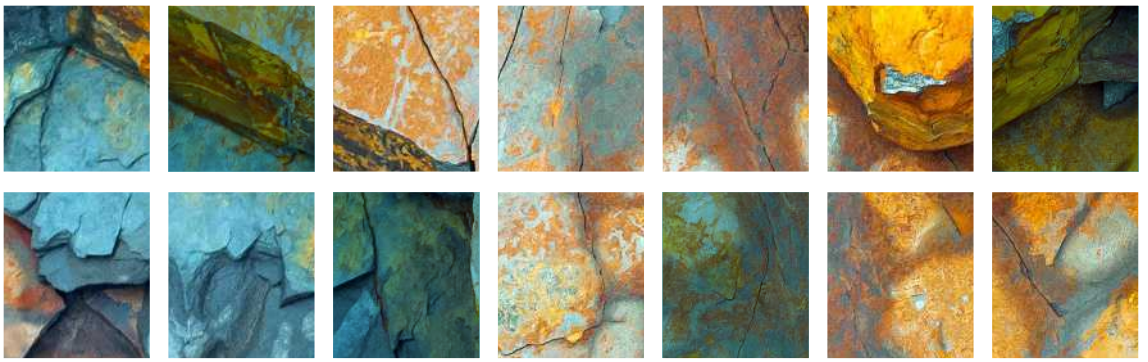
Mapa de riesgos penales y prevención del delito en la empresa

Coordinadores

Pere Simón Castellano
Alfredo Abadías Selma

BOSCH



Wolters Kluwer

BOSCH

Mapa de riesgos penales y prevención del delito en la empresa

Coordinadores

Pere Simón Castellano
Alfredo Abadías Selma

Wolters Kluwer

Wolters Kluwer
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
Tel: 902 250 500 – Fax: 902 250 502
e-mail: clientes@wolterskluwer.com
http://www.wolterskluwer.es

Primera edición: Septiembre, 2020

Depósito Legal: M-23690-2020
ISBN versión impresa: 978-84-9090-461-9
ISBN versión electrónica: 978-84-9090-462-6

Diseño, Preimpresión e Impresión: Wolters Kluwer España, S.A.
Printed in Spain

La citada norma internacional proporciona directrices sobre la aplicación de un enfoque de gestión de riesgos orientado a procesos para ayudar en la aplicación de manera satisfactoria y al cumplimiento de los requisitos de gestión de riesgos de seguridad de la Norma ISO/IEC 27001.

Veamos un gráfico con el detalle de las relaciones entre las normas ISO/IEC de la familia de los Sistemas de Gestión de la Seguridad de la Información (en adelante, SGSI).

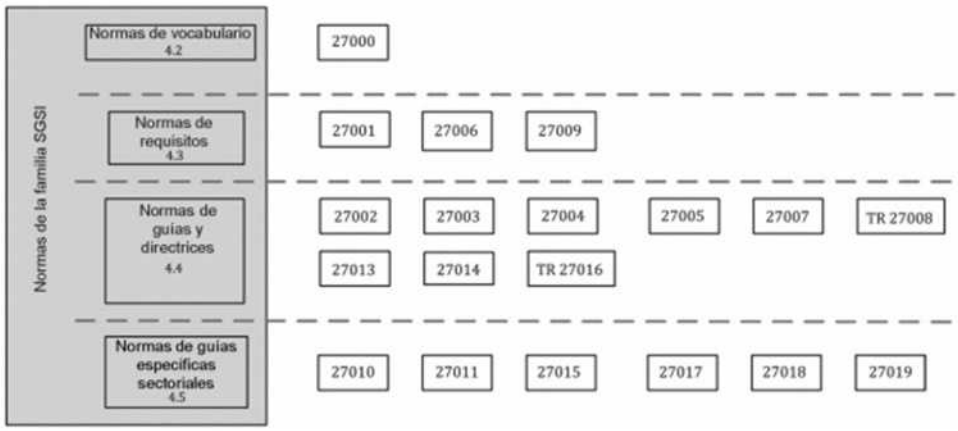


Figura 8. Normas de la familia SGSI. Fuente: UNE—EN ISO/IEC 27000:2019

La norma ISO/IEC 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en los SGSI. En ella se define el riesgo como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños y se relaciona el riesgo con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. El estándar internacional utiliza un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de tratamiento de riesgos. A través de este sistema de gestión se identifican los activos de información que se deben proteger, entre ellos protección de datos personales, y se valoran los riesgos desde una perspectiva de debilidades o vulnerabilidades y amenazas a las que están expuestos proponiéndose controles de para tratar el riesgo reduciéndolo, aceptándolo, transfiriéndolo o incluso eliminándolo.

La norma internacional es muy completa e incluye anexos específicos de matriz de riesgos, para definir el alcance y límites del sistema de seguridad, para identificar y valorar los activos en función de su impacto, para cuantificar la probabilidad y el impacto del riesgo, así como propone métodos para asesorar en relación con las vulnerabilidades, la amenazas tradicionales y definición de riesgo aceptable y criterios para su modificación.

En la figura 8, en inglés, se detalla el paso del riesgo inherente al riesgo residual, en el tratamiento de riesgos aceptables como consecuencia de un asesoramiento satisfactorio.

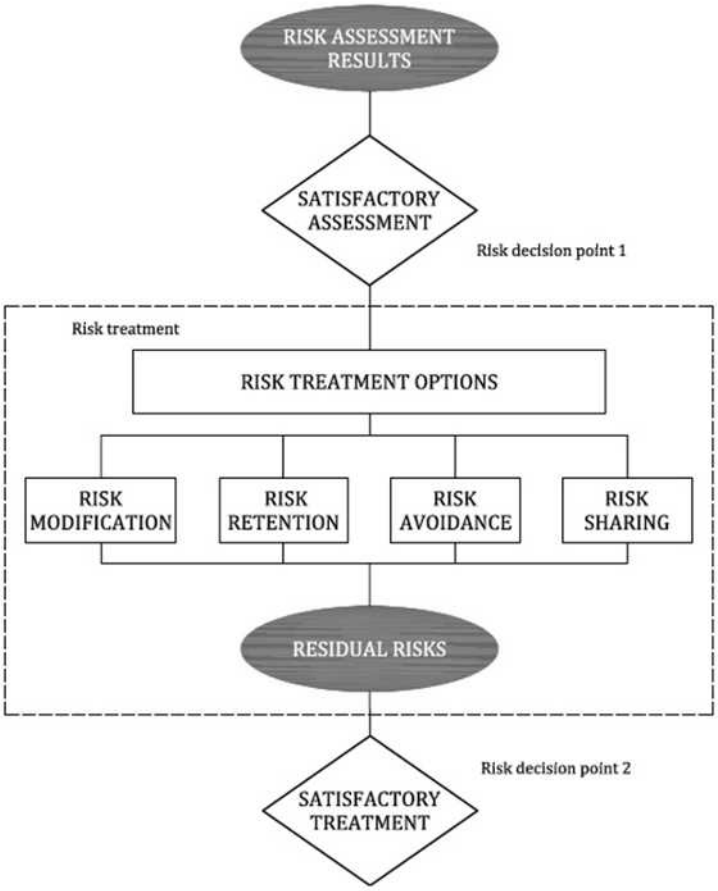


Figura 9. De la evaluación al tratamiento aceptable. Fuente: UNE—EN ISO/IEC 27005:2018

3.10. La norma NIST SP 800-39 sobre gestión de riesgos de la seguridad de la información

Esta metodología esta creada *ad hoc* de los sistemas de seguridad de la información y su enfoque gira entorno al riesgo, que se encuentra relacionado con el uso, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. La norma internacional citada recomienda utilizar un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de mitigación de estos.

Los factores e indicadores con los que se trabajan muestran si la empresa se encuentra sujeta o tiene una alta probabilidad de ser sometida a un riesgo que excede el riesgo permitido o riesgo aceptable. O, dicho con otras palabras, se trabaja con el indicador de los riesgos que están dentro y fuera del llamado «umbral» de riesgo. A través de este sistema de gestión se identifican los activos de información que se deben proteger, entre

ellos también los derechos de la protección de datos personales, y se valoran los riesgos desde una perspectiva de debilidades o vulnerabilidades y amenazas a las que se exponen, proponiéndose controles para tratar el riesgo reduciéndolo, aceptándolo, transfiriéndolo o incluso eliminándolo.

3.11. El método Mosler

El método Mosler es un método eficaz que permite identificar, analizar y evaluar los riesgos, muy utilizado especialmente en el ámbito de la compliance penal y específico para la prevención de riesgos penales. A nivel genérico, el método de Mosler se suele utilizar para evaluar los riesgos que se producen en determinadas actividades, así como aquellos que vienen dados por factores externos a las mismas, pero siempre en el ámbito de los riesgos físicos.

Su aplicación es trasladable al ámbito de riesgos físicos, lo que incluye también catástrofes o causas naturales, y tiene el punto de partida de su enfoque en la visión de la organización en su conjunto. El primer paso es determinar qué escenarios de riesgos o delitos, por ejemplo, el de revelación de secretos, podrían llegar a afectar en la práctica a la organización. El segundo es el análisis de riesgos y por último habrá que contemplar qué elementos debería tener la organización para prevenir cada escenario de riesgo.

De esta forma, el análisis del riesgo se determina en función de los siguientes parámetros:

- Función: afectación del delito al funcionamiento del día a día de la empresa.
- Sustitución: mide la facilidad de sustituir a las personas/cosas afectadas.
- Profundidad: mide el efecto psicológico sobre los trabajadores y sus consecuencias.
- Externalización: se calcula si los efectos negativos serían de carácter individual, local, regional, estatal o internacional.
- Agresión: valora la sanción que el Código Penal impone a cada delito.
- Vulnerabilidad: se valora la posibilidad real de que se llegue a materializar el riesgo.

Cada uno de estos parámetros se puntúa en una escala del uno al cinco y en el que la puntuación otorgada viene definida por una serie de criterios individualizados que el propio modelo define. A partir de ahí, se establecen tres campos para la valoración del riesgo:

- Importancia del riesgo = función x sustitución
- Daño ocasionado = profundidad x externalización
- Peligro = agresión x vulnerabilidad

El método de Mosler también define que el llamado carácter del riesgo es igual a importancia x daño, para finalmente sintetizar la descripción final del riesgo en torno a dos criterios definitivos: peligro y carácter. La multiplicación de estos dos valores es la que ofrece el dato que sirve para analizar el riesgo: de 2 a 250, riesgo muy bajo; de 251

a 500, riesgo bajo; de 501 a 700, riesgo medio; de 701 a 1000, riesgo alto; entre 1001 y 1250, riesgo muy alto.

3.12. El Esquema Nacional de Seguridad

El ENS no constituye ni incorpora una metodología en sentido escrito, sino que establece unos principios básicos y medidas de seguridad mínimas que son asignadas en base a tres niveles de seguridad. El nivel de seguridad bajo se aplicará cuando las consecuencias de un incidente de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados; el nivel de seguridad medio se aplicará cuando supongan un perjuicio grave y el nivel de seguridad alto se aplicará cuando las consecuencias supongan un perjuicio muy grave.

Una de las principales novedades de la LOPDGDD es que el ENS resulta de aplicación preceptiva tanto para el sector público como para aquellos terceros que presten un servicio en régimen de concesión, encomienda de gestión o contrato con este. La disposición adicional primera de la LOPDGDD establece que:

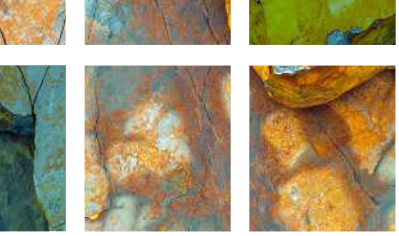
> «El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del (RGPD) Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad».

La implantación y aplicación del ENS puede realizarse siguiendo la metodología MAGERIT, que hemos analizado anteriormente, y que ha sido desarrollada *ad hoc* del ENS y de sus medidas de seguridad.

3.13. Metodología OCEG

El modelo *Open Compliance and Ethics Group* (en adelante, OCEG) constituye un estándar con reconocimiento internacional. Surge de un grupo de discusión diverso que integra economistas, filósofos, financieros, contables y también a la comunidad jurídica. OCEG se centra en el estudio e interrelación de tres elementos esenciales: gobernanza, gestión del riesgo y cumplimiento normativo, para definir la gestión integrada de todos ellos en un único modelo de *Governance, Risk and Compliance* —GRC, unas siglas muy utilizadas en los entornos de cumplimiento normativo—.

OCEG declara expresamente que su modelo permite a las organizaciones operar dentro de los condicionantes legales y contractuales, e incluye una serie de recomendaciones de elementos comunes de los que deberían disponer todos los entornos de cumplimiento: respaldo cultural; estructuras de cumplimiento; identificación de riesgos;



Las reformas introducidas por el legislador nacional en la última década abrazan una forma de entender el cumplimiento normativo desconocida hasta hace bien poco por nuestro ordenamiento jurídico y entrañan *de facto* cambios estructurales cuya profundidad y relevancia es tal que incluso podemos hablar sin problemas de una nueva cultura de cumplimiento normativo.

Una cultura basada en la responsabilidad proactiva y la autorresponsabilidad que se impone desplegando y proyectando sus efectos sobre ámbitos legales muy diversos, entre los que destaca la prevención del delito en la empresa. El elemento nuclear del sistema, que exige comunicación y consulta a la par que revisión y mejora continua, radica precisamente en el mapa de riesgos de la empresa, como instrumento que en la práctica debe permitir gestionar y monitorizar los riesgos de forma eficaz.

La obra, que aglutina autores referentes a nivel nacional e internacional, está dividida en cuatro partes claramente diferenciadas: la primera ofrece al lector una visión sistemática sobre la prevención del delito y el mapa de riesgos en la empresa; la segunda hace lo propio analizando las peculiaridades de determinados sectores de actividad (tercer sector, pymes, sector financiero y public compliance); la tercera estudia el mapa de (ciber)riesgos, con detalle de sus efectos en el ámbito de la protección de datos y la seguridad de la información; finalmente, la cuarta, es en realidad un completo bloque de capítulos de Derecho penal y procesal sustantivo relacionada con la responsabilidad penal de las personas jurídicas.

ISBN: 978-84-9090-461-9
9 788490 904619
3652K29055

Wolters Kluwer