



Las medidas de seguridad en entornos multinacionales

Nélida García / Responsable de Ingeniería de Cuevavaliente Inerco

Las empresas con actividad multinacional ocupan ya un gran espacio en la economía española. Entidades financieras, empresas energéticas, industrias, etc, engrosan el número creciente de organizaciones que tienen sus activos y sus actividades en múltiples países, algunos en entornos con perfiles de riesgo muy diferentes a los de España.

Este tipo de empresas afrontan el reto de disponer de medidas de seguridad acordes a los perfiles de riesgo y a las amenazas concretas de aquellos países en los que operan, además de a situaciones de legislación y de apoyo por la seguridad pública local muy diversas.

¿Cómo diseñar esas medidas de seguridad con criterios equilibrados? ¿Cómo adaptarse a las diferentes necesidades? Estas preguntas son las que han de responder cada vez más a menudo los directores de Seguridad de un creciente número de empresas españolas.

En el contexto de este artículo, no se toman en consideración los análisis relativos a los delitos cibernéticos, sino que únicamente se tienen en cuenta las medidas de seguridad de carácter físico. Esto es debido al carácter de ubicuidad de las ciberamenazas y a la nula o escasa dependencia del país o región donde se producen.

Condicionantes

De forma previa al establecimiento de las directrices en materia de seguridad, se hace necesario un estudio previo de las diferentes variables que pueden influir en las medidas a adoptar en cada compañía. El primer paso es la tipificación de los activos de la compañía, tomando siempre en cuenta tanto per-

sonas como bienes. Esta tipificación deberá realizarse con dos criterios paralelos:

- La funcionalidad del activo en la estructura operativa del negocio: se deberán tener en cuenta todas las líneas de negocio y todas las posibles topologías de emplazamientos.
- Clasificación de cada uno de los activos en diferentes grados o niveles: esta asignación estará basada princi-

palmente, con amenazas directas a la vida y a la seguridad; el crimen organizado, como fenómeno transnacional y la vinculación de organizaciones criminales y grupos terroristas; el espionaje industrial, con la facilidad que ofrecen las tecnologías de la información y comunicaciones, en formas agresivas y con gran impacto; las amenazas intrínsecas que emanan de las infraestructuras críticas en aquellos países sujetos a imposición

La solución de un problema de seguridad reside en los medios de protección que deben aplicarse para reducir o anular las vulnerabilidades detectadas

palmente en un fundamento de criticidad del activo para el negocio. No tendrá la misma consideración a efectos de seguridad una oficina comercial que la sede social de la compañía, por ejemplo. Este nivel de criticidad se estudiará únicamente a efectos de impacto que le generaría a la compañía la indisponibilidad del activo.

Como un paso posterior, se hace primordial el análisis de las diferentes amenazas que aprovechan las brechas de seguridad para atentar contra la integridad del activo. Las amenazas pueden proceder de ataques o de incidentes físicos o lógicos que desde el punto de vista de una organización pueden ser tanto internos como externos. Aunque se deberán analizar de forma particular para cada entorno o país, las principales amenazas que deberán ser tenidas en cuenta pertenecerán a los grupos de amenazas físicas de *security*: el terro-

legal al respecto; en las compañías sujetas a imposición legal en su país, las infraestructuras críticas, como indispensables y sin alternativa, asediadas con riesgos múltiples; los conflictos sociales y/o políticos; y la delincuencia ordinaria, entendida como delitos menores de carácter tanto interno en la propia empresa como externo.

Para contrarrestar estas amenazas se debe realizar un análisis previo de la organización de las Fuerzas de Seguridad Pública que dispone el país o la región y el apoyo que será necesario aportar con personal de seguridad privada, entendiéndose esencial la cooperación entre ambas, dado que esta última deberá ser una seguridad subordinada y complementaria de la seguridad pública existente en cada país.

Otro aspecto fundamental a tener en cuenta es el marco normativo por país o región, que obliga a conocer las normativas sobre seguridad y emergencias,

la protección de datos personales, la específica del sector (bancario, aéreo, petrolífero...), así como su régimen jurídico de aplicación.

Sin embargo, las claves para el diseño de las medidas de seguridad no se basan únicamente en el conocimiento del marco normativo que afecta a cada país, sino que también radican en la observación y en el conocimiento profundo del entorno donde se ubica el activo para garantizar las mejores directrices de seguridad. Este entorno lo pueden configurar otras empresas, los clientes, el desarrollo tecnológico, la situación geopolítica, el estatus social, el nivel de amenaza local y otros muchos elementos que condicionan a la empresa.

Un eficaz entendimiento del entorno en el que operan los diferentes activos de la compañía permitirá establecer las medidas en base a los diferentes servicios que ofrece el mercado de seguridad privada en cada país. La seguridad privada es un sector en el que la innovación tecnológica está permitiendo, especialmente en los últimos años, identificar nuevos servicios aplicados a la búsqueda de un entorno empresarial y personal lo más seguro posible.

Por tanto, se hace necesario conocer el mercado de la seguridad en la ubicación geográfica donde se ubica el activo. El paso principal para entender un mercado es relacionar la oferta de servicios, la oferta de productos, quién ofrece ambos y los condicionantes legales de cada uno de ellos.

Esquema de actuación

Con el paso previo de recopilación y análisis de todos los condicionantes que pueden afectar al director de Seguridad en la toma de decisiones en materia de seguridad, se puede afrontar la tarea de estandarización de directrices en la compañía con ámbito de aplicación internacional.

A nivel corporativo, se define previamente la estrategia de seguridad a través de documentos de alto nivel (ver gráfico 1).



Gráfico 1.

Por otro lado, en cada país estas estrategias se pueden implantar a partir del desarrollo de documentos particularizados para cada región, país o incluso activo (mostrados en color verde). El esquema a implantar se puede mostrar en forma de pirámide, indicando la jerarquía de documentos generales a aquellos más específicos (ver gráfico 2).

Antes del desarrollo de cada uno de estos documentos, y de forma común a todos ellos, se deberá escoger una metodología de análisis de riesgos. Los criterios a seguir para elegir la metodología a aplicar en la materia de seguridad se tendrán que regir por los siguientes estamentos: deberá estar estandarizada en la compañía, ser independiente de



Gráfico 2.

la región o país donde se aplique y disponer de un catálogo de amenazas global.

El tratamiento del riesgo incluye el diseño, planificación e implantación de medidas de seguridad que se describen en cada uno de los diferentes documentos.

- La política de seguridad se constituye como un documento de alto nivel en el que la dirección marca los objetivos y la misión de la seguridad en la compañía. Estará suscrita por el máximo responsable del negocio de cada país.

- El modelo de seguridad corporativo establece un marco de gestión de la seguridad en el que se definen las funciones de seguridad en la empresa; el organigrama del departamento de Seguridad; las políticas, normativas y procedimientos; los activos sobre los que la seguridad tiene responsabilidad; y las amenazas bajo la responsabilidad de seguridad.

- El documento de criterio de protección general es un desarrollo de alto nivel que representa la filosofía corporativa de la organización en materia de aplicación de medidas de protección (técnicas y operativas) sobre los activos.

Sobre este último se sustentan los criterios de protección específicos por cada tipo de activo, las especificaciones técnicas y las especificaciones operativas. Todos estos documentos deberán formar parte del marco de referencia para el diseño, planificación e implantación de las medidas de seguridad en la compañía.

La aplicación del modelo de seguridad corporativo en cada país generará su correspondiente documento de organización local de la seguridad.

En concreto, la forma que encaramos el reto desde Cuevavallente Inercio se resume en el gráfico 3.

Los criterios de protección general organizan las medidas de seguridad en función de las denomina-

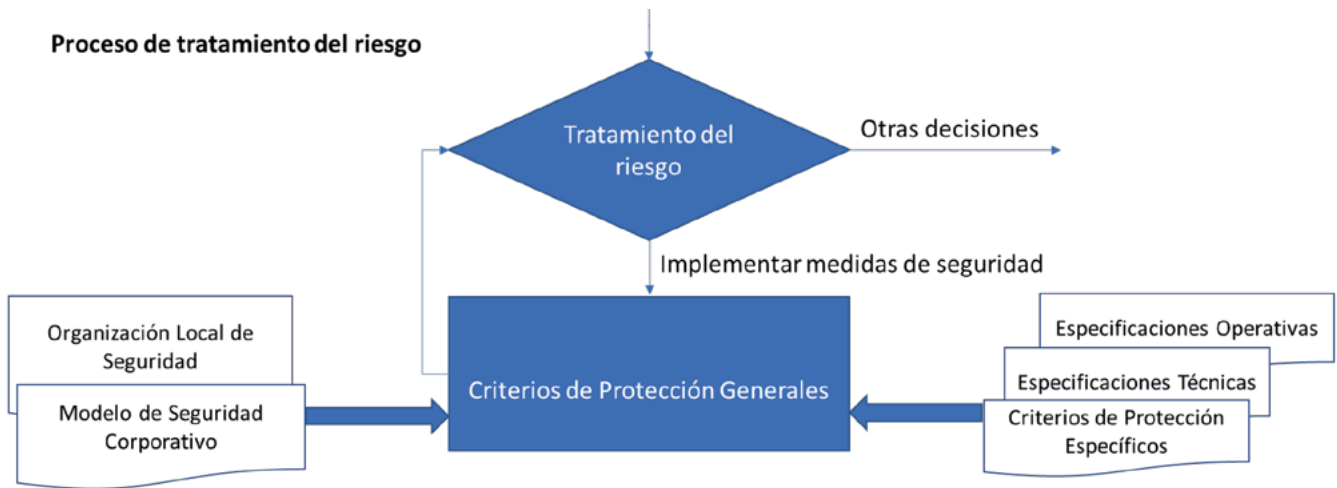


Gráfico 3. Proceso de tratamiento del riesgo.

das esferas (o anillos) de protección, las cuales limitan las diferentes áreas de seguridad:

- Zona pública: es el espacio de libre acceso a las personas comprendido entre el exterior y la zona de seguridad. En él, las personas y los vehículos se mueven libremente sin necesidad de autorización alguna.
- Zona de seguridad: es un área entre la zona pública y la zona protegida en el que las personas y los vehículos se desplazan sin necesidad de autorización, aunque se encuentra supervisada.

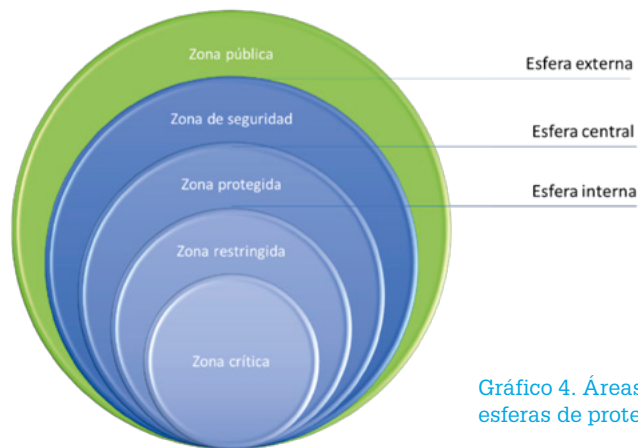


Gráfico 4. Áreas de seguridad y esferas de protección.

OBJETIVOS DE SEGURIDAD	
Protección de intrusión	Medidas que permiten la detección de presencia de personas/objetos en un área determinada
Protección perimetral	Medidas destinadas a evitar la intrusión de personas a las instalaciones a través del perímetro de éstas. Sirve para paliar cualquier tipo de riesgo, siempre que no tenga un origen interno
Control de accesos	Medidas destinadas a garantizar que el acceso de personas, vehículos o materiales a un determinado escenario se realiza únicamente por las personas que están autorizados para ello
Control de público	Medidas destinadas a garantizar que el público presente en un escenario observa un comportamiento dentro de los límites permisibles
Control interno del escenario	Medidas destinadas a detectar comportamientos ilícitos en el interior de un recinto crítico
Aviso de situaciones de emergencia	Medidas destinadas a garantizar la comunicación en situaciones de peligro para las personas o la instalación, desde el lugar donde se produce el ataque con el centro de control o con el personal con capacidad de reacción ante este tipo de situaciones
Vigilancia	Dotación de personal de seguridad (vigilantes y auxiliares) para la realización de diversas funciones de seguridad
Gobierno y gestión de la seguridad	Definición de las políticas, procedimientos, jerarquías del personal, etc. y distribución de las mismas entre los empleados de la empresa que permiten la protección de la instalación y que garantizan la seguridad de los trabajadores

Tabla 1. Objetivos de seguridad aplicados sobre las esferas de protección.

- Zona protegida: espacios donde se encuentra el proceso productivo de la empresa.
- Zona restringida: son espacios de acceso controlado donde se encuentra la parte neurálgica de los procesos de producción o de los procesos que la soportan, o lugares donde se custodian activos importantes de la empresa.
- Zona crítica: son espacios de acceso muy restringido desde donde se controla parte importante del proceso productivo o se custodian activos del máximo valor estratégico para la empresa.


Una vez identificados los riesgos, los objetivos de seguridad que se aplican sobre cada una de las esferas se dividen en varios de ellos, los cuales se pueden observar en la tabla 1.

De aplicar el criterio de protección general a un activo con un perfil de riesgo se obtiene el criterio específico de protección, que indicará el punto de partida de las especificaciones técnicas y operativas a aplicar.

El criterio de protección específico será el que se utilice para el diseño del sistema de seguridad de un activo. No obstante, en la medida que el activo disponga de particularidades que no se ajustan al criterio de protección específico, podrá aplicarse el criterio de protección general.

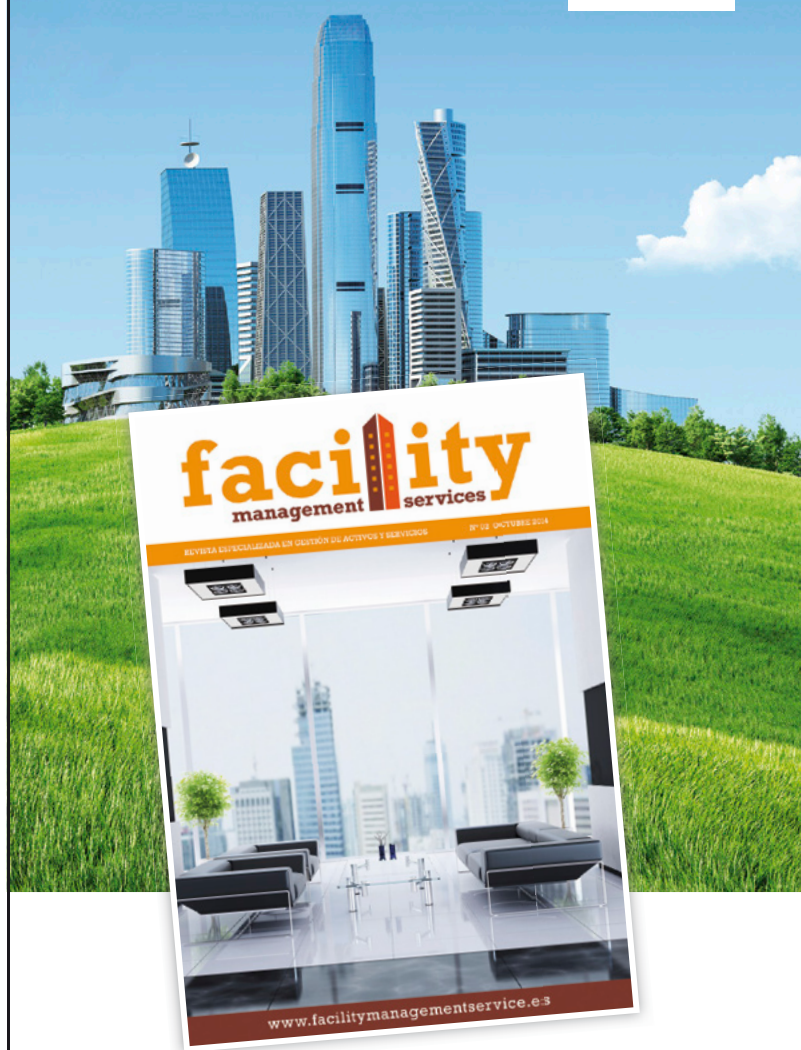
Tanto los criterios de protección específicos como las especificaciones técnicas y operativas son documentos vivos que evolucionan conforme a la evolución de los riesgos, las lecciones aprendidas, las nuevas tecnologías y los cambios regulatorios del sector.

Por lo tanto, la solución de un problema de seguridad reside en los medios de protección que deben aplicarse para reducir o anular las vulnerabilidades detectadas, teniendo en cuenta sus diferentes capacidades. Así, se instalarán medios pasivos si se quiere retrasar la agresión, mientras que se pondrán medios técnicos activos si se desea detectar y seguir la agresión. Pero son los recursos humanos (cuerpos policiales y de emergencia, vigilantes, detectives, personal propio, etc.) los que reaccionan y reducen dicho ataque. Las personas son un elemento imprescindible en cualquier proceso, por muy automatizado que esté, por lo que la intervención humana es necesaria en el ciclo de vida de las medidas de seguridad. Por último, serán las medidas organizativas (una estructura de seguridad con normas de obligado cumplimiento y procedimientos de actuación) las que faciliten la actuación coordinada del conjunto.

Desde Cuevaliente Inerco tenemos la fortuna de contar con la confianza de algunas de las compañías de operativa multinacional de mayor envergadura del país, en las que hemos aplicado la metodología aquí descrita, uniendo sinergias entre el *expertise* adquirido y la aplicación de una metodología de riesgos de desarrollo propio de Cuevaliente, denominada GR2Sec. 

www.facilitymanagementservices.es

Conoce las últimas novedades del sector FM



Aprovéchate de un 50% de descuento*

 Editorial
BORRMART, S.A.

suscripciones@borrmart.es

* precio tarifa: 50€ (IVA no incluido) (válido para territorio español)