IDENTIFICAR LAS AMENAZAS

a las que están expuestos estos activos.

- 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
  - Ejemplo de metodología: MAGERIT v3.
- Algunos ejemplos de amenazas son:
  - Malware.
  - Phishing.
  - Ataques de fuerza bruta.
  - Ataques de denegación de servicio (DoS).
  - Robo de datos.
  - Exploits.
  - Ingeniería social.
  - Ataques a aplicaciones web.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

FASE 4:

ESTUDIO Y ANÁLISIS DE LAS CARACTERÍSTICAS DE NUESTROS ACTIVOS para identificar los puntos débiles o vulnerabilidades y las salvaguardas existentes.

- 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 cuyos sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante.
  - Otro ejemplo es no tener una red segregada por lo que todos los activos están en un mismo segmento de red lo que puede generar que en un ataque de **Ransomware** se puedan infectar todos los ordenadores conectados.
- 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.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

FASE 5:

PARA CADA PAR ACTIVO-AMENAZA, estimaremos la PROBABILIDAD de que la amenaza se materialice y el IMPACTO sobre el negocio que esto produciría.

- 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.

  - Ejemplo de 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.

- Ejemplo de 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.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

Tomamos los siguientes criterios para el Impacto.

Rango impacto / Descripción		Descripción	Pérdidas financieras	Pérdida del activo(s)	Reputación e imagen	Disminución de rendimiento
5	Catastrófico	> 6 % del presupuesto	Total	Mayor que un mes	Alta y muy extendida	> 50 % de variación en los indicadores
4	Desastroso	6% del Presupuesto	Muy gran impacto	De una semana a un mes	Media y muy extendida	25-50 % variación en los indicadores
3	Serio	2% del presupuesto	Gran impacto	De un día a una semana	Media y poco extendida	10-25% variación en los indicadores
2	Menor	1% del presupuesto	Impacto menor	½ día o 1 día	Baja y muy extendida	5-10 % variación en los indicadores
1	Insignificante	< 0,5 % del presupuesto	Casi sin impacto	Menor de ½ día	Baja y poco extendida	Hasta 5% variación en los indicadores

https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario

Fases en el análisis de Riesgo

FASE 5:

PARA CADA PAR ACTIVO-AMENAZA, estimaremos la PROBABILIDAD de que la amenaza se materialice y el IMPACTO sobre el negocio que esto produciría.

- **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

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

- Ejemplo de Matrix de Riesgo.
  - **Probabilidad**: Casi seguro (5), Muy probable (4), Posible (3), Improbable (2), Muy improbable (1)
  - **Impacto**: Insignificante (1), Menor (2), Serio (3), Desastroso (4), Catastrófico (5)
- Cada celda muestra un número que es el producto de la probabilidad por el impacto.
- Los **colores** indican el nivel de riesgo: bajo o verde (1-4), medio o azul (5-10), alto o amarillo (12-15) y critico o rojo (16-25).

Casi seguro	5	5	10	15	20	25
Muy probable	4	4	8	12	16	20
Posible	3	3	6	9	12	15
Improbable	2	2	4	6	8	10
Muy improbable	1	1	2	3	4	5
Probabilidad	x	1	2	3	4	5
	Impacto	Insignificante	Menor	Serio	Desastroso	Catastrófico

Tabla 2 *Estimación del producto «probabilidad x impacto» para evaluar riesgos*

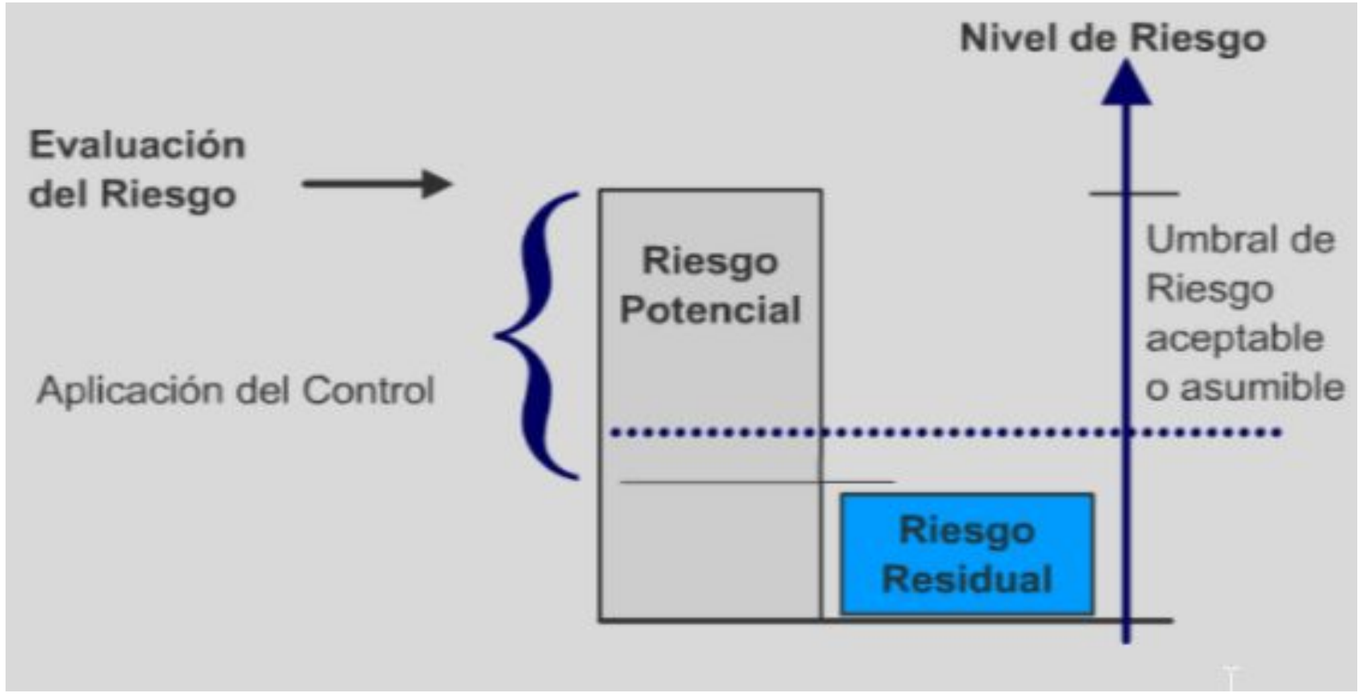
https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario

Riesgo Residual

- El **riesgo residual** es el nivel de riesgo que queda después de que se han implementado todas las medidas de control o mitigación posibles.
- En otras palabras, es el riesgo que persiste incluso después de haber tomado todas las precauciones razonables para reducirlo.
- Para calcularlo, generalmente se sigue un proceso:
  - **Identificación del riesgo**: Identificar los posibles riesgos.
  - **Evaluación del riesgo inicial**: Evaluar el nivel de riesgo antes de aplicar cualquier control.
  - **Implementación de controles**: Aplicar medidas para reducir el riesgo.
  - **Evaluación del riesgo residual**: Evaluar el riesgo que queda después de aplicar los controles.
- La fórmula básica suele ser:

  Riesgo Residual = **Riesgo Inherente** - **Eficacia de los Controles**

- **Siempre hay "Riesgo Residual".**



Fases en el análisis de Riesgo

FASE 6:

Una vez calculado el riesgo, debemos TRATAR AQUELLOS RIESGOS QUE SUPEREN UN LÍMITE que nosotros mismos hayamos establecido.

- 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. Por ejemplo: 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 hacer una segregación de red en un ambiente de control 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.

https://www.incibe.es/empresas/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Fases en el análisis de Riesgo

- Ejemplo del tratamiento de Riesgo

FASE 6:

Una vez calculado el riesgo, debemos **TRATAR AQUELLOS RIESGOS QUE SUPEREN UN LÍMITE** que nosotros mismos hayamos establecido.

Coste-Beneficio	Tratamiento
El coste del tratamiento es muy superior a los beneficios.	**Evitar el riesgo**, por ejemplo, dejando de realizar esa actividad.
El coste del tratamiento es adecuado a los beneficios.	**Reducir o mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.
El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.	**Transferir el riesgo, por ejemplo**, contratando un seguro o subcontratando el servicio.
El nivel de riesgo está muy alejado del nivel de tolerancia.	**Retener o aceptar el riesgo** sin implementar controles adicionales. Monitorizarlo para confirmar que no se incrementa.

https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario


THE
BRIDGE