Análisis de riesgos integrado. Problema con solución

Enrique Bilbao Lázaro / Director técnico de Cuevavaliente Ingenieros

En el interesante trabajo de la Fundación Borredá titulado *10 años de Sistema PIC. Estudio de Situación*, presentado en noviembre, se encuentra una observación destacable dentro del apartado de "Planificación" del capítulo de conclusiones generales: "se acusa la falta de una metodología común para el análisis de riesgos integral". En otros apartados de ese documento, se vuelve a resaltar la dificultad de realizar ese análisis de riesgos integral –o integrado–, que permita proponer medidas de seguridad (*security*) coherentes en cuanto a esfuerzo y atención a los impactos y amenazas, tanto de seguridad física como de ciberseguridad.

Obviamente esta no es una necesidad restringida a los operadores designados como críticos en base a la legislación sobre protección de infraestructuras críticas. El enfoque actual de la *security* (seguridad frente a riesgos deliberados) pasa por el denominado ESRM (*Enterprise Security Risk Management*), enfoque metodológico propuesto por la asociación de profesionales de la seguridad ASIS International con carácter estratégico. El ESRM afronta la evolución de las amenazas deliberadas centrando los modelos de gestión de la seguridad de las empresas en un enfoque holístico, sin diferenciar entre el origen de los riesgos –ya sean físicos o cibernéticos– y poniendo en el centro de la estrategia el análisis de dichos riesgos.

Es evidente que el análisis de riesgos es una actividad imperativa para operadores críticos como mandato legal y también para el resto de las empresas enmarcada dentro de sus necesarias "mejores prácticas" o como parte de otros imperativos legales.

Posible solución

La importancia del análisis de riesgos en gran parte de las actividades de Cuevavaliente Ingenieros nos ha llevado desde hace años a hacer de las metodologías para llevarlo a cabo un punto central de la estrategia de desarrollo de nuestra empresa.

Desde nuestro nacimiento, en 2005, hemos incorporado a nuestros servicios sucesivas aproximaciones a la metodología de análisis de riesgos, tanto en su aplicación a la denominada "seguridad física" (ARG 07 en 2007, GRSec 31000 en 2010), como en su aplicación conjunta a riesgos tradicionales y a ciberriesgos (GR2Sec en 2015).

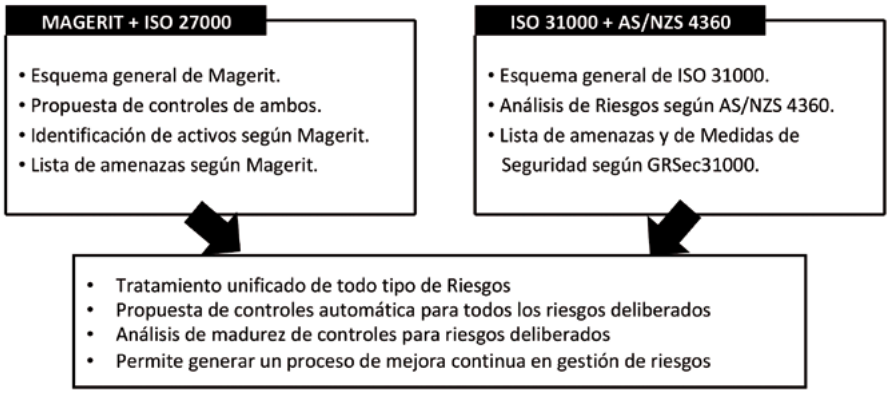
La metodología GR2Sec incluye el ciclo completo de la gestión de riesgos:

- El análisis de riesgos propiamente dicho (fases de la evaluación de riesgos según ISO 31000):
  - Identificación de riesgos.
  - Análisis de riesgos.
  - Evaluación de riesgos.
- Decisión sobre la gestión de los riesgos (tratamiento de los riesgos según ISO 31000):
  - Evitar o eliminar los riesgos.
  - Aceptar los riesgos.
  - Transferir los riesgos.
  - Mitigar los riesgos, en cuyo caso se incluye la propuesta de controles (medidas de seguridad) de los riesgos a mitigar.

El análisis de riesgos en un modelo de mejora continua en la gestión de riesgos.

En este sentido, la metodología permite alimentar los modelos de gestión de seguridad basados en la mejora continua, como los derivados de la

Esquema de las etapas de la metodología GR2Sec.



Fuentes de inspiración y adaptaciones de la metodología GR2Sec.

norma ISO 31000, en sus etapas de planificación e implementación.

En esas etapas, la metodología GR-2Sec aporta:

- Planificación:
  - Permite definir el contexto (activos, amenazas y tiempos).
  - Determina el riesgo inherente tras analizar sus componentes.
- Implantación:
  - Proponiendo los controles (medidas de seguridad) paliativos.

En el esquema de planificación e implantación se presenta el desglose de procesos internos que se realizan mediante la metodología GR2Sec (ver imagen del esquema en la parte superior).

Los fundamentos de la metodología parten de la adecuación de normativas internacionales bien asentadas, como son la ISO 31000 en el caso de la seguridad denominada "física" y la ISO 27001 en el de la ciberseguridad.

El esquema general del proceso de análisis utiliza una adaptación de la metodología Magerit II para su utilización por ambos tipos de riesgos, y las tablas de cálculo de impacto de la AS/NZS 4360 para el cálculo unificado de los impactos.

El esquema general de la metodología GR2Sec se puede observar en el gráfico de la siguiente página.

La herramienta

En los últimos años, Cuevavaliente Ingenieros ha utilizado esta metodología internamente para realizar los trabajos encomendados en los que el análisis de riesgos era parte fundamental, ya sea en anteproyectos de sistemas de seguridad, asesoramiento a departamentos de seguridad en su planificación estratégica o en los más de 40 Planes de Protección Específicos en los que hemos colaborado con operadores para el cumplimiento legal que afecta a sus instalaciones críticas. Se trata, por tanto, de una metodología experimentada.

La evolución de los departamentos de seguridad en los que se gestiona un número considerable de activos hacia los enfoques integrados de los riesgos deliberados (como propone la metodología ESRM) ha generado una demanda nueva: la de disponer de herramientas propias con las que ayudar a la gestión de los riesgos de forma interna.

La constatación de esta demanda ha llevado a Cuevavaliente Ingenieros a integrar la metodología GR2Sec en la plataforma de gestión GlobalSUITE®.

La evolución de los departamentos de seguridad ha generado una demanda nueva: disponer de herramientas propias para la gestión de los riesgos

GlobalSUITE® es una plataforma empleada por múltiples organizaciones españolas e internacionales, que permite la implantación, mantenimiento, automatización y monitorización de cualquier tipo de sistema de gestión de riesgos, seguridad, continuidad de negocio y cumplimiento legal y normativo.