ENRIQUE BILBAO LÁZARO. CUEVAVALIENTE INGENIEROS

Análisis de riesgos para un **departamento de Seguridad**

En una sociedad como la actual, los ciudadanos del primer mundo asumimos como ciertas y «normales» algunas cuestiones que históricamente no lo han sido tanto: nuestro entorno es relativamente seguro y predecible. Podemos llevar a cabo nuestro trabajo, desplazarnos, adquirir productos, disfrutar de nuestras propiedades, etc. El Estado, como agente directo o como regulador de otros agentes (empresas de Seguridad, entidades aseguradoras, etc.), asegura el sistema, poniendo a nuestra disposición servicios y una estructura de relaciones entre las personas y el resto de entidades que la componen, las cuales hacen posible disfrutar de esta burbuja de Seguridad.

NATURALMENTE, la realidad es mucho más compleja que esta mera percepción, y la incertidumbre, los errores y las malas intenciones de terceros llevan a tener que considerar desviaciones respecto a nuestra percepción de Seguridad.

Por otro lado, el concepto de Seguridad tiene un fuerte componente subjetivo, que atiende principalmente a la consideración de seguro como una percepción o sensación más que como un estado absoluto.

Aunque la toma de decisiones sobre inversiones pueda justificarse en percepciones o en sensaciones para un consumidor (me siento inseguro ergo invierto en mi seguridad), difícilmente puede sostenerse esta manera de actuar en un responsable de una empresa, a quien habitualmente se le requiere una justificación razonada y objetiva (dentro de lo posible) para la toma de decisiones.

La principal herramienta para medir la Seguridad y los riesgos que deben afrontarse es el Análisis de Riesgos. Se trata de una herramienta que pretende valorar la posibilidad o contingencia de que una acción (amenaza) se produzca sobre un activo (bien, área, persona, información…), y las previsibles consecuencias que esto supondría. Con ello, se pretende analizar acciones previsibles, y cuantificar a priori los efectos de éstas. Si la herramienta permite considerar en su proceso de análisis el efecto de incluir o no ciertas medidas de Seguridad, es evidente el alto valor que la misma puede tener para justificar la inversión en Seguridad.

Análisis de riesgos útil para el responsable de Seguridad actual

Naturalmente, a lo largo de los años han surgido múltiples metodologías de análisis de riesgos, adaptadas a las necesidades del momento y del sector al que se dirigían. No es objeto de este artículo analizar las más extendidas en España ni compararlas, ya que se trata de una tarea ingente y evidentemente subjetiva.

En lugar de esto, el artículo pretende compartir una reflexión sobre qué debe incluir un análisis de riesgos que pueda ser útil para un responsable de Seguridad.

La primera consideración a tener en cuenta es el contexto: amenazas y activos afectados que van a considerarse. Este contexto variará evidentemente en cada caso, debiendo cubrir los principales alcances y enfoques del departamento de Seguridad de que se trate. **Ver Grafico 1.**

Independientemente de los algoritmos de cálculo que se consideren, y que varían enormemente de acuerdo con la metodología estudiada, parece fundamental considerar al menos, de

cara a valorar las inversiones a considerar, el resultado del análisis de riesgos antes y después de implementar ciertas medidas de Seguridad. Una consideración habitual es la consideración de riesgos con y sin medidas de Seguridad:

- Riesgo inherente: sin considerar medidas de Seguridad.
- Riesgo residual: considerando medidas de Seguridad.

Para facilitar esta operación es conveniente que la metodología de análisis de riesgos esté ligada una propuesta, más o menos automática, de medidas de seguridad a implementar para paliar sus efectos. Esto permitirá comparar las medidas necesarias con las existentes y configurar un plan de acción tendente a disminuir los niveles de riesgo.

Para aquellos departamentos que han asumido un modelo de mejora continua en la gestión de sus riesgos, el análisis de riesgos es parte del proceso repetitivo en su fase de planificación. La evolución de sus riesgos se planifica mediante análisis de riesgos periódicos, los cuales suelen partir de un análisis de riesgos inicial en el que se consideran los riesgos inherentes y residuales, complementándose periódicamente con evaluaciones de las nuevas medidas de Seguridad que modifiquen los riesgos residuales.

Otra consideración fundamental es cómo se evalúa el impacto y sobre qué aspectos. Aunque existen diversas aproximaciones, es necesario tener en cuenta los intereses de cada responsabilidad de cada área de la empresa. Por ello, es frecuente analizar simultáneamente impactos económicos sobre la salud de las personas, al medioambiente, al patrimonio, legales, a la imagen de la empresa, etc. Todo ello, intentando encontrar escalas equivalentes comparativas entre diversos impactos (¿A cuántos heridos «equivale» una pérdida de 1 millón de euros?); y lo más objetivas posibles, lo que asegurará la coherencia de los análisis de riesgos en diversas instalaciones y momentos temporales.

Otro aspecto importante a tener en cuenta es que las medidas de Seguridad que se analizan (también denominadas controles cuando se habla de seguridad de la información), tengan en cuenta todas las alternativas a disposición de los responsables de Seguridad para disminuir los riesgos:

- Medidas Técnicas.
- Medidas Operativas.
- Medidas Organizativas.

Finalmente, es importante destacar que la metodología empleada sea acorde con normativa internacional de reconocido prestigio como, por ejemplo, las normas ISO 31000, ISO 27001, ISO 27002, MAGERIT II, AS/NZS 4360, ISO/TR 17944:2002.

Adaptación y aprovechamiento de análisis de riesgos existentes

Las empresas, independientemente de su ámbito de actuación, están cada día más acostumbradas a considerar la gestión de sus riesgos como parte de su propio negocio. Los riesgos políticos, económicos, etc., son analizados por diversas áreas.

Asimismo, es frecuente que diversos ámbitos de Seguridad (seguridad laboral, seguridad de la información, seguridad antisocial) de una empresa dispongan de análisis de riesgos independientes con información valiosa que debe aprovecharse.

Por este motivo, es importante, a la hora de abordar un nuevo análisis de riesgos, considerar la necesidad de adaptar o integrar los análisis existentes y buscar el modo en que toda esta información pueda aprovecharse.

Otra consideración que puede llevar a tener que asumir esta adaptación es la existencia de metodologías o de enfoques de obligado cumplimiento, que marquen ciertas pautas a considerar en los análisis de riesgos. Estas obligaciones de Compliance son frecuentes en ámbitos regulados, así como en lo concerniente a las Infraestructuras Críticas.

Grafico 1. Activos y Amenazas a considerar según el alcance del área de Seguridad.

Análisis de riesgos de Operadores Críticos

Los análisis de riesgos de las Infraestructuras Críticas están regulados por la legisla-

ción y reglamento correspondientes (Ley 8/2011 y Real Decreto 704/2011 que aprueba su Reglamento), así como por los manuales de mejores prácticas y de contenidos mínimos de los documentos que deben entregar los operadores (Plan de Seguridad del Operador, PSO y Plan de Protección Específico, PPE). Pese a que los operadores tienen libertad en cuanto a metodología a emplear, hay algunos puntos básicos que deben asumir en sus Análisis de Riesgos:

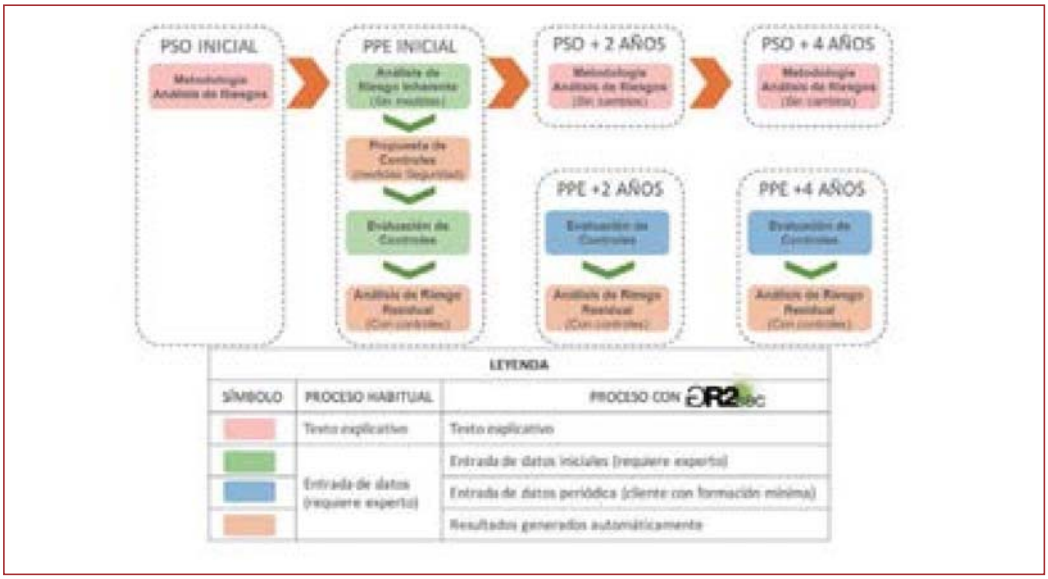

Grafico 2. Diferencia del proceso de análisis de riesgos para un operador crítico usando GR2Sec.

- Definición de la metodología de análisis de riesgos en el PSO.
- Realización de un análisis de riesgos de cada infraestructura crítica en su correspondiente PPE, debiéndose repetir cada dos años con la revisión del documento.
- Listado de amenazas consideradas, incluyendo aquellas facilitadas por el CNPIC a cada operador.
- Consideración de amenazas y activos físicos y lógicos, indiferentemente.
- Controles existentes para la mitigación del riesgo.
- Propuesta de controles (medidas de Seguridad) técnicos, operativos y organizativos, de acuerdo al análisis de riesgos, y estructurados como Plan de Acción
- Consideración de controles permanentes y temporales para adaptarse a diversos Niveles de Amenaza Antiterrorista (NAA).
- Consideración en la metodología de los conceptos probabilidad e impacto
- Consideración exclusivamente de los 4 criterios horizontales indicados en la citada Ley 8/2011 (daño a personas, al medioambiente, a la economía nacional y al servicio prestado), para la valoración de los impactos de cada amenaza sobre cada activo.

Debe destacarse, en este último punto, que los análisis de riesgos a incluir en los PPEs consideran el impacto como el daño que sufre la Sociedad, independientemente del que pueda sufrir la empresa. Esto supone que los análisis de riesgos realizados para los PPEs no son completos a nivel empresarial para la toma de decisiones de un departamento de Seguridad, ya que gran parte de las consecuencias no son analizadas.

Nivel de detalle y complejidad en el desarrollo del Análisis de Riesgos

Por último, es necesario tener en cuenta que gestionar los riesgos de un elevado número de activos con la realización de un análisis de riesgo muy detallado de los mismos puede ser impracticable, especialmente cuando los recursos son limitados. La toma de datos, en especial cuando existe una gran dispersión de activos, suele recaer en personal no especializado en análisis de riesgos o en evaluación de controles existentes, lo que también puede suponer una limitación en cuanto a qué metodología y variables pueden ser las más adecuadas.

En lo referente a estos últimos aspectos, nuestra experiencia desde Cuevaliente Ingenieros, como empresa enfocada y especializada en análisis de riesgos de Seguridad de todo tipo, nos hace concluir que deben elegirse metodologías y niveles de detalle con posibilidades de adecuación a cada circunstancia.

En este sentido, ponemos a disposición de nuestros clientes nuestra amplia experiencia en análisis de riesgos, incluyendo los de infraestructuras críticas de todos los sectores, así como una metodología y herramienta de gestión de riesgos de desarrollo propio ampliamente utilizada denominada GR2Sec de la que puede obtenerse información detallada en www.gr2sec.com.

Esta herramienta genera automáticamente datos del proceso de análisis de riesgos, pudiendo ser explotada por personal con una formación específica mínima, no necesariamente un consultor. En el gráfico 2 se muestra este proceso para el análisis de riesgos de PSOs y PPEs. ●

Fotos: Cuevaliente Ingenieros

Contactos de empresas, p. 9.