AEINSE G34/23
Evaluación del riesgo y los Proyectos de Seguridad

Autores:

Iván Ballesteros Ballesteros

Revisores:

Alfonso Bilbao Iglesias
Pedro Carpintero Pérez
Carlos Martínez Hernández
Domingo Martínez Lacal

Diciembre 2023

Índice

1 Introducción 3
2 Establecer un sistema de gestión de riesgos 6
3 Evaluación de los riesgos 8
3.1 Identificación de los riesgos 8
3.2 Análisis de los riesgos 10
3.2.1 Análisis de las consecuencias 10
3.2.2 Análisis de la amenaza 11
3.2.3 Análisis de la vulnerabilidad 12
3.3 Valoración del riesgo 12
4 Tratamiento del riesgo 14
5 Otros documentos de aplicación 15

1 Introducción

El objeto de esta Guía es definir los criterios que se deberán tener en cuenta para la realización de la Evaluación de Riesgos, como un proceso formal de gestión de la seguridad basada en el riesgo.

Según se vio en la Guía 30/23 y 31/23, y posteriormente en la Guía 34/23, la parte más importante para la realización de un proyecto de seguridad es la realización de un correcto Análisis de Riesgos. Se puede decir al el Análisis de Riesgos es la "clave de bóveda" de todo el proyecto de seguridad.

El primer punto de esta guía de buenas prácticas es poner en contexto la evaluación del riesgo que debe realizarse en los proyectos de seguridad, dentro del proceso de gestión del riesgo de las empresas. Y para ello, será necesario incluir algunos conceptos.

Esta guía se refiere a un Proyecto de seguridad, en relación con las medidas de seguridad electrónica que se instalen para moderar el riesgo frente a amenazas de origen antisocial.

¿Qué significa riesgo de origen antisocial?

A partir de la definición de riesgo de la norma UNE-ISO 31000, podemos decir que **el riesgo de origen antisocial** es el efecto de la incertidumbre que las amenazas de origen antisocial proporcionan a los objetivos de la organización. Estas amenazas son generadas de forma deliberada por las personas.

¿Qué significa gestión del riesgo de seguridad?

La gestión del riesgo de seguridad son las actividades coordinadas para dirigir y controlar la organización con relación a los riesgos de seguridad.

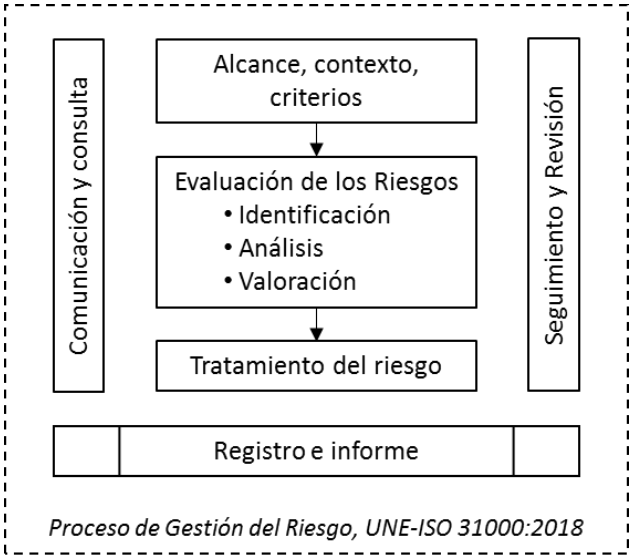
¿Quién es responsable de las actividades de la organización en relación con la seguridad?

Según la Guía UNE-ISO GUIA 73 IN, el **dueño del riesgo** es la persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

En organizaciones de cierto tamaño es habitual que el dueño del riesgo delegue total o parcialmente, en una persona o entidad, las actividades para la gestión de los riesgos de seguridad.

¿Qué es la evaluación del riesgo?

La norma UNE-ISO 31000 establece las directrices para implantar un sistema de trabajo para la gestión del riesgo. El estándar incluye el proceso para la gestión del riesgo, que es una pieza clave para entender el contexto de la evaluación de los riesgos en los proyectos de seguridad.



Proceso de Gestión del Riesgo, UNE-ISO 31000:2018

La evaluación del riesgo es el proceso de identificación, análisis y valoración del riesgo, para establecer un valor o indicador de este que permita tomar decisiones sobre el tratamiento de los riesgos.

El paso posterior a la evaluación corresponde con el tratamiento del riesgo. En este proceso se desarrollan actividades clave para la gestión de riesgo:

- Clasificación de los riesgos para su tratamiento.
- Diseño de medidas o controles para reducir el riesgo y mitigar sus efectos.
- Evaluación del riesgo residual.

¿Se debe hacer una evaluación del riesgo con posterioridad a la decisión de acometer un proyecto de instalaciones de seguridad?

Si nos apoyamos en el proceso de gestión del riesgo de la ISO 31000, se observa que, una vez finalizada la fase de evaluación del riesgo, corresponde a la fase de tratamiento decidir sobre los controles necesarios a aplicar en un proyecto de instalaciones.

No obstante, hay muchos casos en los que la realización del proyecto no corresponde con una respuesta al tratamiento del riesgo después de un proceso formal de evaluación. Ante esta situación, se recomienda hacer con el proyecto la correspondiente evaluación de riesgos.

A continuación se citan algunos ejemplos, en los que usualmente no se toma la decisión de tratamiento en base a un proceso de gestión de la seguridad basada en el riesgo:

- Una instalación que se renueva por cumplimiento normativo de los equipos, o por su obsolescencia tecnológica, suele incluir el mismo número de elementos y en las mismas posiciones que la instalación inicial hace muchos años ¿Han cambiado los riesgos en el tiempo? ¿Por qué se instalan las mismas medidas?
- La construcción de una instalación nueva sin contar con el futuro dueño del riesgo, donde el diseño da respuesta a buenas prácticas en la ubicación de elementos, pero no a una necesidad identificada en un análisis de riesgos y la decisión de tratamiento.

Es una buena práctica hacer una evaluación de riesgos antes de iniciar el proyecto (si no se cuenta con una evaluación previa). Esto permitirá abordar las deficiencias antes de la ejecución del proyecto. Sin embargo, deberá hacerse frente a las siguientes barreras:

- EL presupuesto no incluye una partida para realizar una evaluación de los riesgos.
- El presupuesto del proyecto suele estar cerrado, y no aceptar cambios.
- Es difícil justificar fases posteriores para abordar las deficiencias.
- No se han tenido en cuenta las necesidades y aportaciones del dueño del riesgo o su responsable de seguridad.

Realizar una evaluación de riesgos requiere recursos, y se recomienda que el proyecto de seguridad especifique una partida económica para ello.

¿En qué casos el proyecto de seguridad es producto de una evaluación de riesgos?

Volviendo al proceso de gestión del riesgo, el resultado del tratamiento del riesgo da origen a una propuesta para realizar un proyecto de instalaciones de seguridad, que debe ir acompañado de medidas de organización y de recursos humanos, todo esto podría plasmarse en un Plan de Seguridad de la instalación o en una modificación del existente.

El Plan de Seguridad de la instalación solo es obligado en algunos sujetos obligados, con un alcance especifico detallado en la normativa correspondiente o por la autoridad competente, como es el caso del Plan de Protección Específico “PPE” en las infraestructuras críticas, el Plan de Protección Física “PPF” de fuentes radioactivas, el Plan de Seguridad Ciudadana de instalaciones de pirotécnica o cartuchería, entre otros.

Este plan incluye, entre otras cosas, los medios técnicos (Proyecto de instalaciones de Seguridad), los medios organizativos y las personas para controlar la organización con relación a los riesgos de seguridad.

El Plan de Seguridad de la instalación es un elemento clave, y una buena práctica en la Gestión de los Riesgos de Seguridad. La redacción del plan de seguridad debe guardar proporcionalidad con las medidas de control a implantar.

Es importante indicar que el Plan de Seguridad de una instalación no es el Plan de las Operaciones de los Servicios de Vigilancia. El Plan de operaciones de los servicios de vigilancia debe redactarse acorde al alcance de los medios indicados en el plan de seguridad.

Si se aborda un proyecto de instalaciones de seguridad como respuesta a las medidas indicadas en un plan de seguridad, se debe haber tomado con anterioridad una decisión basada en los riesgos, y por lo tanto, la correspondiente evaluación del riesgo se ha realizado. En este caso no tiene sentido hacer una evaluación en el proyecto de instalaciones, pero es conveniente indicar la evaluación realizada.

2 Establecer un sistema de gestión de riesgos

No existe un sistema de gestión de riesgos de seguridad único. Los procesos del sistema se ajustan a las necesidades de la organización, la actividad de la empresa y su cultura en la gestión del riesgo.

La gestión de la seguridad basada en el riesgo puede apoyarse en la norma ISO 31000, o en el enfoque específico sobre seguridad que aporta ESRM (Enterprise Security Risk Management).

ESRM es un enfoque específico que facilita orientar la seguridad con los objetivos de la empresa, y se apoya en ISO31000, lo que facilita la implantación como sistema para la gestión del riesgo de seguridad.

¿Quién establece el sistema de gestión de la seguridad basada a en el riesgo?

En ocasiones, el sistema se establece a partir de obligaciones de cumplimiento, como es el caso de una infraestructura crítica. En el Plan de Seguridad del Operador "PSO" se refleja la gestión de la seguridad basada en el riesgo del Operador Critico. Y, mientras no se modifique el PSO, las sucesivas evaluaciones de riesgos que deben realizarse en el Plan de Protección Especifico "PPE" de la instalación, se realizan en base al sistema indicado en el PSO.

Otras veces, la organización de la seguridad en la empresa ha establecido su sistema de gestión del riesgo de la seguridad, que a su vez es coherente con su negocio y con el sistema de Gestión de Riesgos de la empresa.

Las empresas que no disponen de un sistema de seguridad basada en el riesgo tienden a apoyarse en sistemas de terceros para tomar decisiones sobre el tratamiento de los riesgos, con las siguientes dificultades:

- Las métricas de los sistemas de terceros no tienen porqué ser las adecuadas para las necesidades de la empresa.
- El valor del apetito[1] y tolerancia[2] por el riesgo no es igual para diferentes empresas.
- Tienen catálogos distintos de amenazas.
- Las técnicas sobre las que se apoyan son distintas.

El resultado, es que un sistema de gestión de riesgos de terceros:

- Requiere ajustar las métricas y el apetito de riesgo a la empresa.
- Ajustar el catálogo de amenazas a la empresa.
- Debe implantarse en la empresa.

[1] Apetito por el riesgo: Cantidad y tipo de riesgo que una organización está preparada para buscar o retener.
[2] Tolerancia al riesgo: Disponibilidad de una organización para soportar el riesgo después del tratamiento del riesgo con el objeto de conseguir sus resultados.

¿Puede utilizarse un sistema de terceros que no esté implantado en la empresa?

Se puede emplear un sistema que no esté implantado en la empresa, pero los beneficios serán limitados, y habrá de tenerse en cuenta lo citado en los párrafos anteriores. Únicamente ~~nos va a~~ permitirá priorizar el tratamiento de los riesgos de seguridad en el momento de la evaluación.

Aunque desde esta guía se recomienda que las empresas implanten un sistema de gestión de los riesgos de seguridad, propio o de terceros, la practica más habitual en los proyectos de seguridad es que el sistema de gestión sea de un tercero y no este implantado en la empresa.

Dentro de las opciones de una evaluación basada en un sistema de terceros, se encuentran dos modalidades, un sistema de terceros propietario o un sistema de terceros basado en una metodología abierta y conocida. Ambas opciones pueden ser adecuadas, mientras que la primera suele corresponder con enfoques específicos, las segundas son más conocidas, de enfoque general y con menos dependencia de terceros.

Entre las opciones abiertas más conocidas en seguridad mencionamos:

- Método Mosler o Penta, empleado ampliamente desde los años 90 en España e Iberoamérica.
  Este método se focaliza en el análisis y evaluación de los riesgos, siendo su mayor fortaleza los factores para evaluar el impacto, y su mayor debilidad, las métricas para evaluar la amenaza y la vulnerabilidad.
- Método Willian T. Fine, "Mathematical evaluations for controlling hazards (1971)". Originario en el control de accidentes con fines de prevención en US Navy. Sigue siendo un método muy conocido en prevención y utilizado en otros riesgos. En España ~~lo aplicamos~~ se aplica desde los años 90 en la gestión de los riesgos de la seguridad.
  Este método tiene las ventajas que permite un análisis cuantitativo o cualitativo de las consecuencias, las métricas facilitan la discriminación de los resultados, e incluye una evaluación de los controles propuestos.
- "Guideline: General Security Risk Assesment", de ASIS International. Propone una metodología completa, muy orientada a las necesidades para una evaluación de los riesgos de la seguridad, incluye un proceso general para la evaluación de estos, permite evaluaciones cualitativas y cuantitativas, pero es una directriz, y requiere desarrollar con las técnicas para la evaluación de los riesgos.
- MAGERIT versión 3.0 "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". Propone una metodología con mucho recorrido, pero que requiere desarrollar su aplicación.

En la medida que se utilicen metodologías más específicas para la evaluación de riesgos, se puede observar que están construidas con técnicas muy concretas, la mayoría incluidas en la norma UNE-ISO 31010, y que permite ajustar mejor la evaluación al caso particular.

Entre las técnicas más utilizadas de esta norma por las metodologías para la evaluación de riesgo tenemos:

- Índices de riesgo.
- Matriz de probabilidad/consecuencia.

Entre las técnicas de apoyo más utilizadas, durante el proceso de evaluación de riesgos se encuentran:

- Tormenta de ideas.
- Entrevistas.
- Listas de verificación.
- Análisis preliminar de peligros.
- Análisis "y si…" (SWIFT).
- Análisis de escenario.
- Análisis de impacto en el negocio (BIA).
- Análisis de árbol de fallos.
- Análisis de árbol de sucesos.
- Análisis causa efecto o diagrama de espina de pescado.
- Análisis del árbol de decisiones.
- Análisis de pajarita.
- Análisis coste/beneficio.

3 Evaluación de los riesgos

La finalidad de la evaluación del riesgo corresponde con obtener indicadores que apoyen las decisiones que se tomarán durante la etapa posterior del tratamiento. Por lo tanto, la información que aporta debe ser adecuada para determinar las medidas que deberían implementarse, modificarse o reducirse para mitigar o moderar el riesgo.

La evaluación de los riesgos tiene tres procesos:

- Identificación.
- Análisis.
- Valoración de los riesgos.

3.1 Identificación de los riesgos

La identificación de los riesgos es el punto de partida para la evaluación, el resultado de este proceso se corresponde con un listado de los riesgos que serán analizados posteriormente por los factores de riesgo: consecuencia, amenaza y vulnerabilidad.

La identificación de los riesgos es una etapa relevante del proceso, los errores pueden conducir a un resultado inaceptable del proceso:

- Errores de alcance, cuando no se identifiquen riesgos que afecte significativamente al negocio.
- Errores de eficiencia, cuando se han identificado un elevado número de riesgos irrelevantes, que requieren recursos en su análisis y no influyen en la consecución de los objetivos de la organización.

La norma ISO 31000 indica algunos de los elementos para tener en cuenta para la identificación de los riesgos, pero no establece un método para ello.

Considerando la relevancia de la identificación de los riesgos de seguridad en el éxito de su evaluación, se puede apoyar este análisis en el enfoque ESRM para ello:

- Crear un listado de los activos y recursos que pueden influir significativamente en los objetivos de la organización.
- Crear un listado de las amenazas, su definición y las características del adversario esperado.
- Crear una matriz de activos y recursos versus las amenazas (Mapa de amenazas)
- Identificar los riesgos, como las posiciones de la matriz en las que las amenazas pueden afectar significativamente a los activos y recursos identificados.
- Si los riesgos se ven afectados de manera significativa por alguna circunstancia. Se repetirá el proceso anterior para cada una de las circunstancias identificadas. Por ejemplo: En horario de apertura y en horario de cierre, cadena de suministro comprometida o no comprometida, etc.

El resultado de este proceso ofrecerá una matriz de "n" activos por "m" amenazas, como la mostrada a continuación. Los riesgos quedan identificados, como las amenazas que aplican de forma plausible con un daño significativo en los activos o recursos.

Ref.	Amenaza	Activo 1	Activo 2	Activo 3	…	Activo n
1	Hurto	No Aplica	No Aplica	Aplica	…	No Aplica
2	Apropiación indebida	No Aplica	No Aplica	No Aplica	…	No Aplica
3	Ocupación indebida	No Aplica	No Aplica	No Aplica	…	Aplica
4	Ocupación con fuerza	No Aplica	No Aplica	No aplica	…	No Aplica
5	Daños con dolo contra los bienes	Aplica	Aplica	Aplica	…	Aplica
6	Usurpación de identidad	No Aplica	Aplica	Aplica	…	Aplica
7	Acusación y denuncia falsa	No Aplica	No Aplica	No aplica	…	No Aplica
8	Fraude	No Aplica	No Aplica	No Aplica	…	Aplica
9	Robo con fuerza hacia las cosas	Aplica	No Aplica	Aplica	…	No Aplica
10	Robo con violencia hacia las personas (atraco)	No Aplica	No Aplica	No Aplica	…	No Aplica
11	Agresión a personas	No Aplica	No Aplica	No aplica	…	No Aplica
…	…	…	…	…	…	…
m	Amenaza m	No Aplica	No Aplica	No aplica	…	No Aplica

De esta forma, en la siguiente fase, los recursos se orientan a analizar los riesgos que pueden influir significativamente en los resultados de la organización.

Como referencia, a continuación, se incluye una lista de amenazas básicas y sus correspondientes definiciones.

1. **Hurto:** Apropiación de bienes en general, con ánimo de lucro y contra la voluntad del dueño, sin empleo de la fuerza hacia las cosas, ni herramientas lógicas, ni intimidación o fuerza hacia las personas.
2. **Apropiación indebida:** Apropiación de bienes, para beneficio propio o de un tercero, que les hubiesen sido confiados y que, llegado el momento se niegue su devolución.

3. **Ocupación indebida:** Ocupación sin autorización de espacios, para su disfrute o para impedir su uso por el dueño. Incluye el activismo.
4. **Ocupación con fuerza:** Ocupación de espacios, con fuerza hacia las cosas, para su disfrute o para impedir su uso por el dueño.
5. **Daños con dolo contra los bienes o vandalismo:** Daños o destrucción intencionada de un bien con disminución de su valor tangible o intangible, o del servicio que aporta al dueño.
6. **Fraude:** Utilización del engaño para obtener algún beneficio en el cumplimiento de los contratos.
7. **Robo con fuerza hacia las cosas:** Apropiación de bienes para obtener algún beneficio, empleando fuerza en las cosas para acceder o abandonar el lugar donde éstas se encuentran.
8. **Robo con violencia hacia las personas o atraco:** Apropiación de bienes para obtener algún beneficio, empleando violencia o intimidación en las personas.
9. **Agresión a personas:** Causar una lesión que menoscabe la integridad corporal, la salud física o mental de una persona.
10. **Tráfico y consumo de sustancias prohibidas:** El tráfico ilícito de drogas tóxicas, estupefacientes y sustancias psicotrópicas, la posesión ilegal de éstas con dichos fines, así como las actividades que promuevan, favorezcan o faciliten su consumo ilegal.
11. **Sabotaje:** Acción deliberada dirigida a manipular, dañar o destruir bienes, con el objeto de anular el funcionamiento del equipo o del proceso que soporta.
12. **Amenaza bomba:** Acción de dar aviso falso de colocación de un artefacto explosivo con la finalidad de detener un proceso, producir daños psicológicos a las personas o como táctica terrorista.
13. **Artefacto incendiario o explosivo:** Acciones destinadas a producir daños a los activos y/o las personas mediante colocación de artefactos explosivos o incendiarios, en el interior o exterior de recintos o edificios. Puede también ser lanzado o portado por personas o a través de dispositivos tripulados o no tripulados.
14. **Ataque con arma blanca o armas de fuego:** Ataque con armas convencionales, destinado a producir daños físicos o psicológicos a las personas.
15. **Secuestro:** Acción dirigida a privar de la libertad a las personas o tomar las instalaciones para obtener un rescate u otras exigencias.
16. **Saqueos:** Es el apoderamiento ilegítimo e indiscriminado de bienes ajenos por la fuerza, como parte de una victoria política, por algún tipo de reivindicación, o como medida de coacción a decisiones políticas.
17. **Chantaje, Soborno, Extorsión o Coacción:** Acciones contra el personal del Instituto encaminadas a obtener de forma deliberada información protegida.

3.2 Análisis de los riesgos

3.2.1 Análisis de las consecuencias

Evaluar las consecuencias, impacto o trascendencia para cada uno de los riesgos es uno de los aspectos más delicados en el proyecto. Ni el analista de los riesgos, ni el responsable de seguridad disponen de tanto conocimiento e información sobre el impacto en el negocio que el dueño del riesgo.

Por lo tanto, se propondrán impactos en base a hipótesis, para permitir que el dueño del riesgo opine sobre lo indicado va a fortalecer la aceptación del análisis. Esto lo podemos hacer mediante distintas técnicas:

La propuesta de impactos en base a hipótesis se puede realizar por distintas técnicas:

- Aplicando la evaluación cualitativa de un experto, que conoce los procesos y los activos.
- Analizando la interrupción de los procesos a partir de un BIA (Business Impact Analysis) formal o similar.
- Cualquier otra técnica que permita analizar las consecuencias y establecer su valor.
- Aplicando las pérdidas totales, calculadas en base a los factores propuestos en "Guideline: General Security Risk Assesment", de ASIS International, donde:

$$K = C_p + C_t + C_r + C_i - I$$

Donde:

K: Criticidad, coste total de perdidas.
Cp: Coste de reemplazo permanente.
Ct: Coste de reemplazo temporal.
Cr: Otros costes asociados al incidente.
Ci: Coste de pérdidas de ingresos, o lucro cesante.
I: Indemnización del seguro.

Debe tenerse en cuenta que el cobro de la indemnización del seguro es un proceso posterior al incidente que produce el daño. El importe de la indemnización es una compensación por el riesgo asumido, y no se conocerá hasta tanto no se cierre el acuerdo con el seguro, y por lo tanto el cobro y su importe será incierto.

Al ser una compensación por el riesgo asumido, es una buena práctica no incluirlo para calcular la reducción de las consecuencias del riesgo.

El resultado final del análisis de las consecuencias del riesgo corresponde con un valor cualitativo o cuantitativo que será utilizado para la valoración del riesgo.

Generalmente, el valor de las consecuencias se obtiene por métodos numéricos, o mediante la aplicación de un índice de consecuencias, o por una matriz para los valores cualitativos.

3.2.2 Análisis de la amenaza

El análisis de la amenaza corresponde con un proceso que requiere conocimiento sobre el adversario, y que puede ser distinto para cada amenaza.

Para amenazas con sucesos frecuentes, es muy adecuado aplicar un estudio frecuencial para determinar la probabilidad de ocurrencia en base a los eventos conocidos. No se puede considerar las situaciones de peligro que no han dejado evidencia o han pasado inadvertidas.

Sin embargo, la mayoría de los riesgos de seguridad son por amenaza de baja probabilidad de ocurrencia, o potenciales incidentes que pudieron pasar inadvertidos, y los datos disponibles sobre estos no son suficientes para realizar un estudio frecuencial.

Para determinar el nivel de amenaza podemos evaluar los factores que pueden condicionar la amenaza, de forma cualitativa o cuantitativa, con apoyo de algunas técnicas de la UNE-ISO 31010 u otras técnicas reconocidas, o bien mediante el análisis de un experto.

El estándar ANSI/ASIS/RIMS RA.1 establece una guía muy completa de elementos para determinar la amenaza, la posibilidad de la amenaza y el nivel de amenaza.

Una vez determinado el nivel de amenaza, se aplica un índice de amenaza para obtener su valor numérico.

3.2.3 Análisis de la vulnerabilidad

El análisis de la vulnerabilidad evalúa cómo de accesible es el activo en riesgo para el atacante. Afectando, por tanto a la oportunidad de materializar el daño.

Este análisis puede realizarse asumiendo que no hay medidas de protección instaladas (caso de un nuevo proyecto) o considerando las medidas de protección existentes o las que se proponen instalarse.

Para analizar la vulnerabilidad en el segundo caso hay que considerar todas las medidas de seguridad (medidas técnicas, humanas y organizativas) así como los elementos que influyen para materializar el daño.

Entre los aspectos que han de tomarse para analizar la vulnerabilidad:

- La eficiencia de los controles de seguridad.
- El tipo de activo a proteger, y su atractivo para adversarios capacitados.
- Los grupos de interés involucrados y el nivel de compromiso con los objetivos de la organización.
- Alineación de los intereses de los potenciales adversarios.
- El tiempo necesario, y la intensidad del ataque para materializar en daño.
- Efectos en cascada y colaterales, así como la eficiencia de los controles asociados.

Las técnicas más frecuentes para analizar la vulnerabilidad son:

- La comprensión del daño como un evento y el uso de técnicas de probabilidad.
- El análisis experto y el uso de técnicas de la UNE-ISO 31010 u otras técnicas reconocidas.

Una vez determinado el valor de la vulnerabilidad, según la metodología, se puede aplicar su valor como probabilidad de que el daño se produzca en caso de que se materialice la amenaza, o bien mediante un indicador asociado a su valor.

3.3 Valoración del riesgo

La valoración del riesgo es el proceso que establece el valor del índice de riesgo acorde a la metodología aplicada (Las métricas de la metodología deben ser ajustadas al objeto del análisis).

Las metodologías establecen la valoración del riesgo a partir de los factores de riesgo que se han definido. Los factores de riesgo generalmente utilizados son: Consecuencias (C), Amenaza (A) y Vulnerabilidad (V).

Generalmente, el cálculo será cuantitativo cuando los factores de riesgo tienen un valor numérico, producto de un índice del factor de riesgo, o de un proceso de cálculo más amplio. En este caso, el índice de riesgo es una función matemática de los tres factores de riesgo, generalmente:

$$R = C * A * V$$

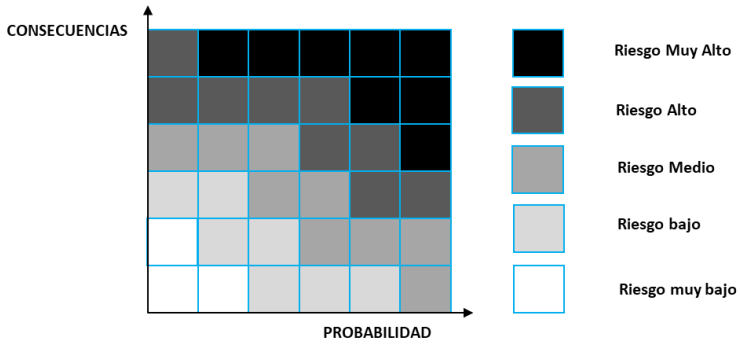
Donde:

R: Riesgo.
C: Consecuencias.
A: Amenaza.
V: Vulnerabilidad.

Deberá evitarse la confusión de los términos. Las metodologías emplean algunas variables con otros nombres para facilitar o diferenciar el proceso de análisis en cada uno de sus factores.

A partir del índice de riesgo, deberá clasificarse su valor como paso previo al Tratamiento de los riesgos. En general, los riesgos que se clasifiquen por encima del apetito y la tolerancia deberán tratarse para mitigar o moderar su valor.

En los casos en los que la metodología establece los factores de riesgo como un valor cualitativo, se aplican matrices para asignar los valores resultantes. Según el valor cualitativo de la Probabilidad y las Consecuencias, se obtiene el índice de riesgo.



A partir de valores cualitativos, de probabilidad y de consecuencias, se obtiene el índice de riesgos.

Es importante tener en cuenta que la aplicación de esta técnica:

- Permite mezclar valores cualitativos con valores cuantitativos.
- El valor de probabilidad se puede obtener a partir de la aplicación de otra matriz Amenaza/Vulnerabilidad, o de un proceso numérico, o de la aplicación de índices.
- El resultado del índice de riesgo aporta directamente la clasificación del riesgo. No se requiere un índice de clasificación como en el cálculo cuantitativo.

En términos generales, las evaluaciones cuantitativas se suelen aplicar a procesos complejos, para conseguir mayor objetividad, y las evaluaciones cualitativas a procesos rápidos para la evaluación.

4 Tratamiento del riesgo

El tratamiento del riesgo tiene la finalidad de abordar decisiones sobre aquellos riesgos que se han clasificado por encima del apetito y de la tolerancia al riesgo.

Por otra parte, los riesgos de origen antisocial con un valor por debajo del apetito son una oportunidad para reducir algunos controles, y mejorar la eficiencia del sistema de seguridad.

¿Qué es la tolerancia al riesgo?

Apoyándose nuevamente en la definición de la ISO GUIA 73, la tolerancia al riesgo es la disponibilidad de la organización para soportar el riesgo después del tratamiento con el fin de conseguir sus objetivos.

El criterio de apetito y tolerancia de los riesgos de origen antisocial deben establecerse en el inicio del proceso de gestión del riesgo, ser adecuados a la cultura del riesgo de la empresa.

Como norma general, en esta etapa el dueño del riesgo decidirá sobre el tratamiento de los riesgos que estén por encima de la tolerancia.

Las opciones de tratamiento conforme a la ISO 31000 son:

- Evitar el riesgo.
- Aceptar o aumentar el riesgo en búsqueda de una oportunidad.
- Eliminar la fuente de riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo.
- Retener el riesgo con base a una decisión informada del riesgo residual.

Los proyectos de seguridad se enfocan para tratar el riesgo a modificar la probabilidad y las consecuencias, pero debe tenerse presente que esto no significa que siempre sea la única o la opción más adecuada.

Las medidas que se propongan en el proyecto deben ser eficientes respecto a la cantidad de riesgo que se modifique.

Una vez diseñadas las medidas, deberá evaluarse nuevamente el riesgo, obteniéndose el denominado “riesgo residual”. Los valores de riesgo inicial, riesgo residual y el coste de las medidas influyen en el dueño del riesgo para decidir sobre el tratamiento.

Una vez decido el tratamiento del riesgo para modificar las consecuencias o la probabilidad mediante un proyecto de medidas de seguridad. El proyecto deberá implementarse y mantener el adecuado seguimiento y revisión.

5 Otros documentos de aplicación

- UNE-ISO GUIA 73 IN “Gestión del riesgo. Vocabulario”. Traducido por AENOR (Asociación Española de Normalización y Certificación), julio 2010.
- UNE-ISO 31000:2018 “Gestión del riesgo. Principios y Directrices”. Traducido por AENOR (Asociación Española de Normalización y Certificación), marzo 2018.
- UNE-ISO 31010:2011 “Gestión del riesgo. Técnicas de apreciación del riesgo”. Traducido por AENOR (Asociación Española de Normalización y Certificación), mayo 2011.
- ANSI/ASIS/RIMS RA.1-2015 “Evaluación de riesgos”. Traducido por AENOR (Asociación Española de Normalización y Certificación), 2016.
- ASIS ESRM-2019 “GUIDELINE Enterprise Security Risk Management”. ASIS INTERNATIONAL, 2019.
- ASIS “GUIDELINE General Security Risk Assesment”. Asis International, 2003.