Guía de buenas prácticas en la seguridad patrimonial

José Manuel García Diego

AENOR ediciones

Guía de buenas prácticas en seguridad patrimonial

José Manuel García Diego

AENORediciones

Título: *Guía de buenas prácticas en seguridad patrimonial*
Autor: José Manuel García Diego

ISBN: 978-84-8143-841-3
Depósito legal: M-7736-2014
Impreso en España - Printed in Spain

Edita: AENOR
Maqueta y diseño de cubierta: AENOR
Imprime: AENOR

Nota: AENOR no se hace responsable de las opiniones expresadas por el autor en esta obra.

AENOR Asociación Española de Normalización y Certificación

Génova, 6. 28004 Madrid • Tel.: 902 102 201 • Fax: 913 103 695
comercial@aenor.es • www.aenor.es

Índice

Introducción

La gestión de la calidad supuso un paso adelante importantísimo para las empresas que querían cumplir adecuadamente con su misión de satisfacer las necesidades y las demandas de los clientes. La alineación de todas las funciones o procesos internos con ese propósito ha propiciado en estos años que todos los procesos operativos empresariales se hayan racionalizado y actualizado. Todas las funciones, o los procesos en aquellas empresas que hayan optado por la gestión de estos, han debido optimizarse para la consecución del objetivo estratégico.

Sin embargo, en general, las empresas no han dispuesto su estructura interna para la gestión de circunstancias contingentes, la gestión de los riesgos de cualquier tipo, lo que alguna vez se ha llamado la gestión de "lo que puede ir mal". No existe en nuestro país cultura de gestión del riesgo empresarial, y las explicaciones pueden ser variadas. Creo que la causa principal es la falta de cultura de la seguridad por parte de la alta dirección; esta carencia se traslada inmediatamente a la organización, que no suele disponer de una función interna encargada de la gestión de los riesgos empresariales. Es muy frecuente que esa misma alta dirección esté ocupada exclusivamente en "lo que puede ir bien" (la producción, las finanzas, las ventas, los recursos, etc.), y muy poco centrada en la gestión de lo contingente, es decir, en "lo que puede ir mal" en la organización.

Tiene ello mucho que ver con la percepción de los riesgos que tenga el empresario, con la dificultad de cuantificar el retorno de la inversión de la no siniestralidad, o simplemente con que implantar algunas medidas o transferir a una compañía de seguros algunos riesgos le proporciona una sensación de seguridad que no tiene por qué corresponderse con la seguridad real.

En cualquier caso, psicológicamente resulta mucho más atractivo ocuparse de las actividades ordinarias de la empresa, de las cuestiones positivas –porque suelen te-

ner retornos también positivos–, que trabajar analizando escenarios de riesgo, de impactos para la actividad, de falta de continuidad de la empresa, etc., todos ellos de pronóstico negativo.

Lo cierto es que la continuidad del negocio puede ponerse en peligro tanto porque no funcionen los procesos productivos como porque se materialicen riesgos para los activos de la empresa que puedan resultar generadores de pérdidas importantes o incluso acabar con ella. Y esta es la razón por la que ambos deben ser adecuadamente gestionados.

La escasa gestión del riesgo que se hace hasta ahora ha venido de la mano de lo impuesto por sucesivas normas legales que obligan a las organizaciones a gestionar determinados riesgos específicos. Este sería, por ejemplo, el caso de la gestión de los riesgos laborales de los trabajadores, impuesta por la Ley 31/1995 de prevención de riesgos laborales. Mucho más difícil ha sido que los empresarios hayan decidido voluntaria y conscientemente gestionar determinados riesgos sin que una ley estuviera detrás obligándoles. No obstante, el temor a determinados escenarios de pérdidas o la imposición de terceras partes con quienes contratan ha sido suficiente, en algunos casos, para que fueran dando respuesta a otras familias de riesgo.

Este sería el caso de los riesgos para la información, activo determinante en cada vez más procesos productivos, y por ello estratégico para el empresario, o la gestión de riesgos para el medio ambiente que puede verse alterado como consecuencia de la actividad empresarial. Otras familias de riesgo también surgen como consecuencia del cumplimiento normativo, generador a su vez del riesgo de cumplimiento, del miedo a la sanción, como la normativa de seguridad privada que afecta a sectores relacionados con la actividad como los bancos, etc.

Más difícil resulta ver ejemplos de gestión de los riesgos que pueden influir en la continuidad del negocio o de aquellos que puedan afectar a la responsabilidad social corporativa, a las expectativas de colectivos ajenos a la empresa, pero próximos a ella como partes interesadas en su actividad (*stakeholders*), como es el caso de asociaciones, organismos públicos, etc.

Para la gestión de todos estos riesgos, que puede ser obligada o voluntaria, se pueden utilizar estándares como UNE-ISO/IEC 27001, UNE-ISO 14001, UNE-ISO 26000, OHSAS 18001 o UNE-ISO 22301, capaces de proporcionar al empresario la mejor calidad en la gestión de sus correspondientes riesgos.

Desgraciadamente, en estos organismos no existen estándares que den respuesta a una familia de riesgos, que seguramente fue la primera de todas, y que por ello nació sin apellidos: la "seguridad". Familia que hoy, para diferenciarla de otras "seguridades" se viene llamando "seguridad física". Se trata de la respuesta no normalizada a determinados riesgos empresariales, muchos de ellos de carácter antisocial (robos, hurtos,

infidelidades, falsificaciones, delitos contra la propiedad industrial o intelectual, etc.) e incluso relacionados con la seguridad personal del propio empresario, que se convierte así en un activo con riesgo para su propia empresa.

En el mundo anglosajón, cuando en los años setenta se empezaron a implantar con fuerza las TIC en entornos corporativos, se hizo necesario diferenciar los riesgos que afectaban a la información contenida en ordenadores centrales de los riesgos asociados a los activos tangibles de la empresa. Fue entonces cuando apareció el apellido actual: a la respuesta a los riesgos del *software* se la llamó *logical security* y a la seguridad del resto de activos *physical security*, término que, al castellanizarlo, tiene evidentes connotaciones de seguridad de los elementos tangibles y que, por ello, a menudo se confunde con las propias medidas de seguridad. Expresiones como "llama a seguridad", o "suelo de seguridad" se usan habitualmente en lugar de las más ortodoxas "llama al vigilante" o "suelo antideslizante".

Hoy se llama seguridad física a todo lo que no puede encuadrarse en alguna de las numerosas especialidades de la seguridad, y eso induce a error a los usuarios, error que suele traducirse con gran frecuencia en pérdidas o, con más frecuencia aún, en riesgos que no se gestionan. Sin embargo, en la actualidad la seguridad física está absolutamente asociada a las nuevas TIC. Resulta absolutamente impropio llamar seguridad física a los datos que se guardan en un servidor del centro de control, y hablar de seguridad de la información cuando esos mismos datos se guardan en el *host*; o a las comunicaciones perimetrales de ese mismo *host* frente a las que se gestionan, a menudo soportadas en fibra óptica o vía satélite, en una central receptora de alarmas. En la realidad actual es prácticamente imposible encontrar servicios de seguridad que no estén soportados en esas nuevas tecnologías: en algunos casos, las puertas ya no se abren con llaves sino con tarjetas de proximidad o con el iris de los ojos, etc. y por ello resulta totalmente obsoleto que aquella seguridad originaria, como especialidad que es de la seguridad general, siga asociada a elementos físicos solo por el nombre que en su día se le dio en inglés.

Por todo lo expuesto, y además porque su ámbito de aplicación tiene como objetivo la prevención y protección de todo el entorno, prefiero denominarla seguridad patrimonial, ya que en definitiva, se trata de gestionar los riesgos para el patrimonio de la empresa.

Dicho esto, debo referirme a la regulación legal de esta modalidad de seguridad, inexistente en general, y que solo alcanzó a determinados sectores de la actividad que el legislador entendió como prioritarios. Son aquellos sectores en los cuales el riesgo de comisión de delitos contra el patrimonio es más alto: bancos, gasolineras, farmacias, joyerías, salas de exposiciones…, tienen la obligación legal de adoptar determinadas medidas de seguridad; para ello se crea la especialidad denominada "seguridad privada", para diferenciarla de la pública. Esta situación empezó a cambiar

con la aprobación por las Cortes Generales de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Está ley está dirigida a la prevención y protección de cualquier riesgo que se cierna sobre servicios que el legislador considere esenciales para la comunidad.

Las estructuras empresariales que prestan estos servicios esenciales, ya sean públicas o privadas, pasan a denominarse infraestructuras críticas y el legislador les impone determinadas obligaciones en la gestión de sus riesgos, tratando de evitar la materialización de las amenazas y, en caso de producirse, la minimización de sus consecuencias. En esta ley, y por primera vez en nuestro país, se obliga a estos empresarios, llamados operadores críticos, a gestionar los riesgos de una forma sistémica, holística, que abarque tanto la seguridad lógica como la física (en expresión del propio texto legal), concepto próximo al de seguridad integral, tan prestigioso en la teoría como poco implantado en la práctica.

También el nuevo proyecto de Ley de seguridad privada, actualmente en sede parlamentaria, incluye en su redacción la obligación de un enfoque integral, sistémico, de la seguridad en las empresas, postulado con el que estoy totalmente de acuerdo y que vengo defendiendo desde hace años. Esta línea legislativa, además del propio interés empresarial, va dibujando lo que será la gestión de la seguridad en los próximos años: seguridad gestionada o, lo que es lo mismo, seguridad organizativa. La etapa de la denominada seguridad subjetiva, la seguridad disuasoria, y la posterior etapa de las medidas de seguridad, van ir dando paso a la denominada gestión de la seguridad.

Esta especialidad tan amplia de la seguridad deberá tener sus propios patrones de gestión, sus políticas, sus procedimientos; la seguridad dejará de ser una medida de seguridad, un producto, e incluso un departamento, para convertirse en un proceso más de la empresa que habrá de ser implantado con criterios de gestión de la calidad.

Y ese es el objetivo de esta publicación: facilitar un modelo de gestión, absolutamente alineado con la gestión de la calidad, totalmente integrable con otros estándares y fundamentada en el cumplimiento práctico de la Norma UNE-ISO 31000:2010 *Gestión del riesgo. Principios y directrices*.

También forman parte de la guía aquellos objetivos de control y controles específicos de carácter genérico que sirven de apoyo a la implantación de un sistema de gestión de la seguridad patrimonial (SGSP). Se facilita igualmente un método de análisis de riesgos patrimoniales de propósito general capaz de apreciar el nivel del riesgo en cualquier sector de la actividad.

El SGSP resultará útil a cualquier empresa de cualquier sector, independientemente del modelo organizativo que tenga implantado, ya sea funcional o de gestión basada en procesos. Asimismo será integrable con cualquier sistema de gestión normalizado de otros riesgos especializados. Aporta criterios de sostenibilidad eficiente para la

seguridad, ya que mediante el uso de un modelo organizativo podrá alcanzarse un nivel de madurez que actualmente solo se puede conseguir mediante un uso intensivo de las siempre costosas medidas de seguridad.

Al igual que los sistemas de gestión estandarizados, es un modelo escalable, ya que el alcance y la periodicidad de la mejora continua pueden ser determinados por la organización. Se aportan, sobre todo pensando en las necesidades de las pymes, controles y consejos de implantación que permitirán conseguir una elevación de los niveles de seguridad de su organización incluso a personas que no tengan la espe-cialización y habilitación de directores de seguridad.

Sobre el autor

José Manuel García Diego es Licenciado en Ciencias del Trabajo (UOC), Diplomado en Relaciones Laborales y está finalizando los estudios del Grado de Derecho (UOC). Es Director de Seguridad habilitado por el Ministerio del Interior, Postgrado en Seguridad en Entidades financieras (UCM), en Seguridad de la Información (UOC), Técnico Superior en Prevención de riesgos laborales (UC) y formador habilitado por el Ministerio del Interior en materia de seguridad. Ha sido Director de Seguridad Integral de Caja Cantabria durante 12 años y es colaborador habitual de revistas especializadas del sector, conferenciante-colaborador en distintas instituciones privadas, públicas y académicas como ICADE, Universidad Internacional Menéndez Pelayo y Universidad de Cantabria (Máster de Riesgos Laborales), además de profesor colaborador del curso de experto en Protección de infraestructuras críticas de la UNED.

ISBN 978-84-8143-841-3

La seguridad patrimonial tiene como objetivo la prevención y protección de los bienes de una empresa.

Esta publicación aborda un sistema de gestión de la seguridad patrimonial, absolutamente alineado con la gestión de la calidad, totalmente integrable con otros estándares y fundamentada en el cumplimiento práctico de la Norma UNE-ISO 31000:2010 *Gestión del riesgo. Principios y directrices*. También se han tenido en cuenta aquellos objetivos de control y controles específicos de carácter genérico que sirven de apoyo a su implantación. Además, se facilita un método de análisis de riesgos patrimoniales de propósito general capaz de apreciar el nivel del riesgo en cualquier sector de la actividad.

Su contenido será útil a cualquier empresa de cualquier sector, independientemente del modelo organizativo que tenga implantado, ya sea funcional o de gestión basada en procesos.

José Manuel García Diego es Licenciado en Ciencias del Trabajo *(UOC)*, Diplomado en Relaciones Laborales y está finalizando los estudios del Grado de Derecho *(UOC)*. Es Director de Seguridad habilitado por el Ministerio del Interior, Postgrado en Seguridad en Entidades financieras *(UCM)*, en Seguridad de la Información *(UOC)*, Técnico Superior en Prevención de riesgos laborales *(UC)* y formador habilitado por el Ministerio del Interior en materia de seguridad. Ha sido Director de Seguridad Integral de Caja Cantabria durante 12 años y es colaborador habitual de revistas especializadas del sector, conferenciante-colaborador en distintas instituciones privadas, públicas y académicas como ICADE, Universidad Internacional Menéndez Pelayo y Universidad de Cantabria *(*Máster de Riesgos Laborales*)*, además de profesor colaborador del curso de experto en Protección de infraestructuras críticas de la UNED.

AENOR Asociación Española de Normalización y Certificación

www.aenor.es

Los imprescindibles de AENOR

Gestión energética

Pack Eficiencia energética

+ **Libro** "Gestión de la eficiencia energética: cálculo del consumo, indicadores y mejora"
+ **Normas** UNE-EN ISO 50001 y UNE 216501
+ **Hojas de cálculo** de los ejemplos sectoriales
+ **Vídeo y reportaje** de los autores

2012 • Rústica + CD-ROM • 65 €

Gestión de la eficiencia energética: cálculo del consumo, indicadores y mejora

2012 • 216 págs. • 20,95 €
Ebook • 14,95 €

Responsabilidad social

Pack Responsabilidad social

+ **Libro** "Principios, prácticas y beneficios de la responsabilidad social"
+ **Norma** UNE-ISO 26000:2012 "Guía de responsabilidad social"
+ Otros **documentos** de interés sobre RS

2012 • Rústica + CD-ROM • 60 €

Principios, prácticas y beneficios de la responsabilidad social

2012 • 136 págs. • 20,80 €
Ebook • 9,95 €

TIC

Modelo para el gobierno de las TIC basado en las normas ISO

2012 • 434 págs. • 24,96 €
Ebook • 12 €

Gestión y calidad

Aspectos clave de la integración de sistemas de gestión

2012 • 214 págs. • 19,95 €
Ebook • 9,95 €

Factores que contribuyen al éxito de una auditoría integrada

2011 • 240 págs. • 34 €

Configuración y usos de un mapa de procesos

2012 • 156 págs. • 24 €
Ebook • 12 €

ISO 9001:2008 comentada

2009 • 292 págs. • 31,20 €

ISO 9000 Las preguntas del auditor

2.ª edición

2009 • 170 págs. • 26 €

Después de la certificación ISO 9001

2.ª edición

2010 • 122 págs. • 20,80 €

ISO 9001:2008 comentada + ISO 9000 Las preguntas del auditor + Después de la certificación ISO 9001 **60 €**

Seguridad y salud en el trabajo

Modelo de empresa saludable. Healthy workplace model

2012 • 84 págs. • 10,04 €
Ebook • 7,26 €

Cómo implantar con éxito OHSAS 18001

2008 • 344 págs. • 25 €

Guía para la auditoría de los sistemas de gestión de la seguridad y salud en el trabajo. OHSAS 18001

2008 • 128 págs. • 31,20 €

OHSAS 18001:2007 Sistemas de gestión de la seguridad y salud en el trabajo

2007 • 46 págs. • 23,50 €
PDF • 26,67 €

OHSAS 18002:2008 Sistemas de gestión de la seguridad y salud en el trabajo. Directrices para la implementación de OHSAS 18001:2007

2009 • 116 págs. • 31,20 €
PDF • 35,40 €

Gestión de la seguridad y salud en el trabajo según OHSAS 18001. Actitudes y percepciones de empresas certificadas

2010 • 160 págs. • 31,50 €

OHSAS 18001 + OHSAS 18002 en soporte impreso **46,49 €**

Servicio de Asesoría sobre Normas Técnicas y Legislación *(SAT)*

Contacte con nosotros, le aportamos soluciones para:

- Poner sus productos de forma segura en el mercado.
- Conocer los requisitos normativos y legislativos para exportar o importar sus productos.
- Aplicar la metodología correcta en los ensayos de acuerdo con las normas.

Servicio
Asesoría Técnica
LE APORTAMOS SOLUCIONES

Un servicio integral de información, completamente personalizado y multisectorial, para los profesionales de cualquier tipo de organización y ámbito de actividad.

Envíenos su consulta a info@aenor.es o contacte a través del 902 102 201 o 914 326 160. Nuestros expertos evaluarán técnica y económicamente su consulta y le presentaremos una oferta.

AENOR

AENORmás
NORMAS AL DÍA

La única solución on-line para la gestión de sus normas, en constante evolución

Le facilita:

- **Su espacio**
- **Actualización automática**
- **Sus alertas**
- **Acceso 24 horas**
- **Tarifa plana anual**

Ahora también actualiza la legislación nacional en sus colecciones de normas.

Suscríbase a las nuevas colecciones de normas UNE y legislación:

- **REBT/** Reglamento Electrotécnico para Baja Tensión.
- **CTE/** Código Técnico de la Edificación.
- **RLAT/** Reglamento de Líneas Eléctricas de Alta Tensión.
- **RITE /** Reglamento de Instalaciones Térmicas en Edificios.
- Reglamento técnico de distribución y utilización de combustibles gaseosos.

Entre y elija su colección

www.aenor.es – aenormas@aenor.es – 914 326 032/127