Entregable de la ENISA:

Paquete informativo para PYME

Con ejemplos de evaluación y de gestión de riesgos de dos PYME

(disponible asimismo en www.enisa.europa.eu/rmra)

Elaborado por el
Departamento Técnico de la ENISA
Sección de Gestión de Riesgos
en colaboración con:

George Patsis
Obrela Security Industries (OSI)
www.obrela.com

Febrero de 2007

Aviso legal

Resumen ejecutivo

En el presente documento se recoge el segundo entregable de la ENISA mencionado en el Programa de trabajo de la Agencia para 2006. Determinadas partes de esta publicación se basan en la necesidad comunicada a la ENISA de contar con un enfoque simplificado de la evaluación de riesgos.

El presente documento trata de ofrecer una visión simplificada y exhaustiva de la gestión y la evaluación de riesgos para su uso en pequeñas y medianas empresas (PYME). Para ello, se adopta una estructura modular, cada una de cuyas partes se dedica a las necesidades específicas de las partes interesadas que intervienen en el proceso de evaluación y gestión de riesgos.

El planteamiento subyacente a esta publicación es el de proteger a los usuarios (no expertos) de la complejidad de las actividades de gestión y evaluación de riesgos. Para ello, se simplifican ciertos asuntos complejos relacionados con la seguridad, reduciéndolos a lo mínimo que se necesita para conseguir un nivel de seguridad aceptable.

Por supuesto, si se requiere un nivel alto de seguridad, habrá que tener en cuenta la gestión de riesgos en toda su complejidad, incluida la inmersión en los detalles concretos de las medidas y de la tecnología correspondientes. En este sentido, las ideas y el enfoque aquí presentados se han concebido con la intención de cubrir un nivel de seguridad aceptable para las organizaciones de pequeñas dimensiones con inversiones en seguridad moderadas. Unos niveles de seguridad más avanzados (en relación, por ejemplo, con los componentes críticos de la infraestructura) exigirían un tratamiento más completo, que va más allá del alcance del presente documento.

Para elaborar este material se han tenido en cuenta las diferentes destrezas que necesitan las partes que intervienen en la evaluación de riesgos. El proceso de evaluación de riesgos que se propone se estructura a partir de un enfoque en cuatro fases simplificado. No esperamos que los usuarios del presente documento tengan conocimientos avanzados de cuestiones de seguridad. En los casos en que tales conocimientos sean necesarios, el enfoque adoptado debe entenderse como una "caja negra" que ofrece un número limitado de opciones generales.

Otro criterio que se ha tenido en cuenta es el de la eficacia en función del coste en todas las etapas de la evaluación y la gestión de riesgos. El presente documento puede ayudar a los responsables de la toma de decisiones a determinar qué enfoque es el más adecuado a su organización para evaluar riesgos, basándose en los costes y en los indicadores de rendimiento. Por otra parte, en el caso en el que se haya optado por la autoevaluación, se indican las herramientas necesarias para llevarla a cabo, sin que se requiera experiencia previa en la materia.

El enfoque simplificado de la evaluación de riesgos que se presenta es un ejemplo de buenas prácticas en la evaluación de riesgos para la información. Está claro que existen otros enfoques y buenas prácticas similares que podrían utilizarse en lugar de los aquí propuestos. En este sentido, el enfoque adoptado no constituye ni un intento de sustituir los criterios existentes, ni de redefinir buenas prácticas. Por el contrario, se expone para brindar a las PYME interesadas un instrumento que no podrían encontrar fácilmente en otras fuentes.

La aplicación de las ideas que se exponen se demuestra con ejemplos. Se han elegido dos tipos de PYME representativas, cuyos riesgos se evalúan utilizando el enfoque señalado. Tales ejemplos se presentan en el marco del enfoque de evaluación de riesgos simplificado propuesto.

Cabe mencionar que el presente documento es el primero de una serie que irá publicando la ENISA para promover la sensibilización sobre la gestión y la evaluación de riesgos en las PYME. Como tal, será objeto de ulteriores mejoras, adaptaciones y ampliaciones. En el futuro, la ENISA procederá a la validación del presente material mediante el desarrollo de proyectos piloto en PYME, la realización de tareas de evaluación y revisión a cargo de equipos de expertos, la difusión a través de asociaciones profesionales o docentes, etc. El objetivo último es obtener una versión del presente documento que pueda ser utilizada por las PYME "tal cual", es decir, sin posteriores mejoras, explicaciones o adaptaciones. Por esta razón, nos referimos al presente documento como una "versión beta", en el sentido de que se introducirán en él mejoras y ajustes adicionales tras el desarrollo de diversos proyectos piloto y la realización de actividades de aplicación y difusión, que nos conducirán a medio plazo a su perfeccionamiento.

Datos de contacto: Departamento Técnico de la ENISA, Sección de Gestión de Riesgos, Dr. L. Marinos, Experto Superior en Gestión de Riesgos; dirección de correo electrónico: RiskMngt@enisa.europa.eu

Índice

Figuras

Tablas

1. Objeto y alcance

Las pequeñas y medianas empresas (PYME) constituyen un área de atención prioritaria para la política económica de la Administración pública y revisten una especial importancia para el crecimiento económico en la Unión Europea. Las PYME nacen habitualmente de la pasión emprendedora y unos fondos reducidos, y aplican sistemas de gestión que son a menudo heterogéneos y autónomos. Por otra parte, sus activos empresariales tangibles e intangibles se definen de forma rudimentaria y, con frecuencia, su valor sólo se conoce parcialmente. Es lo que ocurre en general con uno de los activos más importantes, en concreto la información.

La información, en buena parte como cualquier otro activo empresarial, ha de gestionarse y protegerse estratégicamente. Llamamos seguridad de la información a la protección de este activo dentro de la empresa, incluidos los sistemas y los equipos utilizados para su almacenamiento, proceso y transmisión. Es imprescindible que los directivos de las PYME comprendan el valor de la información contenida en sus sistemas de negocio y que dispongan de un marco para la evaluación y la ejecución de las medidas de seguridad de la información. Se dispone de numerosos marcos y mecanismos de seguridad aprobados internacionalmente para proteger una organización contra la pérdida de información y sus posibles responsabilidades. Puesto que tales marcos son complejos, exhaustivos y, en última instancia, de aplicación costosa, son adoptados en su mayor parte por grandes organizaciones.

Habitualmente, debido a la dinámica y el desarrollo *ad hoc* de muchas PYME, en la fase de consolidación no se abordan de manera sistemática ni las cuestiones de integración ni las de seguridad. Así, las políticas y marcos para la planificación de la seguridad de la información y la recuperación en caso de catástrofe suelen ser muy rudimentarios, incluso inexistentes. A menudo, el conocimiento básico de los riesgos en materia de seguridad de la información en las PYME no va más allá de lo relativo a los virus y al software necesario para combatirlos. En cambio, las amenazas involuntarias, que plantean algunos de los mayores riesgos vinculados a la seguridad de la información para las PYME, no suelen ser objeto de programas de formación y sensibilización del personal.

Los resultados de las encuestas ponen de relieve que el nivel de sensibilización en materia de seguridad de la información entre los directivos de PYME es tan variable como el estado de sus sistemas de información, su tecnología y su seguridad. Aunque una minoría de PYME sí adoptan marcos de seguridad como el constituido por la norma ISO/IEC 27001 o su equivalente internacional, la ISO 17799, la mayoría de sus directivos no han oído hablar de las normas sobre de seguridad y consideran la seguridad de la información como una intervención técnica encaminada a tratar amenazas asociadas a virus y copias de seguridad de datos.

Lejos de culpar a los directivos de las PYME por no comprender el carácter fundamental de la seguridad de la información, en el estudio aquí recogido se concluye que han de implicarse, entender y aplicar procesos formales en este ámbito, incluida la adopción de medidas técnicas y organizativas. Sin tales medidas, sus organizaciones pueden verse gravemente afectadas por amenazas involuntarias o ataques deliberados a sus sistemas de información que, en última instancia, podrían llevarles a la quiebra.

Sirviéndose del contenido de este paquete informativo, las PYME podrán realizar evaluaciones de riesgo en sus respectivos entornos, y seleccionar y aplicar las medidas pertinentes para gestionar los riesgos que identifiquen en relación con la seguridad de la información. En el presente documento les ayudamos a definir tal esfuerzo, a decidir el modo de iniciarlo y llevarlo a cabo, y les damos directrices para que, si disponen de los recursos necesarios, procedan a realizar autoevaluaciones de riesgos para la información. A tal efecto, ofrecemos un método de evaluación de riesgos sencillo, que propicia una identificación y contención rápida y exhaustiva de los riesgos para la información.

El método de evaluación que se presenta se basa en un modelo simplificado generado para pequeñas organizaciones, que comparten ciertas características comunes. En primer lugar, sus estructuras organizativas son relativamente planas, y las personas que ocupan distintos niveles están acostumbradas a trabajar de manera conjunta. En segundo lugar, a menudo se pide al personal que realice varias tareas, con lo cual todos sus componentes quedan expuestos a los distintos procesos y procedimientos utilizados en el conjunto de la organización.

2. Estructura del documento

Para atender a las necesidades de los distintos tipos de PYME, hemos dado al presente documento una estructura modular. Dependiendo de los requisitos de cada PYME y de la medida en que pretenda abordar la evaluación de riesgos, les resultarán de utilidad distintas secciones del mismo. A las PYME que necesiten una visión general de la gestión de riesgos para formular su estrategia futura, les será útil la parte genérica (véanse el capítulo

3. Directrices para los responsables de la toma de decisiones
, y el capítulo 4

4. Un enfoque simplificado: visión general

).

Las PYME que decidan llevar a cabo por sí mismas la gestión de riesgos necesitarán consultar las partes del presente documento que contienen la descripción detallada del método de evaluación de riesgos y los ejemplos aportados (véase el capítulo

5. Directrices de autoevaluación, con dos ejemplos

). Las que vayan a proceder a una autoevaluación necesitarán el material pormenorizado que figura en los anexos para definir las medidas que han de aplicarse (véanse el

Anexo A. Tarjetas de controles organizativos
, y el

Anexo B. Tarjetas de controles basados en los activos

). Para ofrecer una mejor visión del posible uso de este documento, proponemos varios supuestos al respecto, dependiendo de la función que tenga asignada quien lo lee:

- **Personas con experiencia en actividades de gestión:** deben consultar el capítulo 3, relativo a los responsables de la toma de decisiones. En él se explican los antecedentes de la seguridad de la información y la necesidad de una gestión de riesgos. Se proponen posibles opciones para la práctica de la gestión de riesgos y se definen criterios para la toma de decisiones. Puede que los directivos tengan interés en comprender la estructura del proceso de evaluación de riesgos que se propone, la cual se recoge concretamente en el capítulo 4.
- **Miembros de un equipo de evaluación de riesgos sin experiencia:** los miembros de un equipo de evaluación de riesgos deben comprender el enfoque simplificado que se propone y examinar sus detalles y los ejemplos ofrecidos (véase el capítulo 4

4. Un enfoque simplificado: visión general

-).
- **Miembros de un equipo de evaluación de riesgos con experiencia**: los miembros de un equipo de evaluación de riesgos con experiencia deben consultar el método y comprender sus detalles. Además, pueden examinar el material presentado en los anexos y, en particular, la selección de medidas (a las que se alude también en este documento como contramedidas, controles, o controles de seguridad). Como alternativa, pueden asignarse nuevas medidas a activos existentes o añadir nuevos activos (véanse el

Anexo A. Tarjetas de controles organizativos

- , el

Anexo B. Tarjetas de controles basados en los activos

- , y el

Anexo C. Controles organizativos

-).

3. Directrices para los responsables de la toma de decisiones

3.1 Qué ha de considerar un responsable de la toma de decisiones

En la actualidad, la información creada, tratada y utilizada por una organización constituye uno de sus activos más valiosos. La revelación, puesta en peligro o indisponibilidad de la misma pueda **afectar gravemente** a la organización, constituir una **infracción de la normativa** y **perjudicar a la marca.**

La dirección tiene la responsabilidad fundamental de garantizar una seguridad adecuada de la información y de los sistemas de tratamiento de la misma. Propietarios y responsables de la toma de decisiones han de conocer el estado real de su programa de seguridad de la información, con el fin de establecer criterios adecuadamente fundados y realizar inversiones que mitiguen los riesgos de manera adecuada hasta alcanzar un nivel aceptable. Los riesgos para la información pueden dar lugar a situaciones críticas cuando se extrapolan a aspectos empresariales y jurídicos esenciales de la organización. Así, pueden ser causa de tipos de riesgos más genéricos y críticos, como los que siguen:

- **Riesgos jurídicos o de cumplimiento.** Son los que se derivan de las infracciones o la disconformidad con disposiciones legales, normas contables, reglamentos, prácticas establecidas o deontología. Pueden exponer a una organización a una publicidad negativa, a la imposición de multas, sanciones penales o sanciones civiles de índole económica, al pago de daños y perjuicios, y a la anulación de contratos. El robo de información relativa a los clientes, como los datos de tarjetas de crédito, datos financieros, datos de salud u otros datos personales, puede acarrear reclamaciones de terceros. **Reconociendo que la seguridad de la información es un creciente motivo de inquietud y una cuestión plurifacética, y con el fin de proteger los derechos civiles y garantizar la responsabilidad de las empresas, la Unión Europea y los Estados miembros han adoptado una normativa de cumplimiento obligado para las distintas organizaciones, con independencia de su tamaño o sector. Dicha normativa obliga a las empresas a aplicar controles internos para protegerse de los riesgos para la información, y con ella se pretende asimismo mejorar los procedimientos y las prácticas de gestión de riesgos.**
- **Riesgos para la estabilidad financiera**. La inactividad forzosa de las infraestructuras de producción o de gestión o la falta del personal adecuados para la ejecución de la estrategia empresarial pueden llevar al incumplimiento de los fines y los objetivos financieros perseguidos en un entorno correctamente controlado y gestionado. Una **gestión inadecuada de la seguridad de la información puede generar riesgos para la estabilidad financiera de la organización. Tales riesgos, a su vez, pueden abrir la puerta al fraude, el blanqueo de dinero, la inestabilidad financiera, etc.**
- **Riesgos para la productividad.** Implican la posibilidad de pérdidas de explotación y de que se deteriore el **servicio a los clientes,** como consecuencia del incumplimiento de los procedimientos y controles básicos de los procesos. Suelen referirse a todas las actividades de producción en colaboración que contribuyen de algún modo al suministro de un producto o a la prestación de un servicio. Estos riesgos no se limitan al uso de la tecnología; pueden ser el resultado asimismo de actividades organizativas. Se incluyen en esta categoría los riesgos derivados de la inadecuación o el control deficiente de los sistemas y aplicaciones informáticos usados en apoyo del personal en contacto con los clientes, de las operaciones de gestión de riesgo y de las unidades de contabilidad u otras. Una gestión de la seguridad de la información inadecuada puede generar grandes riesgos para la productividad, entre los que figuran unos altos costes de explotación, fallos operativos, decisiones de gestión deficientes

(precio, liquidez y exposición a riesgos crediticios), así como deterioro del **derecho a la intimidad y la perturbación de la atención a los clientes**.

- **Riesgos para la reputación y de pérdida de confianza de los clientes.** Quizá el riesgo más difícil y, sin embargo, uno de los más importantes de entender sea el del daño a la reputación de la organización, un activo intangible, pero de gran relevancia. ¿Facilitarán los clientes a una empresa sus números de tarjeta de crédito después de leer en la prensa que se ha accedido ilícitamente a la base de datos en la que están depositados? ¿Permanecerán los empleados clave en una empresa dañada de tal modo? Y, ¿cuál será la reacción de los accionistas de la compañía? ¿Qué pérdida de ingresos por actividades futuras se prevé? ¿Cuál es la pérdida prevista de capitalización de mercado?

Muchos propietarios de PYME creen que no corren riesgos a causa del tamaño de la propia empresa y de sus activos de información. La mayoría piensan que son las grandes empresas, que disponen de más activos, las únicas que se exponen a riesgos. No es cierto. En primer lugar, la sensibilidad de la información atañe a la calidad, y no a la cantidad. En segundo lugar, las PYME carecen de los recursos o el personal para abordar la seguridad de una manera tan intensiva como las grandes empresas y, por tanto, se ven más expuestas. De hecho, las nuevas tecnologías les permiten utilizar muchos de los sistemas de información que emplean las grandes empresas. Al utilizarlos, se exponen a numerosas amenazas que se asociaban tradicionalmente a las de mayor tamaño. **Así, el 56% de las pequeñas empresas han experimentado al menos un incidente de seguridad en el año anterior.** Por desgracia, una proporción significativa de las empresas que sufren de un problema informático importante nunca se recuperan, y acaban quebrando. Por tanto, es imprescindible para la continuación del éxito que los propietarios de las PYME y los responsables de la toma de decisiones reconozcan tales deficiencias y adopten medidas para abordar las cuestiones de seguridad de la información.

Las medidas de mitigación de los riesgos vinculados a la seguridad de la información (controles) deben ser proporcionadas a los riesgos a los que se expone la información en cuestión. No obstante, el proceso para determinar qué controles de seguridad son apropiados y rentables resulta a menudo complejo y, en ocasiones, tiene carácter subjetivo. **Una de las tareas primordiales para conseguir que ese proceso descanse sobre una base más objetiva consiste en la evaluación permanente de los riesgos de seguridad.**

3.2 Qué ha de saber un responsable de la toma de decisiones

La seguridad de la información tiene que ver con la identificación, reducción y gestión de los riesgos que afectan a los activos implicados. La evaluación de riesgos es el primer paso necesario para comprenderlos y exige una **identificación** y una **valoración** exhaustivas de los mismos. El resultado de tal actividad es esencial para gestionar la empresa, ya que los riesgos detectados pueden influir de manera significativa en la confidencialidad, la integridad y la disponibilidad de los activos de información, y **pueden ser esenciales para mantener una ventaja competitiva, para la estabilidad financiera, para el cumplimiento de la legislación y para el mantenimiento de una sólida imagen comercial**.

En este sentido, la evaluación de riesgos puede ayudar a los responsables de la toma de decisiones a:

- **Valorar las prácticas organizativas y la base tecnológica instalada;**
- **Ejecutar las medidas de protección de la información atendiendo a la posible repercusión en la organización;**
- **Centrar las actividades en materia de seguridad en lo que es importante. Las medidas asociadas a riesgos aceptables pueden descartarse;**
- **Garantizar que las medidas aplicadas y los gastos hechos sean proporcionados a los riesgos a los que se expone la organización. De este modo, podrá mantenerse un equilibrio entre los costes de abordar un riesgo y los beneficios derivados de la evitación de su efecto negativo**.

En una evaluación de riesgos, la organización debe (a) identificar los riesgos en materia de seguridad de la información, (b) valorar los riesgos para determinar prioridades, y (c) definir el

modo de mitigarlos (véase asimismo la **Figura 1: Actividades de evaluación de riesgos en relación con la gestión de riesgos para la seguridad de la información**

).

No obstante, la evaluación de los riesgos para la seguridad de la información constituye únicamente el primer paso en la gestión de los mismos, la cual implica un proceso continuo de identificación de riesgos y de ejecución de planes para hacerles frente. En la figura 1 se ilustra un proceso de gestión de riesgos para la seguridad de la información y la "porción" que representa en ese proceso la tarea de evaluación.

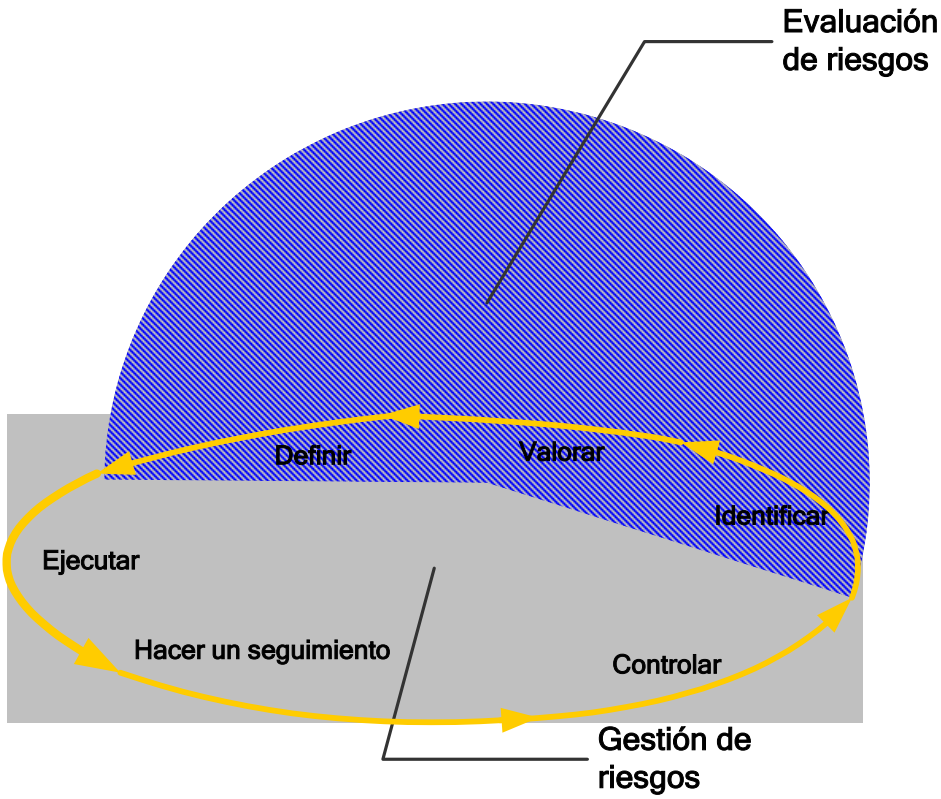

Figura 1: Actividades de evaluación de riesgos en relación con la gestión de riesgos para la seguridad de la información

Queda claro que la evaluación de riesgos en sí misma ofrece una orientación a las actividades de la organización en materia de seguridad de la información; **no da lugar necesariamente a una mejora significativa si no se aplican medidas en la práctica**. Como en cualquier otra disciplina gerencial, la realización de sólo una parte del ciclo vital de la gestión no genera por sí sola los efectos deseados. Ninguna valoración, por detallada o experta que sea, mejorará la situación de seguridad si la organización no pasa a la fase de ejecución. Aparte de la evaluación de los riesgos, una gestión eficaz de éstos comprende los **pasos que siguen**:

- **Planificar** el modo de aplicar la estrategia de protección y los planes de reducción de riesgos a partir de la valoración, mediante la formulación de planes de acción pormenorizados. Esta actividad puede incluir un análisis de coste-beneficio detallado de las distintas estrategias y acciones;
- **Ejecutar** los planes de acción pormenorizados seleccionados;
- Llevar a cabo un **seguimiento** de los planes para determinar su progreso y eficacia. Esta actividad comprende el seguimiento de los cambios acaecidos en los niveles de riesgo;
- Y **controlar** las variaciones en la ejecución del plan mediante la adopción de las acciones correctivas pertinentes.

3.3 Cómo proceder en relación con la seguridad de la información

Parte de la responsabilidad de los directivos de PYME consiste en garantizar la seguridad de su entorno empresarial. Jurídicamente, a ellos les corresponde la responsabilidad por las infracciones en materia de seguridad. Así como deben ocuparse de conseguir un entorno físico seguro, han de garantizar igualmente que la información esté protegida. Ahora bien, dado que los ordenadores no son dispositivos de "instalar y olvidarse", la protección de la información constituye un motivo de preocupación permanente.

Los responsables de la toma de decisiones pueden iniciar la evaluación de riesgos de su entorno y activar la adopción de medidas adecuadas para hacer frente a los riesgos inaceptables. Tal es la condición previa para la gestión de la seguridad de la información. Al llevar a cabo estas tareas, pueden adoptarse diversos enfoques en lo que respecta a la dotación de personal (que encajan, en sentido amplio, en el marco de las decisiones del tipo "fabricar o comprar"). Diferenciamos entre tres enfoques:

- **Internalización de la evaluación de riesgos**: la evaluación de riesgos y la identificación de las medidas necesarias se encomiendan a personal interno. La evaluación de riesgos se basa, pues, en un enfoque (p. ej., una buena práctica, una norma conocida, etc.) que es elegido por la propia organización. Con ello, la propia organización dominará ese enfoque en sucesivas aplicaciones del mismo;
- **Externalización plena de la evaluación de riesgos**: con arreglo a este enfoque, la evaluación de riesgos en su totalidad se encomienda a un contratista externo. El enfoque que se aplique será el elegido por el contratista. Pueden encomendarse asimismo a éste posteriores evaluaciones. No se prevé, pues, la transferencia de conocimientos técnicos especializados al personal interno respecto al ciclo vital completo de la evaluación y la gestión de riesgos de la PYME de que se trate;
- **Externalización parcial de la evaluación de riesgos**: en este enfoque, se encomienda parcialmente la evaluación de riesgos a una empresa externa. La evaluación de riesgos se basará, pues, en un enfoque que es conocido por la PYME en cuestión. De este modo, el personal interno podrá efectuar posteriores evaluaciones. La evaluación inicial efectuada por el contratista sirve como transferencia de conocimientos técnicos especializados al personal interno de la PYME.

El presente documento ofrece a las PYME toda la información pertinente para adoptar una decisión del tipo "fabricar o comprar". Además, incluye toda la información necesaria para facilitar a las PYME la realización de una autoevaluación. El enfoque de evaluación de riesgos propuesto puede utilizarse en las decisiones de internalización o de externalización parcial como directriz tanto para la evaluación inicial como para las evaluaciones futuras (véanse los capítulos

4.Un enfoque simplificado: visión general
, y

5.Directrices de autoevaluación, con dos ejemplos
).

Cada enfoque de la evaluación de riesgos tiene ventajas e inconvenientes en comparación con los demás. En la Tabla 1: Opciones de realización de las evaluaciones de riesgos se ofrece una primera impresión de los hechos relacionados con la decisión del tipo "fabricar o comprar" en lo que respecta a la tarea de evaluación de riesgos. En los apartados que siguen se analizan con detenimiento los parámetros y los factores que deben considerarse al optar por un enfoque determinado de la gestión de riesgos en una PYME.

Opciones de ejecución de las evaluaciones de riesgos	Parámetros y factores de realización				
	Necesidad de conocimientos prácticos internos	Dependencia respecto a terceros	Necesidad de recursos internos	Objetividad de la evaluación	Trabajo[1] de terceros
Internalización	Sí	Baja	1 a 5 personas	Baja	-
Externalización plena	No	Alta	1 persona (para la gestión del proyecto)	Alta	10 a 40 días
Externalización parcial	Sí	Baja	1 o 2 personas	Media	5 a 10 días

Tabla 1: Opciones de realización de las evaluaciones de riesgos

En los apartados que siguen se describen las distintas opciones posibles para la realización de la evaluación y la gestión de riesgos. Un cuestionario ayudará a los responsables de la toma de decisiones a establecer si una determinada opción es adecuada para un tipo dado de PYME.

3.3.1 Internalización

La internalización puede ofrecer numerosas **ventajas, como el desarrollo de una base interna de conocimientos técnicos especializados y de competencias en materia de evaluación y gestión de riesgos. Además, dependiendo de los precios de las actividades de consultoría en el mercado de la seguridad, puede dar lugar a una reducción de los gastos.** Se trata de una opción especialmente atractiva para organizaciones con una estructura sencilla, un historial positivo en la realización interna de actividades similares (p. ej., adaptación a la norma ISO 9001) y capacidad y destrezas adecuadas.

Pueden utilizarse las preguntas que siguen para determinar si la evaluación de riesgos mediante el empleo de personal interno constituye la decisión correcta para una organización:

Preguntas para la toma de decisión	Respuesta	
	☺ Sí	☹ No
¿Es pequeña su organización? ¿Cuenta con una estructura jerárquica horizontal o simple?		
¿Dispone de **conocimientos técnicos especializados en sistemas y redes de TI?**		

[1] El tiempo de trabajo está calculado para una PYME de hasta 100 miembros en plantilla.

¿Cuenta con recursos humanos cualificados y disponibles?		
¿**Dependen sus actividades poco de los sistemas de TI** y no implican el almacenamiento o proceso de datos sobre sus clientes de índole sensible? ¿Ha participado su organización en actividades similares, como las relativas a procesos de mejora de la calidad?		
¿Puede disponer de un grupo de tres a cinco personas que cuenten con un conocimiento amplio y profundo de la organización y posean además la mayor parte de las destrezas que siguen? ▫ capacidad para la resolución de problemas ▫ capacidad analítica ▫ capacidad para trabajar en equipo ▫ destrezas de liderazgo ▫ **capacidad para comprender los procesos empresariales de la compañía y la infraestructura subyacente a la organización** ▫ capacidad para pasar unos días trabajando en este método.		
¿Dispone de una infraestructura de tecnología de la información relativamente sencilla que sea bien conocida al menos por un miembro de su organización?		

Cuantas más respuestas afirmativas se hayan dado a estas preguntas, mayor será la probabilidad de que una autoevaluación de los riesgos constituya la opción adecuada.

Sirviéndose del enfoque de evaluación de riesgos propuesto y de las buenas prácticas aportadas (véanse los capítulos

4. Un enfoque simplificado: visión general

, y

5. Directrices de autoevaluación, con dos ejemplos

), los responsables de la toma de decisiones podrán poner en marcha evaluaciones de riesgos con un enfoque eficaz para identificar y gestionar sus riesgos en materia de seguridad de la información, lo que les permitirá mejorar de manera continua su situación en este ámbito.

3.3.2 Externalización plena

Mediante la externalización plena, una PYME transfiere en su totalidad las tareas de evaluación y gestión del riesgo a un contratista externo. Pueden incluirse en esa transferencia la evaluación inicial y las evaluaciones posteriores, así como actividades de gestión que abarquen todo el ciclo vital de gestión de riesgos (p. ej., aplicación y mantenimiento de las medidas). El contratista aplica su propio enfoque de la evaluación y la gestión de los riesgos. De este modo, no se produce ninguna transferencia de conocimientos técnicos especializados al cliente. Cabe señalar, en todo caso, que la externalización de las actividades de evaluación y de gestión no exime a la dirección de las PYME de su responsabilidad en materia de seguridad (de la información).

Dependiendo de la estructura, la estrategia, los recursos disponibles y la situación del mercado, la externalización **puede ofrecer ventajas inequívocas**. La decisión de externalizar la evaluación de los riesgos para la información permite a las PYME centrarse en las estrategias empresariales esenciales, dejando las actividades periféricas en manos de un experto externo especializado en la seguridad de la información.

Pueden utilizarse las preguntas que siguen para determinar si la externalización plena de la evaluación de riesgos constituye la decisión correcta para una organización:

Preguntas para la toma de decisión	**Respuesta**	
	☺ **SÍ**	☹ **No**
¿Considera necesario **prestar especial atención** a las competencias esenciales y los procesos empresariales estratégicos?		
¿Le **resultaría difícil disponer de un grupo de dos a cinco personas** que cuenten con un conocimiento amplio y profundo de la organización, y tengan además la mayoría de las destrezas que siguen? o **Capacidad para comprender los procesos empresariales y la infraestructura subyacente a la organización** o capacidad para la resolución de problemas o capacidad analítica o capacidad para trabajar en equipo o destrezas de liderazgo o posibilidad de pasar unos días trabajando en este método.		
¿Cuenta con una **infraestructura de TI relativamente grande y de gran complejidad**?		
¿Implican sus actividades empresariales y sus ofertas de servicios **transacciones financieras**?		
¿Está su empresa sujeta en gran medida a unos requisitos o una legislación nacional o comunitaria rigurosos?		
¿Dispone de una infraestructura de tecnología de la información relativamente sencilla que sea bien conocida al menos por un miembro de su organización?		

De nuevo en esta ocasión, cuantas más respuestas afirmativas se den, más adecuada resultará la externalización.

Subcontratar con terceros las actividades de evaluación de riesgos exige **un proceso de selección de proveedores, incluida una auditoría jurídica y la valoración global de los mismos, así como la evaluación de su competencia en el terreno de la seguridad de la información**

(véase asimismo el

Anexo E. Consejos sencillos

, Si todo esto le parece un tanto difícil, no intente hacerlo por su cuenta. Solicite a un experto que le instale su red wifi. No olvide que sus datos constituyen probablemente su activo más importante, y han de protegerse con una red wifi segura. Después de todo, lo que quiere no es convertir su red en un punto de acceso público.

, solicitar del tercero en cuestión el privilegio de auditar sus medidas de protección de la seguridad, sobre todo en los casos en que se procese información corporativa propia y confidencial en sus instalaciones.

).

(el anexo E. Asesoramiento simple, terceros, proveedores de servicios).

Si se opta por la externalización, la cooperación debe basarse en un contrato de nivel de servicio en el que se definan los elementos esenciales, como la certificación profesional de los técnicos de seguridad del proveedor, la confidencialidad y la obligación de no revelación, el plazo, la asignación de recursos, el coste y la metodología que se empleará.

Al suscribir un contrato de nivel de servicio (CNS), deben considerarse las preguntas que siguen (a modo de lista de comprobación):

- **¿Se tratan las cuestiones de responsabilidad?** ¿Qué sucederá por ejemplo si, durante la evaluación, se interrumpen o perturban actividades empresariales fundamentales debido a la incompetencia del proveedor para llevar a cabo la evaluación de la infraestructura de TI y de la red subyacente?
- ¿**Se determinan claramente las responsabilidades**? ¿Quién será responsable de hacer qué? ¿Cuál es la implicación de la organización en lo que se refiere a los recursos?
- **¿Se ha documentado claramente el alcance de las prestaciones?** ¿Qué prestaciones del proveedor se incluyen? Se recomienda encarecidamente que el alcance de las prestaciones comprenda la gama completa de actividades empresariales y la infraestructura subyacente. En cualquier otro caso, es posible que el resultado resulte inadecuado, o incluso engañoso.
- ¿**Cómo deben cumplirse los requisitos jurídicos**, como los previstos en la legislación sobre protección de datos?
- ¿De qué mecanismos se dispondrá para que todas las partes intervinientes en la externalización, incluidos los subcontratistas, sean conscientes de sus responsabilidades en materia de seguridad?
- **¿Cómo se mantendrán y comprobarán la integridad y la confidencialidad de los activos empresariales de la organización?**
- **¿Qué controles físicos y lógicos se emplearán para restringir y limitar el acceso a la información empresarial sensible de la organización a usuarios autorizados?**
- **¿Cómo se garantizarán los servicios en caso de catástrofe?**
- **¿Se incluye en el contrato el derecho a auditar las medidas de protección de la seguridad y la información del proveedor?**
- ¿Se exponen claramente los **recursos mínimos, competencias y certificación profesional** del proveedor?
- ¿Se definen claramente el contenido, la frecuencia y la estructura de los informes?

Obviamente, las organizaciones pueden pedir a los proveedores que ajusten sus evaluaciones a la metodología del enfoque de gestión del riesgo propuesto en este documento (véase el capítulo

5.Directrices de autoevaluación, con dos ejemplos
). En la medida en que la PYME comprenda el contenido del enfoque propuesto, podrá avanzar en el control de las actividades del contratista.

3.3.3 Externalización parcial

Una solución mixta **puede combinar las ventajas tanto de la internalización como de la externalización**. Con una solución de esta índole, la organización puede participar activamente en un proceso de autoevaluación y utilizar a un tercero como "facilitador". Por otra parte, la evaluación de riesgos se basa en este caso en un modelo comprendido por el cliente, como el enfoque descrito en el presente documento (véase el capítulo

4.Un enfoque simplificado: visión general

). Ésta es una **condición previa** necesaria **para conseguir la transferencia de conocimientos técnicos especializados** entre contratista y cliente.

En este supuesto, la PYME desarrolla la capacidad interna para llevar a cabo algunas de las tareas de seguridad relevantes en el plazo y en los casos pertinentes. Pueden derivarse ventajas inequívocas de la posibilidad, por parte de la organización, de regular y gestionar futuros costes de subcontratación y contribuir de manera significativa a los conocimientos prácticos aportados por un tercero especializado.

Pueden utilizarse las preguntas que siguen para determinar si una evaluación de riesgos debe externalizarse parcialmente o no:

Preguntas para la toma de decisión	**Respuesta**	
	☺ **SÍ**	☹ **No**
¿**Considera necesario seguir haciendo hincapié en las competencias esenciales** y los procesos empresariales estratégicos, pero también mejorar el grado de sensibilización interno respecto a la seguridad de la información y la competencia en asuntos que atañen a ésta?		
¿**Podrá disponer de una o dos personas** en su organización que cuenten con un conocimiento amplio y profundo de la organización, y tengan además la mayoría de las destrezas que siguen? ▫ **Capacidad para comprender los procesos empresariales y la infraestructura subyacente a la organización** ▫ capacidad para la resolución de problemas ▫ capacidad analítica ▫ capacidad para trabajar en equipo ▫ destrezas de liderazgo ▫ capacidad para pasar unos días trabajando en este método. ▫ sujeción a un contrato de empleo de mayor duración		
¿**Cuenta con una infraestructura de TI compleja y relativamente grande**, pero con un modelo de negocio relativamente simple?		
¿**Implican sus actividades empresariales y sus ofertas de servicios transacciones financieras**?		
¿Está su empresa sujeta en gran medida a unos requisitos o una legislación nacional o comunitaria rigurosos?		

Como en los enfoques de ejecución previos, cuantas más preguntas se hayan respondido afirmativamente, más adecuada será la elección para la PYME en cuestión.

La decisión de externalizar parcialmente la evaluación de riesgos exige la firma con el contratista de un contrato de nivel de servicio (CNS) como base de partida para la cooperación con él. Entre los elementos esenciales de un CNS figuran la certificación profesional de los técnicos de seguridad del proveedor, la confidencialidad, los plazos, la asignación de recursos, el coste y la metodología a emplear. De nuevo en esta ocasión, las organizaciones pueden pedir al proveedor que se ajuste a la metodología ENISA propuesta en este documento (véase el capítulo

4. Un enfoque simplificado: visión general
).

En los CNS de externalización de las evaluaciones de riesgos para la seguridad de la información deben considerarse, como mínimo, las siguientes cuestiones:

- ¿Conviene el contratista en utilizar un enfoque de evaluación de riesgos predefinido que también conozca el cliente (p. ej., el enfoque aquí propuesto)?
- ¿Se tratan las cuestiones de **responsabilidad**? ¿Qué sucederá por ejemplo si, durante la evaluación, se interrumpen o perturban actividades empresariales fundamentales debido a la incompetencia del proveedor para llevar a cabo la evaluación de la infraestructura de TI y de la red subyacente?
- ¿Se determinan claramente las **responsabilidades** en el CNS? ¿Quién será responsable de hacer qué? ¿Qué intervención tiene la organización en lo que se refiere a los recursos?
- ¿Se ha documentado claramente el **alcance** de las prestaciones? ¿Qué prestaciones del proveedor se incluyen? Se recomienda encarecidamente que el alcance de las prestaciones comprenda la gama completa de actividades empresariales y la infraestructura subyacente. En cualquier otro caso, es posible que el resultado resulte inadecuado, o incluso engañoso.
- ¿Cómo deben cumplirse los **requisitos jurídicos**, como los previstos en la legislación sobre protección de datos?
- ¿De qué mecanismos se dispondrá para que todas las partes intervinientes en la externalización, incluidos los subcontratistas, sean conscientes de sus responsabilidades en materia de seguridad?
- ¿Cómo se mantendrán y comprobarán la **integridad y la confidencialidad de los activos empresariales de la organización?**
- ¿Qué **controles físicos y lógicos** se emplearán para restringir y limitar el acceso a la información empresarial sensible de la organización a usuarios autorizados?
- ¿Cómo se **mantendrá la disponibilidad de los servicios en caso de catástrofe**?
- ¿Se incluye en el contrato **el derecho a auditar** las medidas de protección de la seguridad y la información del **proveedor**?
- ¿Se señalan claramente los **recursos mínimos, competencias y certificación profesional del proveedor**?
- ¿Se definen claramente el contenido, la frecuencia y la estructura de los informes?

4. Un enfoque simplificado: visión general

En este capítulo se expone el contenido de un enfoque simplificado de la evaluación y la gestión de riesgos que puede ser utilizado por las PYME en tareas de autoevaluación, incluso en el marco de proyectos de externalización, como se indica en el capítulo 3.

La mayoría de los enfoques existentes de la evaluación y la gestión de los riesgos de seguridad suelen centrarse en las necesidades de las grandes organizaciones. Actualmente no existe ningún enfoque sencillo diseñado para pequeñas organizaciones, al menos no en forma de directrices disponibles con carácter general. Algunas empresas consultoras han elaborado buenas prácticas a tal fin, pero las utilizan en sus proyectos específicos para determinados clientes. Otros enfoques, aunque se arguye su idoneidad para PYME, siguen siendo demasiado complejos para las autoevaluaciones (p. ej., OCTAVE). Por otro lado, como ya se ha comentado, la mayoría de las PYME no pueden permitirse el coste de externalizar plenamente esta función a terceros.

Nuestra intención es ofrecer a estas organizaciones un enfoque sencillo, eficaz y asequible para la identificación y la gestión de sus riesgos en cuanto a la seguridad de la información. **El enfoque simplificado resultante les dota de un medio para llevar a cabo autoevaluaciones. Se basa en los principios, atributos y resultados de OCTAVE[2] , y se ha adaptado a los entornos y las necesidades habituales de las PYME. De hecho, es un enfoque compatible asimismo con otras normas, como la ISO 13335-2.**

Para una organización que trata de conocer sus necesidades en materia de seguridad de la información, el enfoque presente comprende una técnica de autoevaluación y de planificación de la seguridad basada en la determinación del perfil de riesgos. A diferencia de evaluaciones típicas únicamente centradas en el riesgo tecnológico, en este método se fijan como objetivo el contexto y los riesgos inherentes y se da prioridad a las cuestiones estratégicas relacionadas con la práctica.

La ventaja principal de este enfoque es que puede ofrecer un nivel de seguridad aceptable con un moderado esfuerzo en materia de evaluación y gestión. Tal ventaja se debe a los siguientes aspectos, que potencian su viabilidad:

- El perfil de riesgos de la organización puede identificarse fácilmente;
- Se consideran los activos habituales de las pequeñas organizaciones;
- La protección de los activos mediante determinadas medidas (controles) se define previamente con la ayuda de tarjetas de controles.

Estas ventajas pueden dar lugar a una autoevaluación de bajo coste a cargo de equipos con escasos conocimientos prácticos en materia de seguridad. Si se realiza con precaución y detenimiento, se obtendrá un nivel de seguridad aceptable.

El enfoque de evaluación propuesto puede ser aplicado por no expertos. Durante la evaluación, el equipo encargado de realizarla no tendrá que hacer frente a los diversos aspectos de las amenazas a las que se exponen los activos vulnerables. Por el contrario, se propone un nivel de protección predefinido con arreglo al tipo de activo y al nivel de seguridad exigido.

El desarrollo del modelo de riesgo que subyace a este enfoque se basa en los siguientes supuestos y elementos:

- **La evaluación de los riesgos inherentes** – El entorno puede definir a menudo el contexto de riesgos (riesgos inherentes) en el que opera una empresa. Por ejemplo, una pequeña empresa del sector de panadería opera en un marco de riesgos significativamente menor que el de otra que se dedique a la atención sanitaria o a la prestación de servicios de inteligencia empresarial. Con independencia de las medidas de seguridad, de la infraestructura y de los ingresos, las dos empresas operan en entornos de riesgo totalmente diferentes, que han de considerarse detenidamente antes de formular una estrategia de seguridad de la información, y de seleccionar los controles de seguridad.

[2] *Operationally Critical Threat, Asset, and Vulnerability Evaluation* y OCTAVE son marcas de servicio de la Carnegie Mellon University. OCTAVE se formuló en el Centro de Coordinación de CERT (CERT/CC). Constituido en 1988, es el equipo de respuesta a cuestiones de seguridad informática que lleva más años activo.

- **Los distintos escenarios (perfiles) de amenazas que se dan en las PYME.** En el contexto de las PYME, a pesar de la dispersión que es lógico esperar en lo que respecta a los riesgos inherentes, observamos que las amenazas son más bien típicas y, en la mayoría de los casos, cuando se agrupan, delinean perfiles genéricos aplicables a un gran número de estas empresas. En este sentido, nuestra labor se centró en el establecimiento de modelos mediante la elaboración de perfiles de amenazas genéricos. Los perfiles de riesgos así elaborados ayudan a reflejar el nivel de riesgo inherente de cada organización. Posteriormente, identificamos y agrupamos distintas medidas encaminadas a abordar las amenazas correspondientes a los respectivos perfiles de riesgos.

El **enfoque propuesto es de carácter autodirigido**, en el sentido de que el personal de cada organización asume la responsabilidad de la evaluación de los riesgos, de la selección de los controles y, por tanto, del establecimiento de su estrategia de seguridad. Esta técnica se apoya en el conocimiento por parte del personal de las prácticas y los procesos de seguridad de su organización para **(a) determinar el estado actual de la práctica de la seguridad en la organización, (b) identificar los riesgos que se refieren a los activos críticos, (c) asignar prioridades a las áreas de mejora y establecer la estrategia de seguridad de la organización**. Con estas tareas, se cubre el ciclo vital completo de la evaluación y la gestión de riesgos.

Al aplicar el enfoque propuesto, un pequeño equipo de personas procedentes de las unidades operativas (o de negocio) y del departamento de tecnologías de la información (TI) colaboran para abordar las necesidades de seguridad de la organización, equilibrando así dos aspectos fundamentales al respecto: las medidas organizativas y las basadas en los activos.

Se anima encarecidamente a las organizaciones a aplicar las directrices y las buenas prácticas incluidas en este enfoque únicamente como un plan a corto plazo para satisfacer el objetivo de proteger con rapidez y eficacia los componentes críticos de su actividad empresarial. El contenido de este enfoque cubre los riesgos significativos a los que suelen exponerse las PYME. Sin embargo, no debe entenderse como un sustitutivo permanente de una evaluación completa y exhaustiva de los riesgos que atañen a activos esenciales. Recomendamos firmemente tales "inmersiones" para mejorar la evaluación de los riesgos, sobre todo si se utilizan componentes complejos en relación con activos de gran valor.

Los objetivos que subyacen a la adopción de este enfoque de la evaluación y la gestión de riesgos son los que siguen:

- **Mejorar los umbrales de seguridad de la información existentes en Europa**. El enfoque puede utilizarse como catalizador para acelerar las iniciativas de las PYME en materia de gestión de los riesgos para la seguridad de la información mediante el tratamiento de los riesgos elevados. Por otra parte, mediante la determinación como objetivo de los escenarios de amenaza habituales, mejorarán en última instancia los umbrales de seguridad de la información existentes en Europa.
- Atender los requisitos empresariales, el contexto y las restricciones que suelen darse en los entornos de las PYME, **evitando la terminología especializada y suprimiendo las tareas de elevada exigencia** incorporadas en casi todas las metodologías profesionales y normas sectoriales existentes (es decir, la evaluación de activos, el análisis de impacto empresarial, la identificación de requisitos de seguridad, etc.).
- **Utilizar un enfoque autodirigido** adaptado a los medios, recursos y conocimientos prácticos habituales en el entorno de las PYME.
- **Hacer hincapié en los activos críticos y los mayores riesgos**. El método se elaboró a modo de guía fácil y sencilla para identificar y proteger los activos considerados de mayor relevancia para las organizaciones.
- Elaborar un método de evaluación y de gestión de riesgos **independiente de la adopción de medidas concretas**. A efectos de la obtención de un primer resultado práctico y realista, se han utilizado los controles de OCTAVE. No obstante, el método permite utilizar casi todos los controles normalizados disponibles en la actualidad (ISO, BS7799, NIST, BSI).

4.2 Supuestos de trabajo

Además de los objetivos mencionados, para la elaboración de la presente guía y el enfoque de la evaluación de riesgos que se describe en ella se han tenido en cuenta ciertas consideraciones y supuestos:

- En muchos casos, la PYME puede estar poco familiarizada con la seguridad informática y, en consecuencia, puede beneficiarse del acceso a materiales de sensibilización, formación y orientación.
- El establecimiento de un marco de orientación sobre seguridad a través de los organismos y asociaciones sectoriales de PYME contribuirá a promover el conocimiento de las cuestiones de seguridad por las que tienen escaso bagaje en el terreno de la seguridad de la información.
- Las PYME constituyen un área de atención prioritaria para la política económica de la UE y revisten una especial importancia para el crecimiento económico en la Unión Europea.
- Las PYME nacen habitualmente de la pasión emprendedora y de una financiación limitada y aplican sistemas empresariales a menudo improvisados y, por tanto, heterogéneos y autónomos.
- No suele haber políticas y marcos para la planificación de la seguridad de la información y la recuperación en caso de catástrofe entre las PYME. Además, el conocimiento básico de los riesgos en materia de seguridad de la información en las PYME no se extiende más allá de los virus y del software necesario para combatirlos.
- La mayoría de directivos de PYME apenas comprenden la terminología científica compleja y de elevado nivel técnico relacionada con la seguridad de la información.
- Las empresas de pequeño tamaño suelen operar en un marco en el que el entorno de proceso de datos está normalizado pero es importante para su actividad. Utilizan paquetes informáticos de uso general, que funcionan en parte o en todo como una "caja negra" (con todos los riesgos potenciales asociados), y se conectan a Internet, donde acechan multitud de amenazas para la seguridad de las TI.
- Aunque las amenazas involuntarias plantean algunos de los mayores riesgos vinculados a la seguridad de la información para las PYME, con frecuencia se pasan por alto los programas de formación y sensibilización del personal. Incluso en los casos en que el personal de PYME posee conocimientos especiales de los sistemas de información, es posible que no cuente con conocimientos técnicos específicos sobre asuntos de seguridad de las TI. Un factor agravante es que las empresas, en general, no pueden permitirse invertir recursos suficientes en la evaluación y la gestión de riesgos.

4.3 Un enfoque en cuatro fases

El enfoque de evaluación de riesgos propuesto se divide en **cuatro fases** en las que se examinan las cuestiones de seguridad tecnológica y organizativa, obteniéndose de este modo una visión global de las necesidades en materia de seguridad de la información. Las cuatro fases se ilustran en la figura 2.

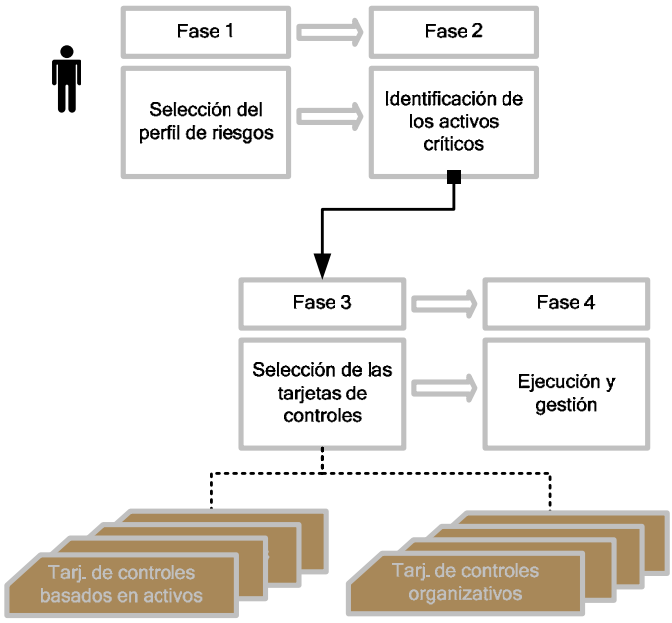

Figura 2: Las cuatro fases del enfoque de evaluación de riesgos propuesto

En el enfoque de la evaluación de riesgos influyen dos aspectos esenciales: **(1) el perfil de riesgos de la empresa, y (2) la identificación de los activos críticos**.

La evaluación de riesgos está dirigida por un pequeño equipo de evaluación interdisciplinario (de tres a cinco miembros, constituido por personal de la PYME, personal externo o personal combinado en función de lo que se indica en el capítulo 3.3 Cómo proceder en relación con la seguridad de la información) que recaba y analiza información y elabora planes de mitigación basados en los riesgos de la organización en materia de seguridad. Para actuar de manera eficaz, el equipo debe tener un amplio conocimiento de las actividades de la organización (a los que se alude asimismo como procesos empresariales) y de su infraestructura de TI.

Como punto de partida, el equipo debe **utilizar la tabla de evaluación del perfil de riesgos para determinar el perfil específico de la empresa en cuestión**. El paso siguiente consiste en la **identificación de los activos críticos de la organización** y de los **requisitos de seguridad** pertinentes desde el punto de vista de la confidencialidad, la integridad y la disponibilidad.

A continuación, hay que seleccionar los controles (tarjetas de controles). El uso de tarjetas de este tipo normalizadas simplifica radicalmente el proceso de selección. Con este fin, el equipo no tiene más que **"elegir" las tarjetas de controles asociados a los riesgos,** tanto para la organización como para los activos críticos identificados, preparadas para cada nivel de perfil de riesgos, categoría de activos y requisito de seguridad (confidencialidad, integridad, disponibilidad).

Las tarjetas prevén controles que se han tomado del catálogo de prácticas utilizado en OCTAVE. Se ha tomado esta decisión porque dichos controles son muy sencillos y resultan más fáciles de comprender por personal no experto en seguridad. Por supuesto, como alternativa pueden utilizarse otros controles. Posiblemente habrá que hacerlo así cuando la PYME tenga ya una política de seguridad basada en otra norma (p. ej., ISO 17799).

En el paso final, el equipo de evaluación de la PYME se ocupa de asignar prioridades a los activos con arreglo a su importancia y efecto en la empresa.

En los apartados que siguen se describen con mayor detalle las fases de la evaluación de riesgos.

4.3.1 Fase 1 – Selección del perfil de riesgos

Durante esta fase, los equipos evalúan su perfil de riesgos empresarial mediante la utilización de un conjunto predefinido de criterios cualitativos**. Sirviéndose de la tabla de evaluación del perfil de riesgos (Tabla 2: Tabla de evaluación del perfil de riesgos**
), los equipos de evaluación pueden identificar su contexto desde el punto de vista de los riesgos. El contexto de riesgo se deriva de la actividad empresarial y del entorno exterior de la organización, y

puede dividirse en **cuatro áreas de riesgos**: **riesgos jurídicos, riesgos para la reputación y de pérdida de confianza de los clientes, riesgos de productividad, y riesgos para la estabilidad financiera.**

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La organización maneja información relativa a los clientes de carácter sensible y personal, incluidas historias médicas y datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE.	La organización maneja información de los clientes de carácter personal, pero no sensible, con arreglo a lo dispuesto en la legislación de protección de datos de la UE.	La organización no maneja datos personales distintos a los del personal empleado.
Riesgos de productividad	La organización emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.	La organización emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.	La organización emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.
Riesgos para la estabilidad financiera	Los ingresos anuales de la organización exceden de 25 millones de euros y/o se producen transacciones financieras con terceros o clientes como proceso habitual dentro de la actividad empresarial.	Los ingresos anuales de la organización no exceden de 25 millones de euros.	Los ingresos anuales de la organización no exceden de 5 millones de euros.
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en la actividad de la organización, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en la actividad de la organización, y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en la actividad de la organización, ni derivar en pérdida de ingresos.

Tabla 2: Tabla de evaluación del perfil de riesgos

Cada área se clasifica en tres clases: alta, media y baja. Estas clases obedecen a criterios cuantitativos de la organización en cuestión respecto al área de riesgo, y ayudan a determinar el nivel de riesgo. El equipo evalúa los riesgos identificados para cada área, con el fin de elaborar el **perfil de riesgos de la organización**.

Como norma general, el mayor riesgo identificado en una determinada clase define el perfil general de riesgos de la actividad. Un nivel alto en la clase de riesgos financieros da lugar a un perfil de riesgos alto. Del mismo modo, un nivel medio da lugar a un perfil medio, y un nivel bajo, a un perfil de riesgos bajo. Por ejemplo, un nivel bajo en las áreas de los riesgos para la reputación y la confianza, los riesgos jurídicos y los riesgos de productividad, pero alto en lo que se refiere a los riesgos para la estabilidad financiera, da lugar finalmente a un perfil de riesgos alto de la organización.

La determinación del perfil de riesgos debe considerarse como una decisión muy importante que da lugar posteriormente a la selección de activos relacionada con el riesgo y a su protección mediante tarjetas de controles.

4.3.2 Fase 2 – Identificación de los activos críticos

Durante esta fase, el equipo de evaluación selecciona los activos críticos basándose en la importancia relativa para la organización, y define los requisitos de seguridad para cada uno de tales activos.

Habitualmente, los directivos de una organización saben cuáles son sus **activos fundamentales** y pueden utilizar sus recursos limitados para hacer hincapié en la protección de los mismos. El equipo de evaluación determina lo que es importante para la organización (p. ej., los activos relacionados con la información) y selecciona los activos más significativos para la misma, a los que se conoce asimismo como **activos críticos**.

En la tabla que sigue se definen las categorías de activos y los tipos que se consideran durante la selección de activos críticos. Se presta atención a los activos utilizados para facilitar a la organización el ejercicio de su actividad. Cabe señalar que los tipos de activos pueden comprender otros tipos de activo adicionales. Por ejemplo, los componentes de una aplicación pueden consistir en servidores, terminales, enrutadores, segmentos de red, etc.

Cabe indicar que la lista que sigue es representativa de la mayoría de las pequeñas empresas, y que no es exhaustiva. Previa petición al respecto (p. ej., en futuras versiones del presente documento), podrán introducirse activos adicionales. Asimismo, es posible que un tipo de activo pueda utilizar otros activos para sus operaciones. Por ejemplo, una aplicación puede utilizar como componentes, un servidor, varios terminales, un dispositivo de almacenamiento y un segmento de red. Ha de tenerse en cuenta que, además de proteger al activo, han de salvaguardarse debidamente también cada uno de sus componentes.

Categoría de activo	Descripción	Activo (tipos)
Sistemas	Sistemas que tratan y almacenan información. Son una combinación de información, programas informáticos y activos de hardware. Todo equipo anfitrión, cliente, servidor o red puede considerarse un sistema. Los sistemas críticos son los identificados como tales para la prestación continua de las ofertas de servicios y productos empresariales, los que almacenan información empresarial esencial (de clientes o propiedad de la empresa), o los que se exponen al mundo exterior para la prestación de servicios o funciones empresariales.	Servidor Ordenador personal Terminal Archivos y copias de respaldo Almacenamiento
Red	Dispositivos importantes para las redes de la organización. Enrutadores, conmutadores y módem son ejemplos de este tipo de componentes. Los componentes o dispositivos inalámbricos, como los teléfonos móviles y los puntos de acceso inalámbricos que utilizan los miembros de la plantilla para acceder a la información (p. ej., el correo electrónico). Normalmente, las redes fundamentales son las utilizadas para sostener aplicaciones o sistemas críticos esenciales, o las que se comparten con terceros y, habitualmente, con redes no comprobadas.	Enrutadores Cableado Puertas de acceso (*gateways*) Puntos de acceso inalámbricos Segmento de red (p. ej., cableado y equipos entre dos ordenadores) Otros (SAT, láser)
Personas	Personas de la organización, incluidas sus destrezas, formación, conocimientos y experiencia. El personal crítico es aquél que desempeña un papel crucial en los procesos de producción u operativos. Debe otorgarse importancia a los recursos esenciales (humanos) que se consideran irremplazables o constituyen un punto único de fallo.	Gestión empresarial y de recursos humanos Operaciones y tecnología Investigación y desarrollo Ventas y marketing Contratistas y terceros
Aplicaciones	Aquéllas que son clave para las ofertas de productos y servicios, o que forman parte de éstas. La perturbación de aplicaciones críticas entorperce gravemente, o incluso congestiona, los procesos dependientes.	Control financiero Atención al cliente Logística Comercio electrónico ERP

Tabla 3: Lista de activos

Resulta esencial durante la identificación considerar las opiniones de la alta dirección (o de los propietarios de la empresa). La participación de altos directivos en el análisis garantiza que se identifique debidamente el valor para el negocio de los activos de información empresarial.

A continuación, es necesaria una evaluación de los requisitos de seguridad relativos a los activos de mayor importancia. En los requisitos de seguridad se esbozan las cualidades de un activo que resulta importante proteger. A continuación se refieren los requisitos de seguridad examinados durante el proceso de evaluación:

- confidencialidad – la necesidad de mantener la información propia, sensible o personal en condiciones de confidencialidad e inaccesibilidad para todo aquél que no esté autorizado para acceder a la misma;
- integridad – autenticidad, precisión y exhaustividad de un activo;
- disponibilidad – la propiedad de un activo que debe estar disponible en el momento de su utilización.

Los equipos de evaluación deben utilizar los criterios de selección de requisitos consignados en la tabla 4, con el fin de determinar los requisitos de seguridad más importantes respecto a las distintas categorías de activos. Los requisitos de seguridad de los activos se emplearán posteriormente, durante la selección de las tarjetas de controles. La selección de los requisitos de seguridad se ha elaborado a modo de guía sencilla y práctica para identificar las propiedades de seguridad de los activos críticos elegidos previamente. Los requisitos ponen de relieve la importancia del activo y son indicadores del nivel de protección que se necesita (p. ej., mediante el uso de controles apropiados):

La tabla que sigue ayudará a los equipos de evaluación a determinar los requisitos de seguridad para las distintas categorías de activos antes mencionadas.

Categoría de activo	Confidencialidad	Integridad	Disponibilidad
Sistemas	Un sistema con requisitos de confidencialidad gestiona a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a los clientes de carácter médico o personal.	Los sistemas con requisitos de integridad suelen gestionar transacciones de índole financiera, adquisiciones de bienes u operaciones de comercio electrónico.	Los requisitos de disponibilidad se dan en sistemas que resultan críticos para las operaciones empresariales ordinarias, y en los casos en que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.
Red	Una red con requisitos de confidencialidad suele cubrir las comunicaciones y el intercambio de información en entornos inseguros o sin comprobar.	Los requisitos de integridad de las redes son necesarios habitualmente cuando se realizan transacciones a través de redes metropolitanas públicas y compartidas o proveedores de telecomunicaciones.	Los requisitos de disponibilidad son especialmente necesarios cuando la red se utiliza como parte de la atención al cliente, o de ofertas de servicios o productos.
Personas	Los requisitos de confidencialidad suelen darse cuando determinadas personas gestionan información confidencial y propiedad de la organización que, si se divulga, puede perjudicar la reputación de la marca de la organización y a su base de clientes.	Los requisitos de integridad en lo que atañe a personas se refieren a secretos compartidos como claves criptográficas o contraseñas. La posesión de tal conocimiento introduce amenazas vinculadas al factor humano que deben abordarse con los controles respectivos.	Los requisitos de disponibilidad respecto a los activos de personal revisten especial importancia cuando dicho personal es un recurso crítico para las operaciones continuas de las ofertas de productos o servicios.
Aplicaciones	Las aplicaciones con requisitos de confidencialidad gestionan a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a	Las aplicaciones con requisitos de integridad suelen gestionar transacciones de índole financiera, la adquisición de bienes o las operaciones de comercio electrónico.	Los requisitos de disponibilidad se dan en aplicaciones que resultan fundamentales para las operaciones empresariales ordinarias, y en los casos en

	los clientes de carácter médico o personal.		que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.

Tabla 4: Cuadro de selección de los requisitos de seguridad

Como resultado de este proceso, los equipos de evaluación deben disponer de un cuadro de activos críticos clasificados por categorías, y una relación de los requisitos de seguridad correspondientes, junto con la información justificativa o de apoyo considerada durante la evaluación.

Este resultado se utilizará posteriormente como elemento de partida en la fase 3 – Selección de las tarjetas de controles, como se indica en el siguiente capítulo.

4.3.3. Fase 3 – Selección de las tarjetas de controles

En la fase 3, el equipo de evaluación selecciona los controles apropiados sobre la base del perfil de riesgos elegido para cada categoría de riesgo y la lista de los activos críticos identificados (incluidos sus requisitos). Los controles se dividen en dos categorías: organizativos y basados en los activos.

Se supone que la organización en su conjunto constituye un único activo que ha de protegerse. Los controles de seguridad de las organizaciones suelen ser generales y se aplican a la organización de activos de un modo horizontal. Por el contrario, los controles basados en los activos se dirigen a la ejecución de la protección que requieren éstos (p. ej., conseguir la disponibilidad de un componente crítico de la red).

Los controles se agrupan asimismo en tarjetas de controles. Se dispone de dos tipos de tales tarjetas para su selección por los equipos que llevan a cabo la evaluación de una PYME:

- Tarjetas con controles aplicables a la organización horizontalmente, relativos a las prácticas y los procedimientos de gestión; y
- Tarjetas con controles aplicables a los activos críticos, específicos de cada categoría de éstos. Estas tarjetas prevén fundamentalmente una serie de controles preseleccionados agrupados con arreglo al perfil de riesgos y a los requisitos de seguridad de cada activo.

En la tabla 5 se refieren las categorías de controles, su estructura y su denominación según se consideran en el presente enfoque. Como se ha mencionado anteriormente, estos controles se han adoptado de OCTAVE. La decisión de utilizarlos se basó en su sencillez. Pueden utilizarse otros como alternativa (p. ej., ISO 17799, IT-Grundschutz, etc.). Una descripción más pormenorizada puede encontrarse en

Categoría de controles	Nº de control	Denominación del control
Organizativos	**SP1**	Formación y sensibilización en materia de seguridad
	SP2	Estrategia de seguridad
	SP3	Gestión de seguridad
	SP4	Políticas y normativas de seguridad
	SP5	Gestión de la seguridad en régimen de colaboración
	SP6	Planificación de contingencias/recuperación en caso de catástrofe
Basados en los activos	**OP1.1**	Planes y procedimientos de seguridad física
	OP1.2	Control de acceso físico
	OP1.3	Seguimiento y auditoría de la seguridad física

	OP2.1	Gestión de sistemas y redes
	OP2.2	Herramientas de administración de sistemas
	OP2.3	Seguimiento y auditoría de la seguridad física
	OP2.4	Autenticación y autorización
	OP2.5	Gestión de vulnerabilidades
	OP2.6	Codificación
	OP2.7	Diseño y arquitectura de seguridad
	OP3.1	Gestión de incidentes
	OP3.2	Prácticas de personal generales

Tabla 5: Controles utilizados en el enfoque presentado

En consecuencia, la fase 3 del enfoque de evaluación propuesto consta de dos pasos separados, pero igualmente importantes:

- Paso A: Selección de los controles organizativos;
- Paso B: Selección de los controles basados en los activos.

Durante estos pasos, se asignan controles a la organización (como un único activo importante) y a los activos críticos identificados, como se indica más adelante.

Selección de las tarjetas de controles organizativos

La selección de las tarjetas de controles organizativos se realiza de un modo bastante sencillo: se dispone de controles organizativos para cada perfil de riesgos (definido en la matriz de perfiles de riesgos). En la tabla que sigue se asignan controles organizativos a los perfiles de riesgos mencionados en el capítulo 4.3.1 Fase 1 – Selección del perfil de riesgos. Los controles que figuran más adelante se recomiendan para mitigar los respectivos riesgos organizativos. Se incluye una descripción pormenorizada de los controles en el Anexo C. Controles organizativos.

Áreas de riesgo	**Alto**	**Medio**	**Bajo**
Riesgos jurídicos	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Riesgos de productividad	(SP3) (SP4) (SP6) (SP5)	(SP4) (SP6)	SP4.1
Riesgos estabilidad financiera	(SP2) (SP1) (SP4)	(SP4)	SP4.1
Riesgos para la reputación y de pérdida de confianza de los clientes	(SP1) (SP5)	(SP4) (SP1)	SP4.1

Tabla 6: Tarjetas de controles organizativos

Selección de las tarjetas de controles basados en los activos

Sobre la base del perfil de riesgos y los requisitos de seguridad de los activos, los equipos de evaluación de las PYME pueden utilizar la tabla de tarjetas de controles basados en los activos (véase la tabla 7) para identificar los controles apropiados para la protección de los activos críticos.

Tarjetas de controles basados en los activos			
Activo	**Tarjetas para riesgo alto**	**Tarjetas para riesgo medio**	**Tarjetas para riesgo bajo**
Aplicación	**CC-1A**	**CC-2A**	**CC-3A**
Sistema	**CC-1S**	**CC-2S**	**CC-3S**
Red	**CC-1N**	**CC-2N**	**CC-3N**
Personal	**CC-1P**	**CC-2P**	**CC-3P**

Tabla 7: Tarjetas de controles basados en los activos

Las tarjetas de controles basados en los activos se agrupan esencialmente en tres categorías, correspondientes al perfil de riesgos, a la categoría de activos y a los requisitos de seguridad de la organización. Por ejemplo, una organización con un perfil de riesgos alto tendrá requisitos de seguridad diferentes de los que corresponden a otra con un perfil de riesgos medio o bajo. Cada tarjeta prevé varios controles basados en los activos (véase el

Anexo B. Tarjetas de controles basados en los activos) para abordar la gama completa de riesgos y requisitos de seguridad adecuados para cada perfil y en función de los requisitos de seguridad seleccionados. En el anexo D. Controles basados en los activos, se ofrece una descripción más detallada de los controles incluidos en las tarjetas.

A efectos de esta presentación, consignamos aquí la tarjeta de controles CC-1A. Como se indica en la tabla, esta tarjeta es apropiada para la protección de una aplicación en un contexto de riesgo elevado (perfil de riesgos alto).

Identificación de la tarjeta de controles basados en los activos	**CC-1A**									
Perfil de riesgo	**Alto**									
Categoría de activos	**Aplicación**									
Requisitos de seguridad	**Seguridad física**	**Gestión de sistemas y redes**	**Herramientas de administración de sistemas**	**Seguimiento y auditoría de la seguridad física**	**Autenticación y autorización**	**Gestión de vulnerabilidades**	**Codificación**	**Diseño y arquitectura de seguridad**	**Gestión de incidentes**	**Prácticas de personal generales**
Confidencialidad		2.1.3			2.4.2	2.5.1	2.6.1			
Integridad		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilidad		2.1.6								

Tabla 8: Ejemplo de tarjeta de controles para el activo "aplicación" con un perfil de riesgos alto

Los equipos de evaluación, utilizando los requisitos de seguridad previamente identificados y la tarjeta de controles, pueden determinar posteriormente controles más específicos (p. ej., los controles de disponibilidad, confidencialidad e integridad). Ha de tenerse en cuenta que, en los casos en que se selecciona más de un requisito, los controles que se aplican al activo son la suma de los correspondientes a cada requisito.

4.3.4 Fase 4 – Ejecución y gestión

En la fase 4, y sobre la base de la información evaluada, el equipo de evaluación formula planes de mitigación con el fin de abordar los riesgos que atañen a los activos críticos.

Una vez determinados (1) el perfil de riesgos de la organización, (2) los activos críticos, y (3) las tarjetas de controles, el equipo de evaluación planifica la ejecución de los controles seleccionados. Se prevé que, debido a sus recursos limitados, las PYME no podrán ejecutar todos los controles identificados respecto a la totalidad de los activos críticos de una sola vez. En este sentido, la asignación de prioridades es un elemento esencial para el éxito de las actividades de reducción de riesgos.

En los planes de ejecución se define el modo en que la organización se propone elevar o mantener el nivel de seguridad existente. Su objetivo es establecer directrices respecto a las iniciativas futuras en materia de seguridad de la información, más que encontrar una solución inmediata a toda vulnerabilidad y motivo de preocupación relacionados con la seguridad.

A continuación figuran ciertos criterios para la asignación de prioridades a las acciones de ejecución de las tarjetas de controles identificadas. No todos son aplicables en las distintas empresas. No obstante, pueden emplearse como guía genérica:

- **Coordinación estratégica con los objetivos de la organización**: ¿es este activo directamente compatible con los objetivos de los planes de trabajo de la organización o de la

división documentados? ¿Qué fines y objetivos de planes de trabajo se tendrán en cuenta y de qué manera?

- **Iniciativas de mejora continua**: ¿es compatible el activo con los esfuerzos de mejora continua de la división? ¿En qué consiste el activo de mejora continua? ¿Como contribuye este activo a la consecución de los fines de mejora continua?
- **Obligaciones jurídicas o normativas**: si un activo es necesario para satisfacer requisitos normativos, este hecho se reflejará al establecer prioridades.
- **Ventajas para todo el sistema**: entre las ventajas para el conjunto del sistema figura la mejora del servicio al cliente para diversos grupos de clientes. Se otorgará una mayor prioridad a los grupos de clientes que se consideran críticos, pero cuanto mayor sea el grupo de clientes en cuestión, mayor será el beneficio.
- **Ahorro de costes y de tiempo**: las estimaciones de ahorro de costes y de tiempo atañen al tiempo del personal y de los clientes, a la generación de ingresos y a las reducciones de costes y presupuestarias directas.
- **Reducción de riesgos**: como resultado del proyecto, la información y los servicios evitarán la pérdida de ingresos y el incumplimiento de políticas y requisitos jurídicos y de auditoría.

El siguiente paso corresponde al proceso de planificación, en el que se indica y supervisa el calendario exacto de ejecución de los procedimientos y herramientas de seguridad.

Una cuestión fundamental prácticamente en todas las ejecuciones es la de determinar si los recursos internos son adecuados y suficientes. En otras palabras, puede que resulte necesario adoptar una decisión sobre la internalización o la externalización de las tareas de ejecución y de gestión relacionadas.

5. Directrices de autoevaluación, con dos ejemplos

En el presente capítulo, se efectúa un desglose más detallado de las cuatro fases, divididas en pasos lógicos. Con ello se pretende ayudar a las PYME a (1) determinar el perfil de riesgos de su organización, (2) identificar los activos críticos que han de salvaguardarse, (3) seleccionar controles y soluciones para la mejora de la seguridad y, finalmente, (4) formular planes de mejora. No obstante, las acciones y soluciones que pueden aplicarse a las PYME no se limitan a las que se refieren en el presente documento.

De nuevo en este caso, se anima encarecidamente a las organizaciones a aplicar las directrices y las buenas prácticas incluidas en este método únicamente a modo de plan a corto plazo, y para satisfacer el objetivo de proteger con rapidez y eficacia los componentes críticos de su actividad empresarial. En cualquier caso, el proceso no sustituye a un enfoque de evaluación de riesgos completa y exhaustiva, que se recomienda decididamente como base de una estrategia de gestión de riesgos a largo plazo.

Antes de tratar de utilizar el método, las PYME han de comprender los tres aspectos singulares del mismo que se refieren a continuación:

- Un pequeño equipo interdisciplinar compuesto por tres a cinco personas lidera el proceso de evaluación de riesgos. En conjunto, los miembros del equipo de análisis deben contar con un amplio conocimiento de los procesos empresariales y de seguridad de la organización, suficientes para llevar a cabo todas las actividades RA. Por esta razón, el método no exige seminarios formales de recogida de datos para poner en marcha la evaluación.
- El método comprende una exploración limitada de la infraestructura informática. Puesto que las organizaciones pequeñas externalizan con frecuencia sus servicios y funciones relacionados con las TI, no suelen haber desarrollado capacidades organizativas para aplicar herramientas de evaluación de la vulnerabilidad, ni para interpretar sus resultados. No obstante, la falta de una capacidad organizativa para utilizar tales herramientas no impide a las organizaciones el establecimiento de una estrategia de protección.
- Más que utilizar los datos sobre vulnerabilidad para perfeccionar su visión de sus prácticas de seguridad vigentes, una organización que realiza una evaluación examina los procesos empleados para configurar de manera segura y mantener su infraestructura informática.

El documento se estructura en fases y pasos como elementos constitutivos básicos. Se plantean dos ejemplos por cada fase. En los ejemplos se utilizan los siguientes supuestos empresariales:

- **Empresa del ejemplo A**. En el ejemplo A, consideramos el caso especial de una empresa mediana de asistencia médica en línea que presta asistencia médica en la red a médicos que requieren asesoramiento para sus pacientes e información sobre avances recientes en el ámbito de la medicina. La base de datos que sostiene la aplicación almacena datos críticos y confidenciales de índole personal. La empresa emplea a 100 personas y cuenta con tres departamentos, el departamento médico y de asistencia médica, el departamento científico y el de gestión, que realiza actividades relativas a los recursos humanos y el control financiero.
- **Empresa del ejemplo B.** La empresa del ejemplo B es un bufete de abogados de dimensión reducida. En este caso, los sistemas de TI se utilizan ampliamente para almacenar información sobre los casos, intercambiar mensajes de correo electrónico y preparar y tramitar los documentos necesarios. La empresa emplea a cinco abogados y una secretaria.

Se ofrecen asimismo las cifras (diagramas de flujo de trabajo) para cada una de las fases; se dan consejos de ejecución para cada paso en los recuadros de puntos de cada una de las descripciones de fases siguientes.

Fase 1 – Selección del perfil de riesgos

El equipo de análisis considera los aspectos de la protección de la información relacionados con los riesgos empresariales que pueden (a) afectar directa o indirectamente o perjudicar la reputación y la confianza de los clientes, (b) dar lugar a infracciones de la legislación, (c) generar pérdidas económicas, y (d) reducir la productividad. A continuación, selecciona un nivel de riesgos apropiado para cada una de estas áreas de riesgo, aplicando el cuadro de evaluación del perfil de riesgos. Las áreas especificadas son las siguientes: riesgos jurídicos, riesgos de productividad, riesgos para la estabilidad financiera, y riesgos para la reputación y de pérdida de confianza de los clientes. Como se muestra en la figura 3, la fase comprende dos pasos.

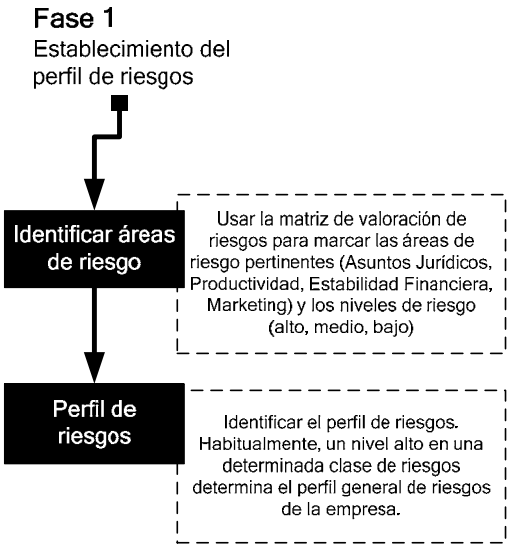

Figura 3: Fase 1 – Diagrama de flujo de la selección del perfil de riesgos

Para determinar el nivel de riesgos real o posible, los miembros del equipo de análisis deben destacar el área de riesgo y leer la descripción que figura en cada columna. Se eligen las áreas de riesgo más cercanas a su perfil empresarial. El proceso se realiza respecto a cada una de las áreas de riesgo. Al final, debe obtenerse una MATRIZ en la que se muestra el nivel de riesgo aplicable en cada una de las áreas de riesgo.

Ejemplo A. (Perfil de riesgos alto)

En el ejemplo A, el equipo utiliza el **cuadro de evaluación del perfil de riesgos** para determinar el contexto de riesgo de la empresa. En este sentido, el equipo establece un nivel de riesgos alto (marcado con color rojo) en el área de los riesgos jurídicos, puesto que la empresa maneja información de índole sensible y personal. Al mismo tiempo, observa un nivel alto en el área de riesgos de productividad, puesto que emplea a 100 personas, un nivel medio (marcado en naranja) en el área de riesgos para la estabilidad financiera, y un nivel bajo (marcado en azul) en el área de riesgos para la reputación y de pérdida de confianza de los clientes, como se muestra en el siguiente cuadro de evaluación del perfil de riesgos.

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	**La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y**	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define	La empresa no maneja datos personales distintos a los del personal empleado por ella.

	datos personales críticos, con arreglo a lo previsto en la legislación de protección de datos de la UE.	ésta en la Ley de protección de datos de la UE.	
Riesgos de productividad	**La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.**	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.	La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial.	**Los ingresos anuales no exceden de 25 millones de euros.**	Los ingresos anuales no exceden de 5 millones de euros.
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial, y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.	La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial , y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.	**La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial , ni derivar en pérdida de ingresos.**

Tabla 9: Cuadro de evaluación del perfil de riesgos – Ejemplo A

A continuación, se estima el perfil de riesgos de la empresa. Las áreas de riesgo constituyen conjuntamente el contexto de riesgo de la empresa. **Se recomienda que el perfil de riesgos equivalga al nivel más alto identificado en las áreas de riesgo subordinadas en la matriz de riesgos.**

En la tabla que figura a continuación se ilustran los niveles de riesgo identificados en las áreas de riesgo predefinidas, y se muestra en qué ámbito debe centrar su esfuerzo la organización para aplicar los controles de seguridad pertinentes. El cuadro puede utilizarse asimismo para establecer prioridades. Los niveles de riesgo altos indican una necesidad urgente de mejora, mientras que los niveles de riesgo bajos ponen de relieve acciones que deben tenerse en consideración para futuras mejoras.

Áreas de riesgo	Nivel de riesgo	Perfil de riesgo
Riesgos jurídicos	**Alto**	**Alto**
Riesgos de productividad	**Alto**	
Riesgos para la estabilidad financiera	**Medio**	
Riesgos para la reputación y de pérdida de confianza de los clientes	**Bajo**	

Tabla 10: Perfil de riesgos de la organización – Ejemplo A

Ejemplo B. (Perfil de riesgos medio)

En el ejemplo B, el equipo utiliza el **cuadro de evaluación del perfil de riesgos** para determinar el contexto de riesgos de la empresa. El equipo de análisis procede identificando un nivel de riesgos bajo (marcado con color azul) en el área de riesgos jurídicos, dado que la empresa no maneja datos personales aparte de los empleados de la organización, un nivel igualmente bajo en el área de riesgos de productividad (marcado en azul), un nivel bajo (marcado en azul) en el área de riesgos para la estabilidad financiera, y un nivel medio (marcado en naranja) en el área de riesgos para la reputación y de pérdida de confianza de los clientes, como se muestra en el siguiente cuadro de evaluación del perfil de riesgos.

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	La empresa maneja información de los clientes de carácter sensible y personal, incluidas historias médicas y datos personales esenciales, con arreglo a lo previsto en la legislación de protección de datos de la UE.	La empresa maneja la información de los clientes de índole personal, pero no sensible, conforme se define ésta en la Ley de protección de datos de la UE.	**La empresa no maneja datos personales distintos a los del personal empleado por ella.**
Riesgos de productividad	La empresa emplea a más de 100 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.	La empresa emplea a más de 50 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.	**La empresa emplea a menos de 10 personas que requieren a diario del acceso a aplicaciones y servicios empresariales.**
Riesgos para la estabilidad financiera	Los ingresos anuales exceden de 25 millones de euros y/o las transacciones financieras con terceros o clientes tienen lugar como proceso habitual parte de su actividad empresarial.	Los ingresos anuales no exceden de 25 millones de euros.	**Los ingresos anuales no exceden de 5 millones de euros.**
Riesgos para la reputación y de pérdida de confianza de los clientes	La indisponibilidad o la calidad del servicio repercuten directamente en el perfil empresarial , y/o más del 70% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.	**La indisponibilidad o la calidad del servicio pueden repercutir indirectamente en el perfil empresarial , y/o menos del 5% de la base de clientes dispone de acceso en línea a los productos y servicios de la empresa.**	La indisponibilidad o la calidad del servicio no pueden repercutir de manera directa o indirecta en el perfil empresarial , ni derivar en pérdida de ingresos.

Tabla 11: Cuadro de evaluación del perfil de riesgos – Ejemplo B

A continuación, se estima el perfil de riesgos de la empresa. Las áreas de riesgo constituyen conjuntamente el contexto de riesgo de la empresa. **Se recomienda que el perfil de riesgos equivalga al nivel más alto identificado en las áreas de riesgo subordinadas en la matriz de riesgos.**

En la tabla que figura a continuación se ilustran los niveles de riesgo identificados en las áreas de riesgo predefinidas, y se muestra en qué ámbito debe centrar su esfuerzo la organización para aplicar los controles de seguridad pertinentes. El cuadro puede utilizarse asimismo para establecer prioridades. Los niveles de riesgos altos indican una necesidad urgente de mejora, mientras que los niveles de riesgos bajos pueden considerarse como un aviso en materia de seguridad que debe tenerse en cuenta para futuras mejoras.

Áreas de riesgo	Nivel de riesgo	Perfil de riesgo
Riesgos jurídicos	**Bajo**	**Medio**
Riesgos de productividad	**Bajo**	
Riesgos para la estabilidad financiera	**Bajo**	
Riesgos para la reputación y de pérdida de confianza de los clientes	**Medio**	

Tabla 12: Perfil de riesgos de la organización – Ejemplo B

Fase 2 – Identificación de activos críticos

La fase 2 requiere decisiones que conformen el resto de la evaluación: la selección de los activos críticos de la organización. Dependiendo del tamaño de la organización, el número de activos de información identificados durante esta fase podrá exceder fácilmente de un centenar. Para que el análisis resulte viable, las PYME han de restringir el ámbito de la evaluación mediante la selección de los pocos activos críticos para la consecución de la misión y de los objetivos empresariales de la organización. Se trata de los únicos activos que se analizarán en actividades posteriores. Como se muestra en la figura 4, la fase comprende tres pasos.

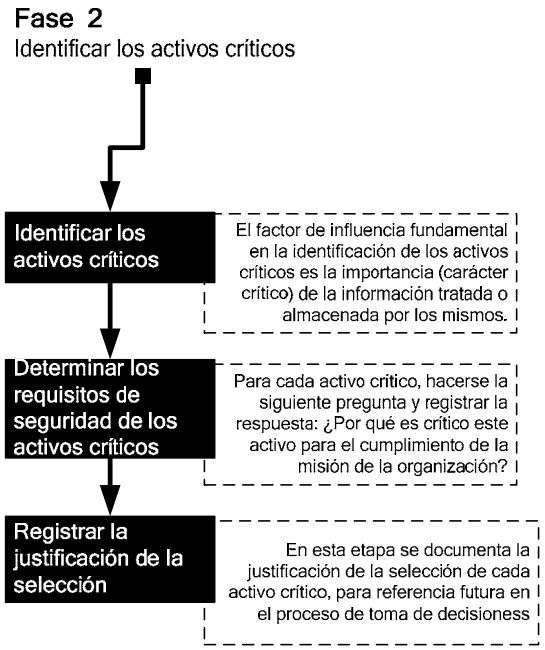

Figura 4: Fase 2 – Diagrama de flujo de la identificación de los activos críticos

Paso 1. Seleccionar los cinco activos críticos de su organización

Cuando se seleccionan activos críticos, no hay por qué limitarse a cinco. Cinco activos son suficientes normalmente para elaborar un conjunto adecuado de planes de reducción en la fase 4. No obstante, los miembros del equipo de análisis deben aplicar su criterio para determinar si se consideran más o menos de cinco. Durante este proceso de selección, los miembros del equipo deben considerar qué activos tendrán un efecto perjudicial significativo en la organización en alguno de los supuestos que siguen:

- **Revelación** de información a personal no autorizado;
- **Modificación** de la información sin autorización;
- **Pérdida o destrucción** del activo;
- **Acceso interrumpido** al activo o a la información almacenada.

En los casos en los que resulta difícil identificar los activos críticos, los equipos deben considerar las distintas funciones y áreas de negocio en la organización. Puede tratarse de diversos proyectos, grupos de trabajo (grupos de personas con descripciones de puesto diferentes), o incluso departamentos organizativos específicos (Departamento de RRHH, Contable, de Marketing, de Ventas, y otros). Estos activos deben consignarse por niveles de importancia para el proceso empresarial. Después de definir las áreas que deben asegurarse, o de reorganizar los activos de la organización, el paso siguiente consiste en elaborar una lista de los activos con arreglo a su repercusión en el proceso empresarial. Una forma más viable de acometer esta tarea consiste en agrupar los activos por departamento o función de la organización.

Un factor de influencia fundamental en la identificación de los activos críticos es la importancia (carácter crítico) de la información tratada o almacenada por los mismos. Mediante el análisis de descomposición, los miembros del equipo pueden identificar fácilmente dónde y cómo se almacena o utiliza la información crítica.

Paso 2. Registrar la justificación de la selección de cada activo crítico

Al seleccionar los activos críticos en el paso 1, se consideran varias cuestiones relacionadas con ellos. En el presente paso, la justificación de esa selección se documenta para su futura consulta en el proceso de toma decisiones. Además, el conocimiento de las razones por las que un activo se estima crítico puede facilitar la definición de los requisitos de seguridad en el siguiente paso. Para cada activo crítico hay que hacer las siguientes preguntas, y registrar las respuestas correspondientes:

- ¿Por qué es el activo crítico para el cumplimento de la misión de la organización?
- ¿Quién lo controla?
- ¿Quién es el responsable del mismo?
- ¿Quién lo utiliza?
- ¿Cómo se utiliza?

Estas preguntas se centran en el modo en que se utilizan los activos y las razones por las que revisten importancia. Si no se da respuesta a todas ellas, debe localizarse a los miembros de la organización que puedan hacerlo e incluirles en el equipo de análisis. La información resultante de la respuesta a tales preguntas resultará de utilidad en una fase posterior del proceso. En este sentido, la información recabada aquí debe registrarse con cuidado.

Paso 3. Determinar los requisitos de seguridad de los activos críticos

En general, al describir un requisito de seguridad respecto a un activo, es necesario comprender qué aspecto del mismo reviste importancia. En el caso de los activos de información, los requisitos de seguridad se centrarán en la confidencialidad, la integridad y la disponibilidad de la información.

Los requisitos de seguridad pueden variar para diferentes categorías de activos en una PYME, pero la selección detenida de los requisitos es fundamental para la tarea de seleccionar los controles que sigue. En otras palabras, los requisitos de alta disponibilidad dan lugar a la imposición de controles de alta disponibilidad, etc.

Los equipos de análisis utilizan los **criterios de selección de requisitos** para determinar los requisitos de seguridad más relevantes. **Los requisitos de seguridad de los activos se emplearán posteriormente, durante la selección de las tarjetas de controles basados en los mismos.** Los criterios de evaluación de los requisitos de seguridad se han elaborado a modo de guía sencilla y práctica para evaluar dichos requisitos en lo que se refiere a la confidencialidad, la integridad y la disponibilidad de los activos críticos seleccionados. La evaluación pone de relieve la importancia de las características de seguridad de los activos e indica los controles apropiados para su protección.

Como resultado, los equipos de análisis deben obtener **un cuadro en el que figuren los activos críticos, junto con una breve descripción de su importancia para la consecución de la misión empresarial, sus elementos básicos y los requisitos de seguridad**.

Para los tres pasos examinados, las tablas del apartado 4.3.2 pueden utilizarse para identificar los activos relevantes y sus requisitos (véase la Tabla 3: Lista de activos y la Tabla 4: Cuadro de selección de los requisitos de seguridad

).

Ejemplo A. (Perfil de riesgo: alto, activo crítico: aplicación – fase 2.)

[Paso 1] En el ejemplo A, se identifica como primer activo crítico la aplicación *web* que presta asistencia en línea a los clientes: los médicos. Esta aplicación resulta esencial para la empresa, ya

que representa el elemento más importante de la oferta de servicio y, por tanto, se selecciona como el activo más crítico.

[Paso 2] En el siguiente paso, los miembros del equipo documentan los elementos que constituyen el activo y la justificación de su selección. De este modo, identifican finalmente la base de datos que almacena la información de los clientes, el segmento de red que sostiene la conectividad con redes internas y externas, el servidor *web* y los cortafuegos o *firewalls* como componentes esenciales del activo.

[Paso 3] A continuación, se determinan los requisitos de seguridad. Mediante el uso de la tabla que sigue (Tabla 13: Cuadro de selección de los requisitos de seguridad – Ejemplo A

), los equipos reconocen las celdas que corresponden a sus requisitos. En el ejemplo A, el equipo selecciona respecto a la base de datos los requisitos de confidencialidad, puesto que los datos almacenados atañen a los clientes de la empresa, y respecto a la red, los requisitos de disponibilidad y confidencialidad, dado que la red transmite información que debe permanecer intacta y secreta para la culminación de las transacciones o las consultas.

Activos	Confidencialidad	Integridad	Disponibilidad
Sistemas	Un sistema con requisitos de confidencialidad gestiona a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a los clientes de carácter médico o personal.	Un sistema con requisitos de integridad suele gestionar transacciones de índole financiera, la adquisición de bienes o las operaciones de comercio electrónico.	Los requisitos de disponibilidad se dan en sistemas que resultan críticos para las operaciones empresariales ordinarias, y en los casos en que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.
Red	Una red con requisitos de confidencialidad suele cubrir las comunicaciones y el intercambio de información en entornos inseguros o sin comprobar.	Los requisitos de integridad de las redes son necesarios habitualmente cuando se realizan transacciones a través de redes metropolitanas públicas y compartidas o proveedores de telecomunicaciones.	Los requisitos de disponibilidad son especialmente necesarios cuando la red se utiliza como parte de la atención al cliente, o de ofertas de servicios o productos.
Personal	Los requisitos de confidencialidad suelen darse cuando determinadas personas gestionan información confidencial y propiedad de la organización que, si se divulga, puede perjudicar la reputación de la marca de la organización y a su base de clientes.	Los requisitos de integridad en lo que atañe a personas se refieren a secretos compartidos como claves criptográficas o contraseñas. La posesión de tal conocimiento introduce amenazas vinculadas al factor humano que deben abordarse con los controles respectivos.	Los requisitos de disponibilidad respecto a los activos de personal revisten especial importancia cuando dicho personal es un recurso crítico para la continuidad de las ofertas de productos o servicios.
Aplicaciones	**Las aplicaciones con requisitos de confidencialidad gestionan a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a los clientes de carácter médico o personal.**	**Las aplicaciones con requisitos de integridad suelen gestionar transacciones de índole financiera, la adquisición de bienes o las operaciones de comercio electrónico.**	**Los requisitos de disponibilidad se dan en aplicaciones que resultan críticas para las operaciones empresariales ordinarias, y en los casos en que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.**

Tabla 13: Cuadro de selección de los requisitos de seguridad – Ejemplo A

Como resultado, los equipos de análisis documentan una tabla en la que figuran los activos críticos junto con la justificación de su selección, sus elementos básicos y los requisitos de

seguridad de los servicios prestados. La tabla que sigue es el resultado del ejemplo A para la fase 1 (véase la Tabla 14: Justificación de los requisitos de seguridad
).

Activo crítico	Categoría de activo	Componentes	Requisitos de seguridad	Justificación de su selección
Aplicación de comercio electrónico	Aplicación	Base de datos Cortafuegos Segmento de red Servidor	**Confidencialidad** **Integridad** **Disponibilidad**	La aplicación es esencial para la empresa, ya que constituye el elemento más importante de su oferta de servicios.

Tabla 14: Justificación de los requisitos de seguridad

Ejemplo B. (Perfil de riesgo: medio, activo crítico: sistema – fase 2.)

[Paso 1] En el ejemplo B, se determinan como activo más crítico los terminales utilizados para la realización de actividades ordinarias como la correspondencia con clientes, la información de clientes relativa a los distintos casos, y la información contable básica relativa a la facturación y las cuentas por cobrar.

[Paso 2] En el siguiente paso, los miembros del equipo documentan los elementos que constituyen el activo y la justificación de su selección. De este modo, identifican cuatro terminales, la red interna y el servidor de archivos.

[Paso 3] A continuación, se determinan los requisitos de seguridad. Mediante el uso de la tabla que sigue, los equipos reconocen las celdas de la misma que corresponden a sus requisitos. En el ejemplo B, el equipo selecciona los terminales con requisitos de disponibilidad como los que se utilizan para actividades empresariales ordinarias y, por tanto, debe mantenerse operativos.

Activos críticos	Confidencialidad	Integridad	Disponibilidad
Sistemas	Un sistema con requisitos de confidencialidad gestiona a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a los clientes de carácter médico o personal.	Un sistema con requisitos de integridad suele gestionar transacciones de índole financiera, la adquisición de bienes o las operaciones de comercio electrónico.	**Los requisitos de disponibilidad se dan en sistemas que resultan fundamentales para las operaciones empresariales ordinarias, y en los casos en que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.**
Red	Una red con requisitos de confidencialidad suele cubrir las comunicaciones y el intercambio de información en entornos inseguros o sin comprobar.	Los requisitos de integridad de las redes son necesarios habitualmente cuando se realizan transacciones a través de redes metropolitanas públicas y compartidas o proveedores de telecomunicaciones.	Los requisitos de disponibilidad son especialmente necesarios cuando la red se utiliza como parte de la atención al cliente, o de ofertas de servicios o productos.
Personal	Los requisitos de confidencialidad suelen darse cuando determinadas personas gestionan información confidencial y propiedad de la organización que, si se divulga, puede	Los requisitos de integridad en lo que atañe a personas se refieren a secretos compartidos como claves criptográficas o contraseñas. La posesión de tal conocimiento introduce	Los requisitos de disponibilidad respecto a los activos de personal revisten especial importancia cuando dicho personal es un recurso crítico para las operaciones continuas de las ofertas de

	perjudicar la reputación de la marca de la organización y a su base de clientes.	amenazas vinculadas al factor humano que deben abordarse con los controles respectivos.	productos o servicios.
Aplicaciones	Las aplicaciones con requisitos de confidencialidad gestionan a menudo datos con información reservada (I+D), información relativa a la base de clientes e información sensible relativa a los clientes de carácter médico o personal.	Las aplicaciones con requisitos de integridad suele gestionar transacciones de índole financiera, la adquisición de bienes o las operaciones de comercio electrónico.	Los requisitos de disponibilidad se dan en aplicaciones que resultan fundamentales para las operaciones empresariales ordinarias, y en los casos en que los períodos de inactividad suelen dar lugar a que se incurra en costes y gastos generales en términos de la asignación de recursos.

Tabla 15: Cuadro de selección de los requisitos de seguridad – Ejemplo B

Como resultado, los equipos de análisis documentan una tabla en la que figuran los activos críticos junto con la justificación su selección, sus elementos básicos y los requisitos de seguridad de los servicios prestados. La tabla que sigue es el resultado del ejemplo B del paso 3 (véase la Tabla 16: Justificación de los requisitos de seguridad

).

Activo crítico	Tipo de activo	Componentes	Requisitos de seguridad	Justificación de su selección
Terminales	**Sistema**	**4 terminales** **Segmento de red** **Servidor**	**Disponibilidad**	**Los terminales son importantes para el ejercicio de actividad diarias, incluidas la correspondencia con clientes, la información de clientes relativa a los casos, y la información contable básica respecto a la facturación y las cuentas por cobrar**

Tabla 16: Justificación de los requisitos de seguridad

Fase 3 – Selección de las tarjetas de controles

En la fase 3, los miembros del equipo de análisis están en condiciones de elegir las tarjetas de controles asociadas a las áreas de riesgo aplicables previamente definidas (en la fase 1) y a la lista de activos críticos identificados. Como se muestra en la figura 5, la fase comprende tres pasos.

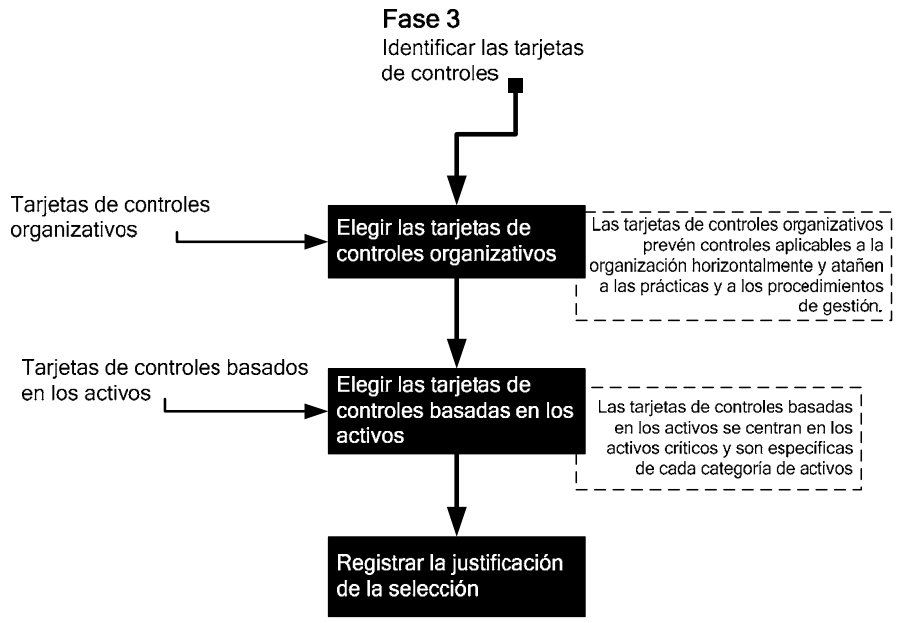

Figura 5: Fase 3 – Flujo de trabajo de la selección de las tarjetas de controles

Las tarjetas de controles prevén la realización de controles incluidos en el catálogo de prácticas utilizado en OCTAVE. Este catálogo comprende un conjunto de buenas prácticas estratégicas y de seguridad operativa. Una organización que lleva a cabo una evaluación de riesgos para la seguridad de la información se mide con arreglo a este catálogo de prácticas. El catálogo se utiliza como medida de lo que la organización hace bien actualmente en materia de seguridad (sus prácticas de seguridad vigentes), y lo que no (sus vulnerabilidades organizativas).

El catálogo de prácticas se divide deliberadamente en **dos tipos de controles**: **los organizativos y los basados en los activos**:

- Los **controles organizativos** hacen hincapié en los temas relativos a la formulación de políticas y aportan buenas prácticas generales en materia de gestión. Atañen a aspectos relacionados con la actividad empresarial, así como a los que requieren una planificación y una participación de toda la organización.
- Los **controles basados en los activos** hacen hincapié en los temas relacionados con la tecnología. Atañen a cuestiones relacionadas con el modo en que las personas utilizan y protegen ésta e interactúan con ella.

El catálogo de prácticas es de índole general; no es específico de ningún ámbito, organización o conjunto de normas. Puede modificarse para su adaptación a una determinada norma aplicable a la atención debida en un cierto ámbito, o a una normativa (p. ej., la comunidad médica y la normativa de seguridad de la legislación sobre portabilidad de los seguros de enfermedad). Asimismo, puede ampliarse para añadir normas específicas de la organización, o modificarse para reflejar la terminología de un determinado ámbito. **Además, puede sustituirse por cualquier lista de controles normalizados compatible.**

Los controles se agrupan además en tarjetas de controles separadas en dos categorías: la correspondiente a los controles organizativos y la correspondiente a los controles basados en los activos. Se dispone de dos tipos de tales tarjetas para su selección por los equipos de evaluación:

- **Tarjetas de controles organizativos,** que prevén controles aplicables a la organización horizontalmente y que atañen a las prácticas y a los procedimientos de gestión. Suelen ser de amplio alcance y con ellas se pretende mitigar los riesgos para la información habituales asociados al perfil de la organización.
- **Tarjetas de controles basados en los activos,** que se centran en los activos críticos y son específicas de cada categoría de activos. Prevén fundamentalmente controles preseleccionados agrupados con arreglo al perfil de riesgos y a los requisitos de seguridad de los activos. Como se ha mencionado anteriormente, los principales grupos de activos de las organizaciones son: información, sistema/red, personal y aplicaciones. Las tarjetas de controles basados en los activos se centran en tareas ordinarias y atienden a los riesgos específicos de los activos.

Una descripción detallada de los controles organizativos puede encontrarse en el Anexo C. Controles organizativos.

Paso 1. Seleccionar las tarjetas de controles organizativos

En este paso, los equipos de evaluación seleccionan las tarjetas de controles organizativos correspondientes a las áreas de riesgo identificadas en la fase 1 (determinación del perfil de riesgos) y, de este modo, definen la orientación de las iniciativas de seguridad de la información en la organización. No obstante, consideraciones prácticas impiden que las PYME ejecuten de inmediato todas las iniciativas tras la evaluación. Probablemente, las organizaciones dispondrán de fondos y recursos humanos limitados para ejecutar la estrategia de protección. Tras la evaluación, el equipo de análisis asigna prioridades a las actividades de dicha estrategia y, a continuación, se centra en la ejecución de aquellas a las que se ha asignado una mayor prioridad.

Los controles organizativos se encuentran disponibles para cada uno de los perfiles de riesgos definidos en la matriz en la que se recogen éstos.

Paso 2. Seleccionar las tarjetas de controles basados en los activos

Sobre la base del perfil de riesgos y los requisitos de seguridad de los activos, los equipos de análisis de las PYME pueden utilizar el cuadro de tarjetas de controles basados en los activos (véase el

Anexo B. Tarjetas de controles basados en los activos) para determinar los controles de este tipo pertinentes. Estas tarjetas prevén la realización de controles esenciales agrupados en tres categorías, correspondientes al perfil de riesgos organizativo, a la categoría de activos y a los requisitos de seguridad. Por ejemplo, una organización con un perfil de riesgos alto tendrá riesgos y requisitos de seguridad diferentes de los que corresponden a otra con un perfil medio o bajo. Del mismo modo, las tarjetas incluirán más controles para hacer frente a una gama más amplia de riesgos y requisitos de seguridad.

Paso 3. Documentar una lista de los controles seleccionados y su justificación

Al elegir las tarjetas de controles basados en los activos críticos en el paso 2, se abordan un gran número de cuestiones relacionadas con estos controles. En este paso hay que justificar la selección de cada tarjeta y las acciones necesarias para su ejecución. Por otra parte, la comprensión del mecanismo de las tarjetas de controles mejora la capacidad para definir los planes de acción en el siguiente paso. Respecto a cada tarjeta, considere y consigne su respuesta a la pregunta que sigue: ¿qué se requiere en términos de recursos y cambios para ejecutar los controles seleccionados? Examine los aspectos operativos de cada control. Considere las siguientes preguntas en relación con cada uno de ellos.

- ¿Quién debe ejecutarlo?
- ¿Quién debe asumir la responsabilidad al respecto?
- ¿Quién debe beneficiarse del mismo?
- ¿Cómo debe ejecutarse?

Estas preguntas se centran en el modo en que se utilizan los controles y las razones por las que revisten importancia. Si no puede responder a todas ellas, puede que necesite pedir la ayuda de las personas en su organización capaces de darles respuesta. La información que usted identifique mediante la contestación de estas preguntas resultará útil en la fase 4, al formular planes de mitigación. Asegúrese de registrar esta información.

Ejemplo A. (Perfil de riesgo: alto, activo crítico: aplicación)

[Paso 1] En el paso 1, los equipos de análisis que utilizan el **cuadro de evaluación del perfil de riesgos y el cuadro de controles organizativos (Tabla 17:** Selección de los controles organizativos - Ejemplo A

) seleccionan las tarjetas de controles organizativos para las áreas de riesgo identificadas en la fase 1 (perfil de riesgos), definiendo así la orientación de las iniciativas de la organización en materia de seguridad de la información.

En el ejemplo A, los controles organizativos previstos para un nivel de riesgos jurídicos alto son las prácticas de seguridad **SP1 y SP4**. Del mismo modo, un nivel alto en el área de los riesgos de productividad impone la necesidad de adoptar contramedidas y prácticas asociadas a los controles organizativos **SP3, SP4, SP5** y **SP6**. Al nivel medio de riesgos para la estabilidad financiera le corresponde SP4, y al nivel bajo de riesgos para la reputación y la confianza de los clientes, SP4.1 (sección incluida en los controles de SP4).

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	**(SP1)**	(SP1)	SP1.1
	(SP4)	(SP4)	
Riesgos de productividad	**(SP3)**	(SP4)	SP4.1
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Riesgos para la estabilidad financiera	(SP2)	**(SP4)**	SP4.1
	(SP1)		
	(SP4)		
Riesgos para la reputación y de pérdida de confianza de los clientes	(SP1)	(SP4)	**SP4.1**
	(SP5)	(SP1)	

Tabla 17: Selección de los controles organizativos - Ejemplo A

[Paso 2] En el paso 2, el equipo de análisis selecciona las tarjetas de control basado en activos utilizando la tabla de tarjetas de control basado en activos. En el ejemplo A, dado el perfil de riesgos alto de la organización identificado en la fase 1, y el tipo de activo crítico identificado en el paso 2, seleccionan la tarjeta 1 para aplicaciones de perfil de riesgos alto, en concreto, la tarjeta CC-1A.

Cuadro de tarjetas de control			
Activos críticos	**Tarjetas para riesgo alto**	**Tarjetas para riesgo medio**	**Tarjetas para riesgo bajo**
Aplicación	**CC-1A**	CC-2A	CC-3A
Sistema	CC-1S	CC-2S	CC-3S
Red	CC-1N	CC-2N	CC-3N
Personal	CC-1P	CC-2P	CC-3P

Tabla 18: Selección de los controles basados en los activos - Ejemplo A

La tarjeta seleccionada en el ejemplo A (véase el

Anexo B. Tarjetas de controles basados en los activos) muestra los controles necesarios para le ejecución de una aplicación en una organización con un determinado perfil de riesgos. El equipo identifica los controles que abordan los requisitos de seguridad identificados en la fase 3. En este ejemplo, se utilizan requisitos de confidencialidad y disponibilidad. Se seleccionan los siguientes controles de activos: **2.1.3, 2.1.6, 2.4.2, 2.5.1**, y **2.6.1**.

Identificación de la tarjeta de controles basados en los activos					**CC-1A**					
Perfil de riesgos					**Alto**					
Categoría de activos					**Aplicación**					
Requisitos de seguridad	**Seguridad física**	**Gestión de sistemas y redes**	**Herramientas de administración de sistemas**	**Seguimiento y auditoría de la seguridad física**	**Autenticación y autorización**	**Gestión de vulnerabilidades**	**Codificación**	**Diseño y arquitectura de seguridad**	**Gestión de incidentes**	**Prácticas de personal generales**
Confidencialidad		**2.1.3**			**2.4.2**	**2.5.1**	**2.6.1**			
Integridad		**2.1.4**			**2.4.2**	**2.5.1**	**2.6.1**			
Disponibilidad		**2.1.6**								

Tabla 19: Tarjeta de controles basados en los activos CC-1A - Ejemplo A

[Paso 3] En el paso 3, los equipos de análisis se ocupan de la recogida de datos y del análisis de los resultados obtenidos en los pasos 1 y 2. Documentando los resultados de pasos anteriores, se consignan en la tabla que sigue tanto los controles basados en los activos como los controles organizativos.

Activo	**Control**	**Justificación de su selección**
Controles basados en los activos	**2.1.3**	Los controles de sistema y gestión de red son esenciales para mantener la disponibilidad y confidencialidad del activo objeto de consideración.
	2.1.6	
	2.1.4	La integridad de la aplicación es importante, dado que la información médica ha de ser precisa.
	2.4.2	La autenticación y la autorización de usuarios internos y externos, o de terceros, puede garantizar un acceso controlado al activo objeto de consideración.
	2.5.1	La gestión de vulnerabilidades, incluida la evaluación periódica de éstas, y las actividades de corrección necesarias, son esenciales para evaluar los sistemas y las medidas de seguridad.
	2.6.1	La información confidencial ha de protegerse durante su transporte y almacenamiento.

Controles organizativos	**SP1**	Formación y sensibilización en materia de seguridad
	SP3	Gestión de seguridad
	SP4	Política de seguridad
	SP5	Gestión basada en la colaboración
	SP6	Recuperación en caso de catástrofe

Tabla 20: Cuadro de controles seleccionados y su justificación – Ejemplo A

Ejemplo B. (Perfil de riesgo: medio, activo crítico: Sistema)

En el paso 1, los equipos de análisis que utilizan el **cuadro de controles organizativos** (Tabla 21: Selección de los controles organizativos - Ejemplo B

) seleccionan las tarjetas de controles organizativos para las áreas de riesgo identificadas en la fase 1 (paso 1 – **Cuadro de evaluación del perfil de riesgos**), definiendo así la orientación de las iniciativas de la organización en materia de seguridad de la información.

En el **ejemplo B**, el control organizativo dictado para un nivel bajo de riesgos jurídicos es el SP1.1, mientras que, para un nivel bajo de riesgos de productividad y para la estabilidad financiera, es el SP4.1. El nivel medio de riesgos en el área de la reputación y la pérdida de confianza de los clientes dicta el uso de los controles organizativos SP1 y SP4.

En la Tabla 21: Selección de los controles organizativos - Ejemplo B

se resumen los controles de ordenación en el ejemplo B antes referido.

Áreas de riesgo	Alto	Medio	Bajo
Riesgos jurídicos	(SP1)	(SP1)	**SP1.1**
	(SP4)	(SP4)	
Riesgos de productividad	(SP3)	(SP4)	**SP4.1**
	(SP4)		
	(SP6)	(SP6)	
	(SP5)		
Riesgos para la estabilidad financiera	(SP2)	(SP4)	**SP4.1**
	(SP1)		
	(SP4)		
Riesgos para la reputación y de pérdida de confianza de los clientes	(SP1)	**(SP4)**	SP4.1
	(SP5)	**(SP1)**	

Tabla 21: Selección de los controles organizativos - Ejemplo B

[Paso 2] En el paso 2, el equipo de análisis selecciona las tarjetas de controles basado en los activos utilizando la tabla correspondiente. En el ejemplo B, dado el perfil medio de riesgos de la organización identificado en la fase 1 (paso 1), y el tipo de activos críticos identificado en el paso 2, seleccionan la tarjeta 2 correspondiente a los sistemas con un perfil de riesgos alto, en concreto, la tarjeta CC-2S.

Cuadro de tarjetas de controles			
Activos críticos	**Tarjetas para riesgo alto**	**Tarjetas para riesgo medio**	**Tarjetas para riesgo bajo**
Aplicación	CC-1A	CC-2A	CC-3A
Sistema	CC-1S	**CC-2S**	CC-3S
Red	CC-1N	CC-2N	CC-3N
Personal	CC-1P	CC-2P	CC-3P

Tabla 22: Selección de tarjetas de controles basados en los activos - Ejemplo B

La tarjeta seleccionada en el ejemplo B (véase el

Anexo B. Tarjetas de controles basados en los activos) muestra los controles necesarios para los activos del sistema en una organización con un perfil de riesgos medio. El equipo identifica los controles que abordan los requisitos de seguridad identificados en la fase 3. Tras la obtención del resultado del ejemplo B de la fase 2 (paso 3), los requisitos de disponibilidad se utilizan para identificar los controles apropiados sobre la base de la **tarjeta** de controles **CC-2S**. De este modo, se seleccionan los controles basados en los activos **2.1.7** y **2.1.6**.

Identificación de la tarjeta de controles basados en los activos										**CC-2S**
Perfil de riesgos										**Medio**
Categoría de activo										**Sistema**
Requisitos de seguridad	**Seguridad física**	**Gestión de sistemas y redes**	**Herramientas de administración de sistemas**	**Seguimiento y auditoría de la seguridad física**	**Autenticación y autorización**	**Gestión de vulnerabilidades**	**Codificación**	**Diseño y arquitectura de seguridad**	**Gestión de incidentes**	**Prácticas de personal generales**
Confidencialidad		2.1.6 2.1.7			2.4.1					
Integridad		2.1.9			2.4.1					
Disponibilidad		2.1.6 2.1.7								

Tabla 23: Tarjeta de controles basados en los activos CC-2S - Ejemplo B

[Paso 3] En el paso 3, los equipos de análisis se ocupan de la recogida de datos y del análisis de los resultados obtenidos en los pasos 1 y 2. Documentando los resultados de pasos anteriores, se consignan en la tabla que sigue tanto los controles basados en los activos seleccionados, como los controles organizativos.

Activo	**Control**	**Justificación de su selección**
Controles basados en los activos	**2.1.6**	Los controles de sistema y gestión de red son esenciales para mantener la disponibilidad y confidencialidad del activo objeto de consideración.
	2.1.7	
Controles organizativos	**SP1**	Formación y sensibilización en materia de seguridad
	SP4	Política de seguridad
	SP1.1	Incluidos en SP1
	SP4.1	Incluidos en SP4

Tabla 24: Justificación de la selección de los controles – Ejemplo B

Fase 4 – Ejecución y gestión

En la fase 4, el equipo de análisis determina acciones y recomienda una lista de éstas, en la que expone la orientación de las mejoras de seguridad. Resulta esencial para el éxito de la ejecución el patrocinio de la alta dirección (responsables de la toma de decisiones) de cara a la mejora continua de la seguridad.

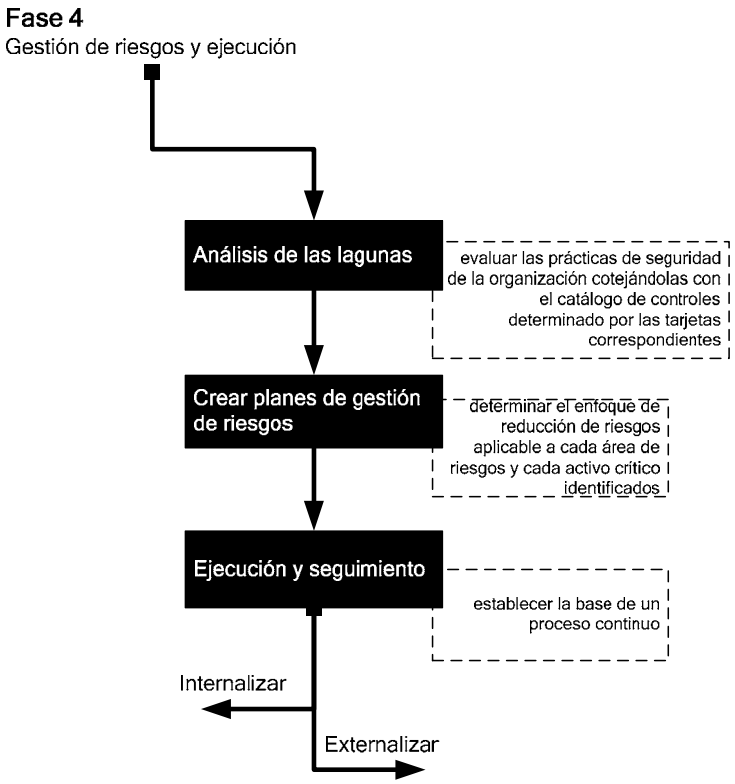

Figura 6: Fase 4 – Flujo de trabajo de la ejecución y gestión

Paso 1. Análisis de las lagunas

El análisis de las lagunas (*gap analysis*) es fundamental para mejorar el modo en que una organización gestiona la seguridad de la información, y determinar la situación en materia de seguridad en cada momento, es decir, lo que se hace bien actualmente y las áreas susceptibles de mejora.

En este paso, los equipos de análisis se ocupan de evaluar las prácticas de seguridad vigentes de la organización respecto a los controles, conforme se describen éstos en las tarjetas de controles. Leen con detenimiento ciertas tarjetas de controles seleccionadas y extraen información detallada sobre las políticas, los procedimientos y las prácticas de seguridad en curso de la organización, obteniendo así un punto de partida para la mejora.

Durante el proceso de análisis de las lagunas, los equipos de proceso utilizan las tarjetas de controles como "requisitos" y evalúan las diferencias existentes entre éstos y las prácticas de seguridad, tanto a escala de la organización como de los activos críticos. Los equipos de análisis deben documentar pormenorizadamente los resultados en dos planes diferenciados: **(1) uno para la mejora organizativa** y **(2) otro para la protección de los activos**.

El resultado de este proceso puede constituir la base de la actividad de planificación que se emprende a continuación. Se divide en dos categorías: la de los **(a) controles organizativos**, en la que los equipos de análisis deben establecer lo que se hace y lo que no, y definir acciones para la mejora a

escala de la organización, y la de los **(b) controles basados en los activos**, en la que los equipos de análisis evalúan las medidas de protección vigentes aplicadas a los activos críticos identificados.

Paso 2. Crear planes de reducción de riesgos

En este paso, los miembros del equipo de análisis han identificado ya los activos críticos, el perfil de riesgos de la organización y los requisitos de seguridad, han seleccionado además los controles apropiados y están a punto de determinar el enfoque de mitigación para cada área de riesgo y activo crítico identificados.

Al dar estos pasos iniciales hacia la mejora, las organizaciones pueden comenzar a generar el impulso necesario para aplicar su estrategia de protección.

El resultado de esta actividad es el plan de reducción de riesgos, que **da lugar a una serie de pasos** que puede dar la organización para elevar o mantener su nivel de seguridad. Su objetivo es establecer directrices respecto a las iniciativas futuras en materia de seguridad de la información, más que encontrar una solución inmediata a toda vulnerabilidad y motivo de preocupación relacionados con la seguridad. Puesto que un plan de mitigación contiene una orientación organizativa sobre las actividades de seguridad de la información, proponemos que se estructure dicho plan en torno a las tarjetas de controles (fase 3) seleccionadas (organizativos y basados en los activos críticos).

Paso 3. Ejecución, seguimiento y control

Uno de los principios del método de evaluación de riesgos es el que hace referencia al concepto de proceso continuo. Este principio expresa la necesidad de que los resultados de las evaluaciones de riesgos relativos a la seguridad de la información se lleven a la práctica como único modo de garantizar la mejora de la seguridad. **Si una organización no lleva a la práctica los resultados de la evaluación, tampoco mejorará su situación en lo que se refiere a seguridad**.

Una de las tareas más difíciles en toda actividad de mejora es mantener el impulso generado durante la evaluación. No obstante, consideraciones prácticas impiden que la mayoría de las organizaciones ejecuten de inmediato todas las iniciativas tras la evaluación. Probablemente, las PYME dispondrán de fondos y recursos humanos limitados a este respecto.

En **el presente paso, los equipos de análisis asignan prioridades a las actividades y, a continuación, se centran en la ejecución de aquellas a las que se ha asignado una prioridad más elevada**.

Existen tres opciones diferenciadas:

- **Aceptación de los riesgos**. Cuando se acepta un riesgo, no se emprende acción alguna para su mitigación, y, en caso de que el riesgo se materialice, las consecuencias se aceptan.
- **Mitigación de los riesgos**. Cuando se mitiga un riesgo, se determinan y aplican acciones encaminadas a contrarrestar la amenaza y, por tanto, a reducir el riesgo.

Una vez identificadas las actuaciones específicas, los miembros de los equipos de análisis han de asignar responsabilidades para su realización, así como una fecha para su culminación. Deben reordenarse las respuestas (respecto a cada actuación)a las preguntas que siguen:

- ¿Quién será **responsable** de cada actuación?
- ¿Qué puede hacer la dirección para **facilitar** la culminación de cada actuación?
- ¿Cuánto **costará**?
- ¿**Cuánto tiempo** llevará?
- **¿Lo podemos hacer nosotros por nuestra cuenta?**
- **¿Necesitamos asistencia externa?**

NOTA:

las dos últimas preguntas son fundamentales para determinar **si una organización puede abordar o no internamente la ejecución** de los **controles necesarios**. Las respuestas a las mismas son

igualmente importantes y muy difíciles de establecer, dado que las dos opciones (externalización o internalización) presentan ventajas e inconvenientes.

La externalización es una **decisión del tipo "fabricar o comprar" aplicada al recurso en cuestión**. Si se hace bien, la externalización puede ofrecer ventajas concretas. Los objetivos principales de la externalización son, además del apoyo a determinadas funciones, el recorte de gastos, el redimensionamiento y un deseo de dar prioridad al negocio básico (competencia esencial). La falta de competencia en materia de TI en la organización puede constituir asimismo una razón para la externalización. A medida que las TI cobran importancia, las empresas se enfrentan a menudo a una amplia disparidad entre las capacidades y las destrezas necesarias para realizar el potencial de las tecnologías de la información y la realidad de sus propios conocimientos internos especializados en tecnología.

Con todo, existen varias opciones que deben considerarse y que combinan las competencias esenciales de la organización, con la asistencia externa o de terceros (externalización parcial o completa). Como se deduce de la **figura 7**, tanto la gestión como la ejecución pueden externalizarse. **Las ofertas de servicios que suelen presentar los proveedores pueden resumirse como sigue:**

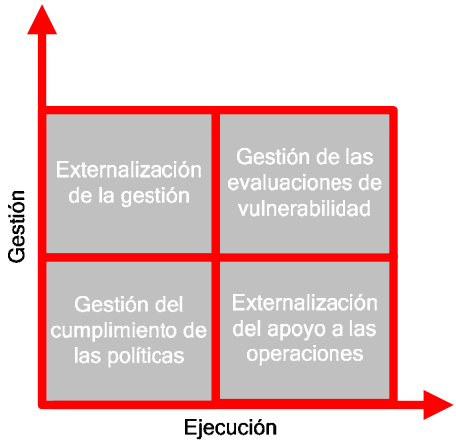

Figura 6: Opciones de externalización de la gestión y la ejecución

- **Externalización de la gestión**. En la externalización de la gestión, los proveedores prestan servicios de gestión de la seguridad de la información. En otras palabras, **el proveedor asigna un encargado de seguridad** para gestionar el programa de la organización en este ámbito. El precio se calcula habitualmente con arreglo a una tarifa trimestral que depende de la dimensión y de la complejidad de la organización, las destrezas necesarias y la cultura existente.
- **Gestión del cumplimiento de las políticas**. En los regímenes de este tipo, los asesores de seguridad **realizan auditorías programadas cada cierto tiempo** con el fin de garantizar el cumplimiento continuo de los controles y la política de seguridad de la información establecida por la organización, e identificar todo caso de disconformidad. Como resultado de este proceso periódico, la organización recibe un informe pormenorizado sobre el estado general de los sistemas, las áreas de incumplimiento y las directrices para conseguir que estos sistemas regresen a la senda del cumplimiento. Se incluyen igualmente análisis e informes de tendencias que le ayudan a determinar si mejora o no la situación de seguridad y las razones de tal evolución.
- **Gestión de las evaluaciones de vulnerabilidad**. Con arreglo a estas modalidades de contratos de nivel de servicio, los **proveedores prestan un conjunto singular de servicios de evaluación de la vulnerabilidad** que pueden adaptarse para dirigirse a todos los posibles puntos de entrada de información de la organización: Internet, redes internas, aplicaciones, acceso remoto e instalaciones inalámbricas. Sobre la base de los factores impulsores de la actividad empresarial, los activos técnicos y los factores de amenaza, los

proveedores ayudan a los clientes a determinar el intervalo apropiado para las evaluaciones periódicas y el grado óptimo de investigación en profundidad y en extensión.

- **Gestión del apoyo a las operaciones.** Los servicios de apoyo a las operaciones de seguridad en curso ofrecen recursos a las organizaciones clientes para abordar sus **operaciones de seguridad internas** a diario. Los proveedores suelen ofrecer diversos niveles modulares de asistencia, desde la simple consultoría y asesoramiento para la aplicación de soluciones y políticas de seguridad hasta la ingeniería y la realización técnica de una infraestructura de seguridad. Las operaciones de seguridad en curso suelen incluir tareas como el refuerzo de servidores, cambios de configuración de seguridad, el *patching* de seguridad de aplicaciones, etc.
- **Respuesta a casos de emergencia e incidentes**. Los servicios de respuesta a casos de emergencia e incidentes garantizan la asistencia con ingenieros expertos en las instalaciones de la organización en situaciones de urgencia o de crisis. Los servicios de respuesta y gestión de incidentes habilitan a las organizaciones cliente para **responder con rapidez y confianza a incidentes de seguridad de índole informática**, incluida la puesta en peligro de sistemas, las infecciones con virus, y el rechazo de ataques al servicio, contribuyendo a reducir al mínimo los períodos de inactividad y la pérdida de ingresos.

Los requisitos de seguridad de las organizaciones que externalizan la gestión y el control de todos o algunos de sus sistemas de información, redes y entornos informáticos deben abordarse en contratos de nivel de servicio (CNS) entre las partes. Como mínimo, en todo CNS deben tratarse las cuestiones que siguen (controles) para la externalización de las operaciones y la gestión de la seguridad de la información:

A. Nivel de externalización y asunción de responsabilidades;
B. Seguimiento del cumplimiento;
C. Responsabilidades de gestión;
D. Alcance del servicio;
E. Modo en que se atenderán los requisitos jurídicos, como la legislación sobre protección de datos;
F. Los mecanismos de que se dispondrá para que todas las partes intervinientes en la externalización, incluidos los subcontratistas, sean conscientes de sus responsabilidades en materia de seguridad;
G. Modo en que se mantendrán y comprobarán la integridad y la confidencialidad de los activos empresariales de la organización;
H. Los controles físicos y lógicos que se emplearán para restringir y limitar el acceso a la información empresarial sensible de la organización a usuarios autorizados;
I. El modo en que se mantendrá la disponibilidad de los servicios en caso de catástrofe;
J. El derecho de auditoría;
K. La competencia en cuanto a recursos y la certificación profesional;
L. El contenido, la frecuencia y la estructura de los informes.

Ejemplo A. (Perfil de riesgo: alto, activo crítico: aplicación)

[Paso 1] En este paso, los equipos de análisis se ocupan de la evaluación de las prácticas de seguridad vigentes de la organización, comparadas con los controles descritos en las tarjetas de controles. Dichos equipos leen con detenimiento los controles aplicables al perfil de la organización (según se describe en las tarjetas de controles seleccionadas (fase 3, paso 3) y extraen información detallada sobre las políticas, los procedimientos y las prácticas de seguridad en curso de la organización, obteniendo así un punto de partida para la mejora.

La tabla que sigue se refiere al ejemplo A:

Activo	Control	¿Seguimos actualmente los controles incluidos en las tarjetas de controles?
Controles basados en los activos	**2.1.3**	No
	2.1.4	Parcialmente
	2.1.6	No
	2.4.2	Parcialmente
	2.5.1	No
	2.6.1	No
Controles organizativos	**SP1**	No
	SP3	No
	SP4	Sí
	SP5	No
	SP6	Parcialmente

Tabla 25: Lista de análisis de las lagunas – ejemplo A

[Paso 2] En el paso 2, los equipos de análisis leen los controles (anexos A, B, C, D) y deciden respecto a las acciones necesarias.

Activo	Control	Acción
Controles basados en los activos	**2.1.3**	El equipo decide proteger la información sensible mediante un almacenamiento seguro, como las cadenas de custodia definidas, el depósito de copias de respaldo fuera de las instalaciones de la organización, los medios de almacenamiento separables, y los procesos de descarte de información sensible o de sus medios de almacenamiento.
	2.1.4	El equipo decide proteger la información sensible mediante la comprobación periódica de la integridad de la base de software instalada para la aplicación.
	2.1.6	El equipo decide desarrollar un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, reclama la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos, y exige la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.
	2.4.2	El equipo decide establecer políticas y procedimientos de uso de la información documentados respecto al acceso individual y colectivo, con el fin de (A) fijar las normas para la concesión de niveles de acceso apropiados, (B) establecer un derecho inicial de acceso, (C) modificar el derecho de acceso, (D) suspender el derecho de acceso, y (F) revisar y comprobar periódicamente los derechos de acceso.
	2.5.1	El equipo decide seleccionar herramientas de evaluación de vulnerabilidades, listas de comprobación y *scripts*, manteniéndose al día respecto a los tipos de vulnerabilidades y los métodos de ataque conocidos, revisando fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones, identificando componentes de la estructura que han de evaluarse, programando evaluaciones de vulnerabilidad, interpretando resultados y dando respuesta a éstos, y manteniendo la seguridad del almacenamiento y la disposición de datos de vulnerabilidad.
	2.6.1	El equipo decide NO ejecutar la codificación de los datos transmitidos. Los datos almacenados se protegen en lo que respecta a la confidencialidad mediante un sistema de control de accesos.

Controles organizativos	**SP1**	El equipo decide emprender una campaña de sensibilización básica mediante la instrucción de todos los abogados respecto a los riesgos que conlleva el uso del correo electrónico, Internet, etc.
	SP3	Debe establecerse una función de gestión de la seguridad. Se asignará un encargado de seguridad.
	SP4	El equipo decide asimismo formular una política de seguridad genérica en la que se definan las distintas responsabilidades en lo que respecta a la información.
	SP5	Se deciden los procedimientos de gestión basada en la colaboración que atañen a los terceros responsables del mantenimiento de la aplicación.
	SP6	Se aplicará y se comprobará periódicamente un plan de recuperación en caso de catástrofe.

Tabla 26: Lista de actuaciones – ejemplo A

[Paso 3] En el paso 3 para el ejemplo A, los equipos de análisis asignan prioridades a las actividades y, a continuación, se centran en la ejecución de aquellas a las que se ha asignado una prioridad más elevada. Deciden las acciones de prioridad elevada que se llevarán a cabo en el trimestre siguiente, las de prioridad media que se ejecutarán el semestre posterior y las de prioridad baja que se llevarán a cabo antes de que concluya el próximo ejercicio.

Una vez identificadas las actuaciones específicas de la lista, tendrán que asignarse responsabilidades para su realización, así como una fecha para su culminación. Responda las preguntas que siguen respecto a cada actuación de su lista, y registre los resultados:

- ¿Quién será responsable de cada actuación?
- ¿Para qué fecha debe haberse abordado la actuación?
- ¿Qué puede hacer la dirección para facilitar la culminación de cada actuación?
- ¿Cuánto costará?
- ¿Cuánto tiempo llevará?
- ¿Lo podemos hacer nosotros por nuestra cuenta?
- ¿Necesitamos asistencia externa?

El resultado de su plan se resume en la tabla que sigue:

Activo	Control	Responsable	Se requiere asistencia externa	Hito	Prioridad
Controles basados en los activos	**2.1.3**	Empleado A	No	Mes / día	Alta
	2.1.4	Empleado A	Sí		Media
	2.1.6	Empleado A	Sí		Alta
	2.4.2	Empleado A	Sí		Media
	2.5.1	Empleado A	No		Baja
	2.6.1	Empleado A	No		Media
Controles organizativos	**SP1**	Empleado B	No		Baja
	SP3	Empleado B	No		Media
	SP4	Empleado B	Sí		Media
	SP5	Empleado B	No		Alta
	SP6	Empleado B	No		Alta

Tabla 27: Plan de ejecución - ejemplo A

Ejemplo B. (Perfil de riesgo: medio, activo crítico: sistema)

[Paso 1] En este paso, los equipos de análisis se ocupan de la evaluación de las prácticas de seguridad vigentes de la organización, comparadas con los controles descritos en las tarjetas de controles. Dichos equipos leen con detenimiento los controles aplicables al perfil de la organización (según se describe en ciertas tarjetas de controles seleccionadas (fase 3, paso 3) y extraen información detallada sobre las políticas, los procedimientos y las prácticas de seguridad en curso de la organización, obteniendo así un punto de partida para la mejora.

La tabla que sigue se refiere al ejemplo B:

Activo	Control	¿Seguimos actualmente los controles incluidos en las tarjetas de controles?
Controles basados en los activos	**2.1.6**	No
	2.1.7	Sí
Controles organizativos	**SP1**	Parcialmente
	SP4	Sí
	SP1.1	No
	SP4.1	Sí

Tabla 28: Lista de análisis de las lagunas – ejemplo B

[Paso 2] En el paso 2, los equipos de análisis leen los controles (apéndices A, B, C, D) y deciden respecto a las acciones necesarias.

Activo	Control	Acciones
Controles basados en los activos	**2.1.6**	El equipo decide desarrollar un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, reclama la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos, y exige la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.
	2.1.7	El equipo decide informar e instruir a todo el personal para que comprenda y pueda llevar a cabo sus tareas con arreglo a los planes de respaldo.
Controles organizativos	**SP1**	El equipo decide emprender una campaña de sensibilización básica mediante la instrucción de todos los abogados respecto a los riesgos que conlleva el uso del correo electrónico, Internet, etc.
	SP4	El equipo decide asimismo formular una política de seguridad genérica en la que se definan las distintas responsabilidades en lo que respecta a la información.
	SP1.1	Incluido en SP1
	SP4.1	Incluido en SP4

Tabla 29: Lista de actuaciones – ejemplo B

[Paso 3] En el paso 3 del ejemplo B, los equipos de análisis asignan prioridades a las actividades y, a continuación, se centran en la ejecución de aquellas a las que se ha asignado una prioridad más elevada. Deciden las acciones de prioridad elevada que se llevarán a cabo en el trimestre siguiente, las de prioridad media que se ejecutarán en el semestre posterior y las de prioridad baja que se ejecutarán antes de que concluya el próximo ejercicio.

Una vez identificadas las actuaciones específicas de la lista, tendrán que asignarse responsabilidades para su realización, así como una fecha para su culminación. Responda las preguntas que siguen respecto a cada actuación de su lista, y registre los resultados:

- ¿Quién será responsable de cada actuación?
- ¿Para qué fecha debe haberse abordado la actuación?
- ¿Qué puede hacer la dirección para facilitar la culminación de cada actuación?
- ¿Cuánto costará?
- ¿Cuánto tiempo llevará?
- ¿Lo podemos hacer nosotros por nuestra cuenta?
- ¿Necesitamos asistencia externa?

El resultado de su plan se resume en la tabla que sigue:

Activo	Control	Responsable	Se requiere asistencia externa	Hito	Prioridad
Controles basados en los activos	**2.1.6**	Empleado A	No	Mes / día	Alta
	2.1.7	Empleado A	No		Alta
Controles organizativos	**SP1**	Empleado A	No		Media
	SP4	Empleado A	No		Baja
	SP1.1	Empleado A	No		Baja
	SP4.1	Empleado A	No		Alta

Tabla 30: Plan de ejecución - ejemplo B

Anexo A. Tarjetas de controles organizativos

Formación y sensibilización en materia de seguridad (SP1)	
SP1	Esta tarjeta prevé la realización de controles para garantizar que los miembros del personal comprenden sus funciones y responsabilidades en lo que se refiere a la seguridad. Deben impartirse a todo el personal conocimientos y formación y han de enviársele recordatorios periódicos en materia de seguridad. Los conocimientos y funciones del personal han de documentarse claramente, y debe comprobarse periódicamente su conformidad.
Estrategia de seguridad (SP2)	
SP2	Esta tarjeta prevé la realización de controles para garantizar que las estrategias empresariales de la organización incluyen habitualmente aspectos de seguridad. Del mismo modo, en las estrategias y políticas de seguridad deben tenerse en cuenta las estrategias y objetivos empresariales de la organización. Las estrategias, metas y objetivos en materia de seguridad deben documentarse y revisarse, actualizarse y comunicarse periódicamente a la organización.
Gestión de la seguridad (SP3)	
SP3	Esta tarjeta prevé la realización de controles para garantizar la adopción y ejecución de un proceso de gestión de la seguridad. Este proceso debe evaluar de manera continua los niveles de seguridad de la información requeridos, y definir los controles apropiados y equilibrados en cuanto a costes y riesgos que deben aplicarse y documentarse.
Políticas y normativas de seguridad (SP4)	
SP4	Esta tarjeta exige a las organizaciones que dispongan de un conjunto exhaustivo de políticas de seguridad de la información documentadas y al día que se revisen y actualicen periódicamente.
Gestión de la seguridad en régimen de colaboración (SP5)	
SP5	Esta tarjeta prevé la realización de controles de seguridad que garanticen la aplicación de procedimientos documentados y supervisados para la protección de la información de la organización cuando ésta colabora con entidades externas (p. ej., terceros, colaboradores, subcontratistas u otros socios).
Planificación de contingencias/recuperación en caso de catástrofe (SP6)	
SP6	Esta tarjeta prevé la realización de controles de seguridad para garantizar la continuidad de las operaciones empresariales en caso de catástrofe o indisponibilidad de la información. Los elementos clave de la tarjeta son los que siguen: ▫ planes de continuidad de la actividad empresarial y de operación en casos de emergencia; ▫ planes de recuperación en caso de catástrofe; y ▫ planes de contingencia para la respuesta en casos de emergencia.

Anexo B. Tarjetas de controles basados en los activos[3]

Identificación de la tarjeta de controles basados en los activos					CC-1A					
Perfil de riesgos					Alto					
Categoría de activos					Aplicación					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad		2.1.3			2.4.2	2.5.1	2.6.1			
Integridad		2.1.4			2.4.2	2.5.1	2.6.1			
Disponibilidad		2.1.6								

Los controles de confidencialidad basados en aplicaciones para un perfil organizativo de riesgos alto suelen abordar requisitos de seguridad a escala de aplicaciones, sistemas, redes y personal, con el fin de salvaguardar el ciclo vital de información esencial. Los controles se seleccionan fundamentalmente para tratar los activos de información en lo que atañe a su revelación a entidades no autorizadas, ya sean externas, o internas del entorno de la organización.

Los controles esenciales para la protección de la confidencialidad de activos críticos son los que siguen:

OP2.4.2 Este control exige que haya políticas y procedimientos de uso de la información documentados respecto al acceso individual y colectivo, con el fin de (A) fijar las normas para la concesión de niveles de acceso apropiados, (B) establecer un derecho inicial de acceso, (C) modificar el derecho de acceso, (D) suspender el derecho de acceso, y (F) revisar y comprobar periódicamente los derechos de acceso.

OP2.5.1 Este control exige que exista un conjunto documentado de procedimientos para la gestión de la vulnerabilidad, incluida la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y *scripts*, manteniéndose al día respecto a los tipos de vulnerabilidades y los métodos de ataque conocidos, revisando fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones, identificando componentes de la estructura que han de evaluarse, programando evaluaciones de vulnerabilidad, interpretando resultados y dando respuesta a éstos, y manteniendo la seguridad del almacenamiento y la disposición de datos de vulnerabilidad.

OP2.1.3 Este control exige que se proteja la información sensible mediante un almacenamiento seguro, como las cadenas de custodia definidas, el depósito de copias de respaldo fuera de las instalaciones de la organización, los medios de almacenamiento separables, y los procesos de eliminación de información sensible o de sus medios de almacenamiento.

OP2.1.4 Este control exige que se compruebe regularmente la integridad del software instalado.

[3] La asignación de controles a las tarjetas de control de activos en el presente anexo se ha efectuado de un modo que permite la consecución de un grado de protección adecuado. En el caso de los activos con requisitos de seguridad muy elevados, podrían considerarse controles adicionales. En cualquier caso, mediante el uso de estas tarjetas de control de activos, puede lograrse una protección media razonable, que parece apropiada para la mayoría de las PYME. A medio plazo, la ENISA se propone validar los supuestos asumidos en el presente documento mediante proyectos piloto.

OP2.1.6 Este control exige que exista un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, y exige la realización de copias de respaldo programadas regularmente, tanto del software como de los datos, así como la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

Identificación de la tarjeta de controles basados en los activos					CC-1S					
Perfil de riesgos					Alto					
Categoría de activos					Sistema					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad		2.1.3 2.1.4 2.1.5 2.1.9			2.4.1 2.4.6		2.6.1			
Integridad		2.1.4 2.1.5 2.1.8 2.1.9 2.1.10			2.4.1 2.4.3 2.4.6			2.7.1 2.7.2		
Disponibilidad		2.1.6 2.1.7 2.1.9			2.4.6					

Un perfil de riesgos alto es aquel en el que, si el sistema deja de funcionar correctamente, el servicio empresarial queda interrumpido. Los sistemas no pueden albergar determinadas aplicaciones empresariales, o pueden causar la pérdida de información fundamental. El origen de la amenaza puede consistir en la inestabilidad del sistema debido a un mal funcionamiento mecánico, o en una instalación y uso inadecuados.

Los controles de confidencialidad basados en el sistema para un perfil de riesgos alto comprenden métodos que garanticen una configuración y una funcionalidad adecuadas del sistema. Suelen abordar requisitos de seguridad a escala de aplicación, del sistema, de la red y del personal, con el fin de garantizar la estabilidad del sistema y la integridad de la información esencial. La disponibilidad constante del sistema es un requisito para la continuidad de la actividad empresarial. Los controles se seleccionan fundamentalmente para tratar los activos de información en lo que atañe a su revelación a entidades no autorizadas, ya sean externas o internas del entorno de la organización.

Los controles esenciales para la salvaguarda de la integridad en el caso de los activos críticos son los que siguen:

OP2.1.3 Este control exige que se proteja la información sensible mediante un almacenamiento seguro, como las cadenas de custodia definidas, el depósito de copias de respaldo fuera de las instalaciones de la organización, los medios de almacenamiento separables, y los procesos de eliminación de información sensible o de sus medios de almacenamiento.

OP2.1.4 Este control exige que se compruebe regularmente la integridad del software instalado.

OP2.1.5 Este control exige que todos los sistemas se encuentren actualizados respecto a revisiones, parches, y recomendaciones en documentos consultivos sobre seguridad.

OP2.1.6 Este control exige que exista un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, y exige la realización de copias de respaldo programadas regularmente, tanto del software como de los datos, así como la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.

OP 2.1.7 Este control exige que todo el personal comprenda y sea capaz de desempeñar sus responsabilidades en los planes de respaldo.

OP2.1.8 Este control exige que los cambios del hardware y el software de las TI se planifiquen, supervisen y documenten.

OP2.1.9 Este control exige que los miembros del personal de TI sigan los procedimientos correctos al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario. Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros. Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.

OP2.1.10 Este control exige que sólo operen en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.

OP2.2.1 Este control exige que los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisen regularmente para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.

OP2.2.2 Este control exige el uso de herramientas y mecanismos para conseguir una administración de sistemas y de red segura, así como su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen: comprobadores de la integridad de datos, herramientas criptográficas, escáneres de vulnerabilidad, herramientas de comprobación de la calidad de las contraseñas, escáneres de virus, herramientas de gestión de procesos, sistemas de detección de intrusos, administraciones remotas seguras, herramientas de servicio de red, analizadores de tráfico, herramientas de respuesta a incidentes, y herramientas forenses para el análisis de datos.

OP2.3.1 Este control exige que la organización utilice de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes. La actividad es objeto de seguimiento por parte del personal de TI, la actividad de sistemas y redes se registra, los registros se revisan regularmente, la actividad inusual se trata con arreglo a la política o el procedimiento pertinentes y las herramientas se revisan y actualizan periódicamente.

OP2.4.1 Este control exige que se utilicen los controles de acceso y la autentificación de usuario pertinentes (p. ej., permisos de archivo, configuración de redes) y coherentes con las políticas establecidas al respecto, con el fin de restringir el acceso de los usuarios a la información, las utilidades del sistema, el código fuente de programas, sistemas sensibles, aplicaciones y servicios específicos, conexiones de red en la organización y conexiones de red con origen fuera de ésta.

OP2.4.3 Este control exige que los métodos y mecanismos de control de acceso restrinjan el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.

OP2.4.6 Este control exige que se utilicen mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de tales mecanismos las firmas digitales y los recursos biométricos.

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

OP2.7.1 Este control exige que, al abordar la arquitectura y el diseño de sistemas nuevos y revisados, se tengan en cuenta las estrategias, políticas y procedimientos de seguridad, el historial de situaciones de riesgo para la seguridad, y los resultados de evaluaciones de riesgos para la seguridad.

OP2.7.2 Este control exige que la organización disponga de diagramas actualizados que muestren la tipología de red y arquitectura de seguridad del conjunto de la empresa.

Identificación de la tarjeta de controles basados en los activos					CC-1N					
Perfil de riesgos					Alto					
Categoría de activos					Red					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad					2.4.6	2.5.3	2.6.1			
Integridad	1.1.4	2.1.1 2.1.10			2.4.1 2.4.3 2.4.4 2.4.6	2.5.3		2.7.2		
Disponibilidad	1.1.4				2.4.6					

Un perfil de riesgos alto conlleva la existencia de amenazas que se dan en la red, vulnerabilidades que pueden dar lugar a ataques externos, o accesos internos no autorizados a ciertas áreas de la red de elevado interés o riesgo.

La ausencia de seguridad en la red ejerce un efecto inmediato y directo en el funcionamiento de las aplicaciones y en el flujo de información.

Los controles de confidencialidad basados en la red y correspondientes a un perfil organizativo de riesgos alto deben proteger la información esencial e interna de posibles pérdidas o abusos. Por otra parte, la información almacenada en la red debe encontrarse disponible, ser de fácil acceso, y separarse con arreglo a su nivel de relevancia.

Los controles esenciales para la salvaguarda de la confidencialidad, la integridad y la disponibilidad en la red son los que siguen:

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

OP2.4.6 Este control exige que se utilicen mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de tales mecanismos las firmas digitales y los recursos biométricos.

OP2.7.2 Este control exige que la organización disponga de diagramas actualizados que muestren la tipología de red y arquitectura de seguridad del conjunto de la empresa.

OP2.1.1 Este control exige que existan planes de seguridad documentados para la salvaguarda de sistemas y redes.

OP2.4.1 Este control exige que se utilicen los controles de acceso y la autentificación de usuario pertinentes (p. ej., permisos de archivo, configuración de redes) y coherentes con las políticas establecidas al respecto, con el fin de restringir el acceso de los usuarios a la información, las utilidades del sistema, el código fuente de programas, sistemas sensibles, aplicaciones y servicios específicos, conexiones de red en la organización y conexiones de red con origen fuera de ésta.

OP2.4.3 Este control exige que los métodos y mecanismos de control de acceso restrinjan el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.

OP2.1.10 Este control exige que sólo operen en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.

OP 2.5.3 Este control exige que las evaluaciones de vulnerabilidad de la tecnología se realicen de manera periódica, y que las vulnerabilidades se traten cuando sean detectadas.

OP1.1.4 Este control exige que existan políticas y procedimientos documentados para la gestión de visitantes, incluidos los relativos a la firma al acceso, el acompañamiento, los registros de acceso, la recepción y los servicios de hospitalidad.

OP2.4.6 Este control exige que se utilicen mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de tales mecanismos las firmas digitales y los recursos biométricos.

Identificación de la tarjeta de controles basados en los activos										CC-1P
Perfil de riesgos										Alto
Categoría de activos										Personal
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad										3.2.1 3.2.2 3.2.3
Integridad	1.1.4 1.3.2									3.2.1 3.2.2 3.2.3
Disponibilidad										

Un perfil de riesgos alto conlleva la existencia de amenazas respecto a la gestión de personal, y a los recursos humanos en general. El nivel de compromiso del personal en cuanto a la utilización de controles de seguridad apropiados respecto a los recursos de red determina el nivel de protección que puede alcanzarse.

La manipulación de la información y la reutilización de registros de mayor antigüedad con un valor elevado para la organización constituye un aspecto fundamental. La información interna o confidencial del personal debe tratarse con respeto. El seguimiento de las políticas de personal respecto a tales procedimientos garantiza la confidencialidad, la integridad y la disponibilidad de la información.

Los controles esenciales para garantizar la confidencialidad, la integridad y la disponibilidad de la información, en combinación con un activo crítico como las personas, son los que siguen:

OP3.2.1 Este control exige que los miembros del personal apliquen unas buenas prácticas en materia de seguridad: proteger la información de la que son responsables; abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social); disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información; utilizar buenas prácticas en relación con las contraseñas; comprender y observar las políticas y normativas en materia de seguridad; y reconocer e informar de los incidentes que se produzcan.

OP3.2.2 Este control exige que todo el personal, a todas las escalas de responsabilidad, desempeñe las funciones que se le han asignado y asuma sus responsabilidades en lo que atañe a la seguridad de la información.

OP3.2.3 Este control exige que existan procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en emplazamientos en los que se almacena la misma. Esta condición atañe a empleados, contratistas, socios, colaboradores y personal de organizaciones terceras, así como al personal de mantenimiento de sistemas y el de mantenimiento de instalaciones.

OP1.1.4 Este control exige que existan políticas y procedimientos documentados para la gestión de visitantes, incluidos los relativos a la firma al acceso, el acompañamiento, los registros de acceso, la recepción y los servicios de hospitalidad.

OP1.3.2 Este control exige que puedan justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.

Identificación de la tarjeta de controles basados en los activos					CC-2A					
Perfil de riesgos					Media					
Categoría de activos					Aplicación					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad					2.4.2		2.6.1			
Integridad					2.4.2					
Disponibilidad		2.1.6 2.1.7								

Un perfil de riesgos medio atañe al almacenamiento y el proceso de información propia interna o de valor moderado que conllevaría habitualmente un perfil de amenazas genérico relativo a la existencia de entidades externas malintencionadas que pretenden infringir o poner en peligro la confidencialidad de información específica y de valor moderado. Los controles de confidencialidad basados en aplicaciones para un perfil organizativo de riesgos medio suelen abordar requisitos de seguridad a escala de aplicaciones, sistemas, redes y personal, con el fin de salvaguardar el ciclo vital de información esencial. Los controles de integridad basados en aplicaciones respecto a un perfil organizativo de riesgos medio definen el grado de precisión de la información de una aplicación, mientras que la disponibilidad alude al nivel de accesibilidad.

Los controles esenciales para la protección de la confidencialidad, la integridad y la disponibilidad en la red son los que siguen:

OP2.4.2 Este control exige que existan políticas y procedimientos de uso de la información documentados respecto al acceso individual y colectivo, con el fin de fijar las normas para la concesión de niveles de acceso apropiados, establecer un derecho inicial de acceso, modificar el derecho de acceso, suspender el derecho de acceso, y revisar y comprobar periódicamente los derechos de acceso.

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

OP2.1.6 Este control exige que exista un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, y exige la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos, así como la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.

OP2.1.7 Este control exige que todo el personal comprenda y sea capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.

Identificación de la tarjeta de controles basados en los activos					CC-2S					
Perfil de riesgos					Media					
Categoría de activos					Sistema					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de vulnerabilidades	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad		2.1.6 2.1.7			2.4.1					
Integridad		2.1.9			2.4.1					
Disponibilidad		2.1.6 2.1.7								

Un perfil de riesgos medio implica amenazas de nivel moderado que se producen en caso de inestabilidades del sistema y dan lugar a la indisponibilidad del servicio empresarial durante un período de tiempo breve. Los sistemas no son capaces de dar soporte a las aplicaciones o funciones debidamente.

Los controles basados en el sistema para un perfiles de riesgos medio comprenden métodos que garantizan una configuración y una funcionalidad del sistema para un acceso apropiado.

El control esencial para la protección de la confidencialidad, la integridad y la disponibilidad en la red es el que sigue:

OP2.4.1 Este control exige que se utilicen los controles de acceso y la autentificación de usuario pertinentes (p. ej., permisos de archivo, configuración de redes) y coherentes con las políticas establecidas al respecto, con el fin de restringir el acceso de los usuarios a la información, las utilidades del sistema, el código fuente de programas, sistemas sensibles, aplicaciones y servicios específicos, conexiones de red en la organización y conexiones de red con origen fuera de ésta.

OP2.1.6 Este control exige que exista un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, y exige la realización de copias de respaldo programadas regularmente, tanto del software como de los datos, así como la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.

OP2.1.7 Este control exige que todo el personal comprenda y sea capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.

OP2.1.9 Este control exige que los miembros del personal de TI sigan los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario. Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros. Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.

Identificación de la tarjeta de controles basados en los activos							CC-2N			
Perfil de riesgos							Media			
Categoría de activos							Red			
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de la vulnerabilidad (OP 2.5)	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad							2.6.1			
Integridad					2.4.3					
Disponibilidad		2.1.5								

Un perfil de riesgos medio conlleva la existencia de amenazas que se dan en caso de vulnerabilidades de la red debido a una arquitectura de ésta errónea o deficientemente ejecutada, que puede dar lugar a ataques externos o a accesos internos no autorizados a ciertas áreas de la red de interés moderado o de valor medio para la organización.

La ausencia de seguridad en la red ejerce un efecto inmediato y directo en el funcionamiento de las aplicaciones y en el flujo de información. El riesgo se considera medio cuando el sistema no permite el acceso a componentes fundamentales que podrían afectar directamente a la reputación o la salud financiera de la organización.

Los controles esenciales para la salvaguarda de la confidencialidad, la integridad y la disponibilidad en la red son los que siguen:

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

OP2.4.3 Este control exige que los métodos y mecanismos de control de acceso restrinjan el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.

OP2.1.5 Este control exige que todos los sistemas se encuentren actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.

Identificación de la tarjeta de controles basados en los activos										CC-2P
Perfil de riesgos										Media
Categoría de activos										Personal
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de la vulnerabilidad (OP 2.5)	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad										3.2.1 3.2.2
Integridad										3.2.1 3.2.2
Disponibilidad	1.1.4									

Un perfil de riego medio conlleva la existencia de amenazas que se dan en la gestión de recursos humanos de empresas de mediano tamaño cuando las prácticas de seguridad vigentes pueden dar lugar a problemas empresariales de repercusión moderada.

Los incidentes debidos a un uso indebido de contraseñas o derechos de acceso pueden dar lugar a filtraciones de información. Un nivel medio de confidencialidad de la información determina la escala de riesgo y la pérdida de fondos para la organización.

El seguimiento de las políticas de personal respecto a tales procedimientos garantiza la confidencialidad, la integridad y la disponibilidad de la información.

Los controles esenciales para garantizar la confidencialidad, la integridad y la disponibilidad de la información, en combinación con un activo crítico como las personas, son los que siguen:

OP3.2.1 Este control exige que los miembros del personal apliquen unas buenas prácticas en materia de seguridad: proteger la información de la que son responsables; abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social); disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información; utilizar buenas prácticas en relación con las contraseñas; comprender y observar las políticas y normativas en materia de seguridad; y reconocer e informar de los incidentes que se produzcan.

OP3.2.2 Este control exige que todo el personal, a todas las escalas de responsabilidad, desempeñe las funciones que se le han asignado y asuma sus responsabilidades en lo que atañe a la seguridad de la información.

OP1.1.4 Este control exige que existan políticas y procedimientos documentados para la gestión de visitantes, incluidos los relativos a la firma al acceso, el acompañamiento, los registros de acceso, la recepción y los servicios de hospitalidad.

Identificación de la tarjeta de controles basados en los activos					CC-3A					
Perfil de riesgos					**Baja**					
Categoría de activos					**Aplicación**					
Requisitos de seguridad	**Seguridad física**	**Gestión de sistemas y redes**	**Herramientas de administración de sistemas**	**Seguimiento y auditoría de la seguridad física**	**Autenticación y autorización**	**Gestión de la vulnerabilidad (OP 2.5)**	**Codificación**	**Diseño y arquitectura de seguridad**	**Gestión de incidentes**	**Prácticas de personal generales**
Confidencialidad					2.4.2					
Integridad										
Disponibilidad										

Un perfil de riesgos bajo atañe al almacenamiento y el proceso de información pública o interna, pero sin un grado de significación fundamental que pueda dar lugar a más de una pérdida mínima de fondos. La reputación de la organización no está en juego en este caso. No obstante, deben aplicarse los controles que eviten incluso este tipo de fuga de información y que puedan garantizar el ciclo vital de la información.

Por otra parte, aunque no exista repercusión en cuanto a la confidencialidad, la integridad y la disponibilidad de la información para todo usuario autorizado debe asegurarse.

Un control esencial para la confidencialidad en el activo de aplicaciones es el que sigue:

OP2.4.2 Este control exige que existan políticas y procedimientos de uso de la información documentados respecto al acceso individual y colectivo, con el fin de fijar las normas para la concesión de niveles de acceso apropiados, establecer un derecho inicial de acceso, modificar el derecho de acceso, suspender el derecho de acceso, y revisar y comprobar periódicamente los derechos de acceso.

Identificación de la tarjeta de controles basados en los activos					CC-3S					
Perfil de riesgos					Baja					
Categoría de activos					Sistema					
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de la vulnerabilidad (OP 2.5)	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad		2.1.9			2.4.1					
Integridad					2.4.1					
Disponibilidad		2.1.6								

Un perfil de riesgos bajo implica amenazas de nivel mínimo que conllevan inestabilidades del sistema y dan lugar a la indisponibilidad del servicio empresarial durante un período de tiempo breve.

Los controles basados en el sistema para un perfil de riesgos mínimo comprenden métodos que garantizan una configuración y una funcionalidad del sistema para un acceso apropiado.

La repercusión de la indisponibilidad del sistema no afecta a la reputación de la organización, dado que la información no es privada, ni crítica para ella.

La indisponibilidad del sistema no afecta a la calidad del servicio ni del producto.

El control esencial para la protección de la confidencialidad y la disponibilidad en los sistemas es el que sigue:

OP2.4.1 Este control exige que se utilicen los controles de acceso y la autentificación de usuario pertinentes (p. ej., permisos de archivo, configuración de redes) y coherentes con las políticas establecidas al respecto, con el fin de restringir el acceso de los usuarios a la información, las utilidades del sistema, el código fuente de programas, sistemas sensibles, aplicaciones y servicios específicos, conexiones de red en la organización y conexiones de red con origen fuera de ésta.

OP2.1.6 Este control exige que exista un plan de copias de respaldo de datos documentado que se actualiza de manera rutinaria y se comprueba periódicamente, y exige la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos, así como la comprobación y verificación periódicas de la capacidad para restaurar a partir de tales copias.

OP2.1.9 Este control exige que los miembros del personal de TI sigan los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario. Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros. Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.

Identificación de la tarjeta de controles basados en los activos							CC-3N			
Perfil de riesgos							Baja			
Categoría de activos							Red			
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de la vulnerabilidad (OP 2.5)	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad							2.6.1			
Integridad										
Disponibilidad										

Un perfil de riesgos bajo implica amenazas que se dan en los casos de vulnerabilidades menores en la red, o la indisponibilidad de la información debido a una arquitectura de red errónea o deficientemente ejecutada. En cualquier caso, la repercusión puede considerarse poco significativa, puesto que la información no reviste gran interés, ni se considera altamente confidencial para la organización. Por tanto, la posible pérdida económica para la organización es pequeña.

En cualquier caso, se recomiendan los controles de seguridad que atañen a la información transferida y codificada.

Los controles esenciales para la salvaguarda de la confidencialidad en la red son los que siguen:

OP2.6.1 Este control exige que se utilicen controles de seguridad apropiados para proteger la información sensible durante su almacenamiento y transmisión, incluida la codificación de datos en la transmisión, y en la escritura en disco, el uso de infraestructura pública esencial, la tecnología de redes privadas virtuales, y la codificación para todas las transmisiones basadas en Internet.

Identificación de la tarjeta de controles basados en los activos										CC-3P
Perfil de riesgos										Baja
Categoría de activos										Personal
Requisitos de seguridad	Seguridad física	Gestión de sistemas y redes	Herramientas de administración de sistemas	Seguimiento y auditoría de la seguridad física	Autenticación y autorización	Gestión de la vulnerabilidad (OP 2.5)	Codificación	Diseño y arquitectura de seguridad	Gestión de incidentes	Prácticas de personal generales
Confidencialidad										
Integridad										
Disponibilidad	1.1.4									

Un perfil de riesgos bajo implica amenazas potenciales con una escasa repercusión en la gestión de recursos humanos en los casos en que las prácticas de seguridad vigentes pueden dar lugar a problemas empresariales, pero con un riesgo mínimo para la organización.

El grado de relevancia de la información no es elevado. Por tanto, la repercusión en términos financieros es baja, y la pérdida de dinero puede considerarse poco significativa.

En cualquier caso, el seguimiento de las políticas de personal respecto a tales procedimientos garantiza la confidencialidad, la integridad y la disponibilidad de la información.

El control esencial para garantizar la confidencialidad, la integridad y la disponibilidad de la información, en combinación con un activo como las personas, son los que siguen:

OP1.1.4 Este control exige que existan políticas y procedimientos documentados para la gestión de visitantes, incluidos los relativos a la firma al acceso, el acompañamiento, los registros de acceso, la recepción y los servicios de hospitalidad.

Anexo C. Controles organizativos

Formación y sensibilización en materia de seguridad (SP1)	
SP1.1	Los miembros del personal comprenden sus funciones y responsabilidades en materia de seguridad. Este hecho está documentado y comprobado.
SP1.2	Se dispone de conocimientos técnicos internos adecuados para la totalidad de servicios, mecanismos y tecnologías empleados (p. ej., registro, seguimiento o codificación), incluido el funcionamiento de éstos en condiciones de seguridad. Este hecho está documentado y comprobado.
SP1.3	Se imparten a todo el personal conocimientos y formación y se le envían recordatorios periódicos en materia de seguridad. El conocimiento del personal está documentado, y la conformidad se comprueba periódicamente. La formación comprende los temas que siguen:
	. estrategias, metas y objetivos en materia de seguridad
	. reglamentos, políticas y procedimientos de seguridad
	. políticas y procedimientos de colaboración con terceros
	. planes para contingencias y recuperación en caso de catástrofe
	. requisitos relativos a la seguridad física
	. perspectiva de los usuarios respecto a
	- la gestión de sistemas y redes
	- las herramientas de administración del sistema
	- el seguimiento y la auditoría en lo que atañe a la seguridad física y asociada a las tecnologías de la información
	- autenticación y autorización
	- gestión de vulnerabilidades
	- codificación
	- arquitectura y diseño
	- gestión de incidentes
	- prácticas generales de personal
	- observancia de la legislación, sanciones y actuaciones disciplinarias por infracciones de la seguridad
	- modo de acceder correctamente a la información sensible y trabajo en las áreas en las que ésta es accesible
	- políticas y procedimientos de extinción de la relación laboral en lo que atañe a la seguridad

Estrategia de seguridad (SP2)	
SP2.1	Las estrategias empresariales de la organización incorporan de manera rutinaria consideraciones de seguridad.
SP2.2	En las estrategias y políticas de seguridad se tienen en cuenta las estrategias y objetivos empresariales de la organización.
SP2.3	Las estrategias, metas y objetivos en materia de seguridad se documentan y se revisan, actualizan y comunican periódicamente a la organización.

Gestión de la seguridad (SP3)	
SP3.1	La dirección asigna fondos y recursos suficientes a las actividades de seguridad de la información.
SP3.2	Se definen funciones y responsabilidades en materia de seguridad para todo el personal de la organización.
SP3.3	En las prácticas de la organización en materia de contratación y de extinción de la relación laboral con el personal se tienen en cuenta las cuestiones de seguridad de la información.
SP3.4	Los niveles requeridos de seguridad de la información y el modo en que se aplican a personas y grupos se documentan y aplican.
SP3.5	La organización gestiona los riesgos que atañen a la seguridad de la información, con inclusión de:
	- la evaluación de los riesgos para la seguridad de la información, tanto periódicamente, como en respuesta a cambios significativos en la tecnología, amenazas internas o externas, o los sistemas y operaciones de la organización
	- la adopción de medidas para mitigar los riesgos hasta alcanzar un nivel aceptable
	- el mantenimiento de un nivel de riesgos aceptable
	- la utilización de evaluaciones de riesgos para la seguridad de la información con el fin de facilitar la selección de medidas de seguridad y control rentables, equilibrando los costes de ejecución con las posibles pérdidas
SP3.6	La dirección recibe informes rutinarios, y actúa basándose en ellos, en los que se resumen los resultados de:
	- la revisión de los registros de sistema
	- la revisión de los historiales de auditoría
	- las evaluaciones de vulnerabilidades tecnológicas
	- los incidentes de seguridad y las respuestas dadas a los mismos
	- las evaluaciones de riesgos
	- las revisiones de la seguridad física
	- los planes y recomendaciones para la mejora de la seguridad

Políticas y normativas de seguridad (SP4)	
SP4.1	La organización dispone de un conjunto exhaustivo de políticas vigentes y documentadas que se revisan y actualizan periódicamente. Estas políticas abordan áreas temáticas fundamentales en materia de seguridad, entre las que se cuentan:
	- la gestión y la estrategia de seguridad
	- la gestión de riesgos para la seguridad
	- la seguridad física
	- la gestión de sistemas y redes
	- las herramientas de administración de sistemas
	- el seguimiento y la auditoría
	- la autenticación y la autorización
	- la gestión de vulnerabilidades
	- la codificación
	- la arquitectura y el diseño de la seguridad
	- la gestión de incidentes
	- las prácticas de seguridad de personal
	- la legislación aplicable
	- la sensibilización y la formación
	- la seguridad de la información basada en la colaboración
	- la planificación de contingencias y la recuperación en caso de catástrofe
SP4.2	Existe un proceso documentado para la gestión de políticas de seguridad, incluidas las tareas de:
	- creación
	- administración (incluidas revisiones y actualizaciones periódicas)
	- comunicación
SP4.3	La organización cuenta con un proceso documentado para la evaluación periódica (técnica y no técnica) del cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.
SP4.4	La organización cuenta con un proceso documentado para garantizar el cumplimiento de las políticas de seguridad de la información, la legislación aplicable y los requisitos en materia de seguros.
SP4.5	La organización aplica de manera uniforme sus políticas de seguridad.
SP4.6	Únicamente el personal autorizado puede comprobar y revisar las políticas y procedimientos de seguridad.

Gestión de la seguridad en régimen de colaboración (SP5)	
SP5.1	La organización ha procedido a la documentación, el seguimiento y la ejecución de procedimientos para la protección de su información cuando colabora con entidades externas (p. ej., terceros, colaboradores, subcontratistas o socios).
SP5.2	La organización ha comprobado que los servicios, mecanismos y tecnologías de seguridad externalizados satisfacen sus necesidades y requisitos.
SP5.3	La organización documenta, supervisa y aplica estrategias de protección de la información perteneciente a entidades externas a la que se accede desde componentes de su infraestructura, o que es utilizada por su personal.
SP5.4	La organización ofrece y verifica actividades de sensibilización y formación sobre las políticas y los procedimientos de seguridad de entidades externas para el personal que interactúa con éstas.
SP5.5	Existen procedimientos documentados respecto al personal externo cuya relación con la organización ha concluido, en los que se especifican las medidas de seguridad pertinentes para finalizar su posibilidad de acceso. Estos procedimientos se comunican a la organización externa y se coordinan con ella.

Planificación de contingencias/recuperación en caso de catástrofe (SP6)	
SP6.1	Se ha efectuado un análisis de operaciones, aplicaciones y de la significación de los datos.
SP6.2	La organización ha documentado
	- los planes de continuidad de la actividad empresarial y de operación en casos de emergencia
	- los planes de recuperación en caso de catástrofe
	- los planes de contingencia para la respuesta en casos de emergencia
SP6.3	En los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial se consideran los requisitos y conrtroles de acceso físico y electrónico.
SP6.4	Los planes de contingencia, recuperación en caso de catástrofe, y continuidad de la actividad empresarial se revisan y comprueban periódicamente.
SP6.5	Todo el personal
	- tiene conocimiento de los planes de contingencia, recuperación en caso de catástrofe y continuidad de la actividad empresarial
	- comprende sus responsabilidades y está capacitado para cumplirlas

Anexo D. Controles basados en los activos

Seguridad física (OP1)	
Planes y procedimientos de seguridad física (OP1.1)	
OP1.1.1	Existen planes de seguridad de las instalaciones documentados, concebidos para salvaguardar locales, edificios y cualquier otra área restringida.
OP1.1.2	Estos planes se revisan, comprueban y actualizan periódicamente.
OP1.1.3	Los procedimientos y mecanismos de seguridad física se comprueban y revisan periódicamente.
OP1.1.4	Existen políticas y procedimientos documentados para la gestión de visitantes, que incluyen
	· el registro en la entrada
	· el acompañamiento por las instalaciones
	· los registros de acceso
	· la recepción y los servicios de hospitalidad
OP1.1.5	Existen políticas y procedimientos documentados para el control físico del hardware y el software, incluidos
	· terminales, portátiles, módem, componentes inalámbricos y todos los demás elementos utilizados para acceder a la información
	· el acceso, el almacenamiento y la recuperación de copias de seguridad de datos
	· el almacenamiento de información sensible en medios físicos y electrónicos
	· la supresión de información sensible, o de los medios en los que se encuentra almacenada
	· la reutilización y el reciclaje de papel y medios electrónicos.
Control de acceso físico (OP1.2)	
OP1.2.1	Existen políticas y procedimientos documentados respecto al acceso individual y en grupo, que comprenden:
	· las normas de concesión del nivel pertinente de acceso físico
	· las normas para la determinación de los derechos iniciales de acceso
	· la modificación del derecho de acceso
	· la anulación del derecho de acceso
	· la revisión y la comprobación periódicas de los derechos de acceso
OP1.2.2	Existen políticas, procedimientos y mecanismos documentados para controlar el acceso físico a entidades definidas. Se incluyen aquí:
	· áreas de trabajo
	· medios de hardware (ordenadores, dispositivos de comunicación, etc.) y de software
OP1.2.3	Existen procedimientos documentados para verificar la autorización de acceso antes de autorizar el acceso físico.
OP1.2.4	Los terminales y otros componentes que permiten el acceso a información sensible se encuentran físicamente protegidos con el fin de evitar accesos no autorizados.
Seguimiento y auditoría de la seguridad física (OP1.3)	
OP1.3.1	Se conservan registros de mantenimiento para documentar las reparaciones y modificaciones de los componentes físicos de las instalaciones.
OP1.3.2	Pueden justificarse las acciones de una persona o de un grupo respecto a la totalidad de medios controlados físicamente.
OP1.3.3	Se examinan regularmente registros de auditoría y seguimiento para detectar anomalías, y se emprenden acciones correctivas en caso necesario.

Seguridad de las tecnologías de la información (OP2)	
Gestión de sistemas y redes (OP2.1)	
OP2.1.1	Existen planes de seguridad documentados para la salvaguarda de sistemas y redes.
OP2.1.2	Los planes de seguridad se revisan, comprueban y actualizan periódicamente.
OP2.1.3	Se protege la información sensible mediante su almacenamiento en condiciones de seguridad, como el que proporcionan
	· las cadenas de custodia definidas
	· las copias de respaldo almacenadas fuera de las instalaciones
	· los medios de almacenamiento separables
	· un proceso de eliminación de la información sensible o de sus medios de almacenamiento
OP2.1.4	La integridad del software instalado se verifica regularmente.
OP2.1.5	Todos los sistemas se encuentran actualizados respecto a revisiones, parches, y recomendaciones en documentos de asesoramiento sobre seguridad.
OP2.1.6	Existe un plan de copias de respaldo de datos que
	· se actualiza regularmente
	· se comprueba periódicamente
	· requiere la realización de copias de respaldo programadas regularmente, tanto del software, como de los datos
	· requiere la comprobación y verificación periódicas de la capacidad para restaurar a partir de copias de respaldo
OP2.1.7	Todo el personal comprende y es capaz de desempeñar sus responsabilidades con arreglo a los planes de respaldo.
OP2.1.8	Los cambios del hardware y el software de las TI se planifican, supervisan y documentan.
OP2.1.9	Los miembros del personal de TI siguen los procedimientos pertinentes al publicar, modificar y anular contraseñas, cuentas y privilegios de usuario.
	· Se requiere una identificación única de usuario para todos los usuarios del sistema de información, incluidos los usuarios terceros.
	· Las cuentas y contraseñas por defecto han sido suprimidas de los sistemas.
OP2.1.10	Sólo operan en los sistemas los servicios necesarios; todos los innecesarios se han suprimido.
Herramientas de administración de sistemas (OP2.2)	
OP2.2.1	Los nuevos instrumentos de seguridad, procedimientos y mecanismos se revisan de manera ordinaria para determinar su aplicabilidad en la consecución de las estrategias de seguridad de la organización.
OP2.2.2	Las herramientas y los mecanismos para conseguir el uso de una administración de sistemas y de red segura, y su revisión y actualización o sustitución con carácter periódico. Son ejemplos de estas herramientas los que siguen:
	· comprobadores de la integridad de los datos
	· herramientas de codificación
	· escáneres de vulnerabilidades
	· herramientas de comprobación de la calidad de las contraseñas
	· escáneres de virus
	· herramientas de gestión de procesos
	· sistemas de detección de intrusos

	· administraciones remotas seguras
	· herramientas de servicio de red
	· analizadores de tráfico
	· herramientas de respuesta en caso de incidente
	· herramientas forenses para el análisis de datos
Seguimiento y auditoría de seguridad de las TI (OP2.3)	
OP2.3.1	La organización utiliza de manera ordinaria herramientas de seguimiento y auditoría de sistemas y redes.
	· La actividad es objeto de seguimiento por parte del personal de TI.
	· Se registra la actividad de sistemas y redes.
	· Los registros se revisan regularmente.
	· La actividad inusual se trata con arreglo a la política o el procedimiento pertinentes.
	· Las herramientas se revisan y actualizan periódicamente.
OP2.3.2	Los cortafuegos y otros componentes de seguridad se auditan periódicamente para determinar su conformidad con la política pertinente.
Autenticación y autorización (OP2.4)	
OP2.4.1	Se utilizan controles de acceso y mecanismos de autenticación de usuario apropiados (p. ej., permisos de archivo, configuración de red) coherentes con la política establecida al respecto, con el fin de restringir el acceso de los usuarios a
	· la información
	· las utilidades del sistema
	· el código fuente de programas
	· los sistemas sensibles
	· determinadas aplicaciones y servicios
	· conexiones de red en la organización
	· conexiones de red con origen fuera de la organización
OP2.4.2	Existen políticas y procedimientos de uso de la información documentados respecto al acceso individual y en grupo con el fin de:
	· establecer las normas de concesión del nivel pertinente de acceso
	· establecer un derecho inicial de acceso
	· modificar el derecho de acceso
	· anular el derecho de acceso
	· revisar y comprobar periódicamente los derechos de acceso
OP2.4.3	Los métodos y mecanismos de control de acceso restringen el acceso a los recursos con arreglo a los derechos determinados en políticas y procedimientos.
OP2.4.4	Los métodos y mecanismos de control de acceso se revisan y comprueban periódicamente.
OP2.4.5	Se dotan métodos o mecanismos para garantizar que la información sensible no es objeto de acceso, alteración o destrucción de un modo no autorizado.
OP2.4.6	Se utilizan mecanismos de autenticación para proteger la disponibilidad, integridad y confidencialidad de la información sensible. Son ejemplos de estos instrumentos los que siguen:
	· las firmas digitales
	· la biometría

Gestión de vulnerabilidades (OP 2.5)	
OP2.5.1	Existe un conjunto documentado de procedimientos para la gestión de vulnerabilidades, entre los que figuran:
	· la selección de herramientas de evaluación de vulnerabilidades, listas de comprobación y *scripts*
	· el mantenimiento al día respecto a los tipos de vulnerabilidades conocidos y los métodos de ataque
	· la revisión de fuentes de información sobre anuncios de vulnerabilidad, alertas de seguridad y notificaciones
	· la identificación de componentes de infraestructura para su evaluación
	· la programación de evaluaciones de vulnerabilidad
	· la interpretación de resultados y la respuesta a éstos
	· el mantenimiento de un almacenamiento seguro y la disposición de datos sobre vulnerabilidad
OP2.5.2	Los procedimientos de gestión de vulnerabilidades son objeto de seguimiento, así como de revisiones y actualizaciones periódicas.
OP2.5.3	Las evaluaciones de vulnerabilidad de la tecnología se realizan de manera periódica, y las vulnerabilidades se tratan cuando se detectan.
Cifrado (OP2.6)	
OP2.6.1	Se utilizan controles de seguridad apropiados para proteger la información sensible durante su almacenamiento o transmisión, incluidos
	· el cifrado de datos durante la transmisión
	· el cifrado de datos al escribir en disco
	· el uso de infraestructura de claves públicas
	· la tecnología de redes privadas virtuales
	· el cifrado de todas las transmisiones a través de Internet
OP2.6.2	Se utilizan protocolos cifrados cuando se gestionan de manera remota sistemas, enrutadores y cortafuegos.
OP2.6.3	Los controles y protocolos de cifrado se someten a revisiones y comprobaciones periódicas.
Diseño y arquitectura de seguridad (OP2.7)	
OP2.7.1	En la arquitectura y el diseño de sistemas nuevos y revisados se tienen en cuenta
	· las estrategias, políticas y procedimientos de seguridad
	· el historial de situaciones de riesgo en materia de seguridad
	· los resultados de las evaluaciones de riesgos para la seguridad
OP2.7.2	La organización dispone de diagramas actualizados que muestren la tipología de red y la arquitectura de seguridad del conjunto de la empresa.

Seguridad del personal (OP3)	
Gestión de incidentes (OP 3.1)	
OP3.1.1	Existen procedimientos documentados para la identificación de presuntos incidentes e infracciones de seguridad, así como para la elaboración de informes al respecto, y para la adopción de respuestas a los mismos, entre los que figuran:
	· los incidentes que atañen a las redes
	· los incidentes relativos al acceso físico
	· los incidentes de ingeniería social
OP3.1.2	Los procedimientos de gestión de incidentes se comprueban, verifican y actualizan periódicamente.
OP3.1.3	Existen políticas y procedimientos documentados respecto a la colaboración con los órganos encargados de velar por el cumplimiento de las leyes.
Prácticas de personal generales (OP3.2)	
OP3.2.1	Los miembros del personal se atienen a buenas prácticas en materia de seguridad, como las que siguen:
	· asegurar la información respecto a la que son responsables
	· abstenerse de divulgar información sensible a terceros (resistencia a la ingeniería social)
	· disponer de la capacidad adecuada para utilizar los equipos y el software de las tecnologías de la información
	· utilizar buenas prácticas en lo que se refiere a las contraseñas
	· comprender y observar las políticas y reglamentos de seguridad
	· reconocer los incidentes e informar de éstos
OP3.2.2	Todo el personal, a todas las escalas de responsabilidad, desempeña las funciones que se le han asignado y asume sus responsabilidades en lo que atañe a la seguridad de la información.
OP3.2.3	Existen procedimientos documentados para autorizar y supervisar a aquéllos que manejan información sensible o trabajan en emplazamientos en los que se deposita la misma. Se trata de:
	· empleados
	· contratistas, socios, colaboradores, y personal de entidades terceras
	· personal de mantenimiento de sistemas
	· personal de mantenimiento de instalaciones

Anexo E. Consejos sencillos[4]

RECOMENDACIONES IMPORTANTES EN MATERIA DE SEGURIDAD PARA PEQUEÑAS Y MEDIANAS EMPRESAS

A continuación se exponen las bases que le permitirán defender su empresa

- ☐ Ejecutar controles y exámenes básicos de todos sus empleados y contratistas (p. ej., basados en referencias o recomendaciones).
- ☐ Conocer y documentar los activos de valor de su organización.
- ☐ Disponer de políticas y procedimientos de seguridad breves, eficaces y claramente documentados.
- ☐ Impartir a sus empleados formación básica para la sensibilización en materia de seguridad.
- ☐ Aplicar parches a las vulnerabilidades de software de manera automática, o tan pronto como sea posible, después de comprobar su funcionalidad.
- ☐ Saber quién accede a sus sistemas y por qué.
- ☐ Utilizar contraseñas seguras y modificar éstas periódicamente.
- ☐ Asegurarse de aplicar funciones de antivirus en todos sus equipos informáticos y móviles, y de que su sistema antivirus se actualiza automáticamente.
- ☐ Utilizar diferentes productos antivirus para su servidor y sus ordenadores clientes.
- ☐ Utilizar un sistema de filtrado de contenidos para protegerse del *spam* o envío de correo no deseado, del *phishing*, y de los contenidos malintencionados y prohibidos.
- ☐ Utilizar cortafuegos, sobre todo si dispone de un acceso a Internet de banda ancha.
- ☐ Utilizar un sistema de defensa de red "todo en uno" en el caso de redes de pequeño tamaño.

Contraseñas

Son las claves de acceso a su información electrónica. Cuando la información no está protegida por contraseñas, cualquiera puede acceder a ella. Si se utiliza una contraseña demasiado fácil, es muy posible que alguien las adivine o las descifre. A continuación figuran algunos consejos para la utilización de contraseñas seguras.

- Abra el diccionario por cualquier página al azar y seleccione una palabra larga (por ejemplo, de cuatro sílabas). Utilice esta palabra, pero introduzca el número de página en medio de la misma. Por ejemplo, si "multiforme" figura en la página 345 de su diccionario, su contraseña quedaría así: "multi345forme". (Si olvida la contraseña, ha de ser capaz de recordar qué página seleccionó.)
- Elija una "*pass phrase*" o fase privada que tenga algún significado para usted. Por ejemplo, "mi cebra se llama Spot y tiene 9 años". Ésta se puede

[4] El objeto del presente anexo es orientar de manera sencilla a los usuarios sobre las cuestiones básicas de seguridad. Su contenido se ha extraído de las fuentes [1], [6] y [10] mencionadas en la bibliografía.

transformar en una contraseña así: "mcslS&t9a". Se trata de una contraseña muy segura, puesto que utiliza letras, cifras y caracteres especiales. Descifrarla resultará extremadamente difícil.

Para que una contraseña sea útil es absolutamente necesario:

- utilizar al menos 8 caracteres;
- modificar las contraseñas regularmente, por ejemplo, cada mes;
- si un empleado abandona la empresa, modificar su antigua contraseña de inmediato;
- utilizar una contraseña para cada aplicación; no emplear nunca la misma para todo.

Por otro lado, hay cosas que debe evitar en cualquier caso con las contraseñas.
A saber:

- nunca anote una contraseña;
- no utilice nunca su nombre, ni el de su socio, ni el de los niños, ni la matricula del coche, ni cumpleaños ni cualquier otra cosa relativa a usted o a su familia que sea bien conocida o pueda deducirse fácilmente con un poco de "ingeniería social";
- no utilice nunca códigos especiales de cosas suyas, como su número de teléfono, su número de la seguridad social, el número de licencia del software en cuestión, o todo aquello que pueda ser deducido por alguien;
- evite en todo caso los mismos números o letras, por ejemplo "11111111" en una contraseña, y no emplee nunca la palabra "contraseña", porque ésa es la primera que el *hacker* probará;
- no comparta nunca su contraseña con otros;
- no utilice nunca una contraseña por defecto propuesta por un programa informático; cámbiela;
- no utilice funciones de "recordar contraseña" en un ordenador, puesto que las contraseñas almacenadas de este modo son fácilmente recuperables con un poco de destreza.

En resumen, trate sus contraseñas con cuidado. Opte por una segura, modifíquela regularmente y protéjala adecuadamente.

Virus, gusanos y troyanos

Los puristas dirían que se trata de amenazas diferentes, pero, desde una perspectiva empresarial, pueden tratarse como el mismo tipo de peligro. Lo importante es que todos ellos pueden causar, y causan de hecho, daños en los ordenadores y en la información almacenada en éstos. Sin embargo, resulta verdaderamente sencillo evitarlos. Utilice programas antivirus. Cualquier software de este tipo servirá, porque todos funcionan más o menos del mismo modo y cumplen el mismo tipo de función. Lo más importante es, sencillamente, utilizar uno.

Lo que la mayoría no tiene en cuenta es que los programas informáticos antivirus deben actualizarse. Es necesario aplicar actualizaciones diarias (sí, diarias), porque los que escriben este tipo de software publican nuevas versiones cada día.

Si no instala el software pertinente y lo mantiene actualizado, existe un 100% de posibilidades de que resulte infectado por un virus, tarde o temprano.

Sea cual fuere el programa antivirus que utilice, debe instalarlo de modo que compruebe cualquier dato nuevo de manera automática. De este modo, si usted recibe datos nuevos en un disquete, un CD o a través de Internet, se comprobará si contienen virus antes de que puedan causar ningún daño.

Una regla de oro en este terreno es que todo archivo o dato infectado por un virus ha de ser destruido. Algunos programas antivirus afirman que son capaces de "desinfectar" archivos, pero esta opción nunca está garantizada. La apuesta más segura consiste en destruir el archivo que contiene el virus. Si se trata de un mensaje de correo electrónico, elimínelo en todo caso sin ni siquiera llegar a abrirlo.

Spam

Tal vez piense que se trata únicamente de una molestia, pero, por desgracia, también conlleva peligros. El *spam* o correo electrónico no deseado puede:

- Constituir una vía de acceso para el fraude;
- Consistir en cadenas de mensajes malintencionados;
- Contener un código oculto capaz de alterar la configuración de su ordenador (p. ej., dirigiéndole a un sitio porno en la Red);
- Contener un código oculto que convierta a su ordenador en un centro emisor de *spam* (es decir, que un gran volumen de *spam* se envíe desde su ordenador a todo el mundo), enviando de este modo las direcciones de todos sus clientes por todo el mundo, ¡y con una nueva copia del spam, el gusano o el troyano adjunto al envío!.

En el caso de un código oculto, éste muy probablemente se incluya en la categoría de "troyano", y es muy posible que sea detectado por su software antivirus. No obstante, existen ciertas reglas que ha de seguir en lo que se refiere al *spam* cuyo cumplimiento le permitirá reducir los riesgos al mínimo.

- Si el mensaje de correo electrónico es claramente inútil, no le atañe, ni a usted ni a su empresa, está muy mal escrito, etc., limítese a suprimirlo sin ni siquiera llegar a abrirlo.
- Nunca responda a mensajes de correo del tipo *spam*. Su dirección de correo electrónico ha sido obtenida de algún modo, y los creadores de *spam* no saben si usted existe en realidad o no.
- Si responde, confirmará su existencia y comenzará a recibir mucho más *spam*.
- No haga clic en ningún botón con un mensaje del tipo "haga clic aquí para eliminar su nombre de nuestra lista de correo" incluido en el correo electrónico. Normalmente, es un truco. No se le eliminará de la lista, y estará confirmando su existencia.
- Comunique su dirección de correo electrónico únicamente a personas en las que pueda confiar.
- Esta norma es muy difícil de cumplir cuando se gestiona una empresa, puesto que lo que se quiere es que la dirección de correo electrónico esté disponible para el mayor número posible de personas. Piense en la posibilidad de tener dos direcciones de correo electrónico: una de disponibilidad pública, y otra para su uso personal y sujeta a un control estricto.
- Si un sitio de Internet le pide su dirección de correo electrónico, realice una rápida evaluación de riesgos. ¿Se trata de una organización legítima con una reputación consolidada? ¿Es alguien del que nunca ha oído hablar antes, o que no consigna una dirección física de su empresa en su sitio *web*? Recuerde que los delincuentes tratan de pasar por empresas legítimas.
- Los sitios de Internet que prometen eliminarle de sus listas de correo electrónico de tipo *spam*, generalmente, incumplen su promesa. No los utilice nunca.

También se puede bloquear el *spam*. Existe software especializado en ello, pero puede resultar demasiado caro para las pequeñas empresas. Probablemente merezca la pena

preguntar a su proveedor de servicios de Internet (ISP) si pueden, por una pequeña cuota adicional, prestarle un servicio de bloqueo de *spam* sirviéndose de sus propios recursos. En cualquier caso, hay que obrar con prudencia en este terreno: el bloqueo de *spam* es tanto un arte como una ciencia. Se pueden bloquear mensajes de correo legítimos si se fijan unos criterios *antispam* demasiado rigurosos.

N.B. Si recibe un mensaje de correo electrónico en el que se amenaza directamente a su empresa de cualquier modo, por ejemplo, con un posible chantaje, póngase en contacto con la policía de su zona, de inmediato. Rápidamente le remitirán a un equipo instruido para tratar amenazas electrónicas. Es poco probable que esto le suceda, pero por si acaso...

Spyware

Se trata de pequeños programas que se introducen en el sistema informático con el fin de recabar información de manera encubierta acerca del usuario o de la empresa en cuestión, sin que éstos sean conscientes de lo que sucede. Estos programas actúan mayoritariamente con fines de publicidad, pero también pueden recabar información sobre direcciones de correo electrónico, e incluso contraseñas y datos de tarjetas de crédito.

Recientemente se ha alertado oficialmente acerca del *spyware* que se utiliza para obtener información comercialmente "sensible", como los datos relativos a contratos.
Estos programas no son una buena idea, y el usuario prudente tratara de restringirlos, o de eliminarlos por completo. Existen dos paquetes eficaces disponibles en Internet y capaces de suprimir este tipo de programas. Ambos son gratuitos para uso personal, y de pago en el caso de las empresas. Son los siguientes:

- Lavasoft's <Ad-aware>
- Spybot

Se recomienda su descarga y ejecución, al menos una vez a la semana. Le sorprenderá lo que son capaces de encontrar. (Y no lo olvide, ¡también es necesario actualizarlos!)

Cortafuegos

Toman su nombre de las barreras físicas construidas en los edificios para evitar la propagación de incendios. En términos informáticos, un cortafuego es un elemento que actúa como barrera para impedir el acceso no autorizado con origen o destino en un sistema informático privado. Puede considerarse como una especie de puerta de seguridad y alarma antirrobo para ordenadores, que ayuda a reducir todas las amenazas deliberadas señaladas anteriormente. Actualmente, los cortafuegos se consideran esenciales si se dispone de uno o varios ordenadores conectados a Internet.

El cortafuegos puede consistir en un programa informático, o en un elemento de hardware. Cuando se trata de proteger grandes sistemas informáticos, puede corresponder a una combinación de software y hardware.

Su aspecto más destacado es que el cortafuegos comprobará todos los datos que entran en el ordenador, e incluso también los que salen, con el fin de asegurarse de su legitimidad. En resumen: un cortafuegos constituye su mejor defensa contra los *hackers* o piratas informáticos. Tomando un caso de la vida real, un cortafuegos puede impedir que su ordenador pase a ser controlado por un tercero y configurado como unidad de difusión de correo electrónico de tipo *spam*. Cabe recordar que, cuando se conecta un ordenador a Internet, se abren 65.536 "puertas" (técnicamente, "puertos") a través de los que los datos pueden acceder a su equipo. Lo que necesita en realidad en este caso es tener abiertos los puertos pertinentes únicamente para enviar o recibir datos, y que se mantengan cerrados el resto del tiempo.

Se trata de un área muy compleja de la informática, y no es éste el lugar oportuno para exponer sus principios y prácticas, que son objeto de tesis doctorales. Por suerte,

actualmente, el software de cortafuegos no es muy caro, resulta sencillo de aplicar, y puede obtenerse con facilidad.
Si tiene un ordenador, compre un programa de cortafuegos. Su instalación es sencilla. Basta con aceptar su configuración por defecto. Si dispone de dos o más ordenadores conectados a Internet, es posible que un cortafuegos de hardware constituya una mejor inversión, y puede instalarse entre el conjunto de sus ordenadores y el cable de conexión a la Red. Los cortafuegos de hardware son más complejos, y es preferible que se lo instale y configure un experto. Un profesional procurará que su cortafuegos no sea tan seguro que no le permita siquiera conectarse a Internet.

(Las empresas con uno o dos ordenadores pueden adquirir una solución combinada de software cortafuegos y antivirus en un solo paquete. Esta opción presenta ventajas económicas y técnicas para las pequeñas empresas.)

Parches

Los parches son poco conocidos, pero son muy importantes y se usan contra los virus y las actividades de pirateo informático. Todo software tiene sus problemas y defectos. En la mayoría de los casos, los defectos son tan poco importantes que pueden pasarse por alto y, probablemente, no tendrán ninguna repercusión en la empresa. Sin embargo, algunos defectos son demasiado importantes para pasarlos por alto.

Todos los productores de software ofrecen parches, es decir, actualizaciones diseñadas para eliminar problemas de sus programas. Si usted dispone de un solo ordenador, y éste no está conectado a ningún otro elemento (como otro ordenador, Internet, etc.), es probable que no necesite preocuparse por los parches mientras su equipo funcione sin problemas.

Las cuestiones que se refieren a continuación atañen fundamentalmente al sistema operativo del ordenador, es decir, al programa básico que hace posible el funcionamiento general del equipo. Seguramente utiliza usted alguna versión de Microsoft Windows, quizá el OSX de Apple, o acaso Unix/Linux. Todos estos sistemas operativos requieren de algún parche cada cierto tiempo. Pero muchas aplicaciones también requieren de parches en ocasiones. Los navegadores de Internet y los paquetes de gestión de correo electrónico necesitan parches a menudo, y no es infrecuente que los paquetes de contabilidad comunes requieran asimismo un parche.

Si no mantiene los parches de su software al día, se arriesga a que estos programas fallen o, en el caso de los navegadores o los programas de correo electrónico, permitan la entrada de software malintencionado que corromperá su equipo, o de usuarios igualmente malintencionados que se harán con el control de su ordenador.

La mayoría de los fabricantes de software ofrecen un servicio de notificación a través del correo electrónico para comunicar a sus clientes la publicación de nuevos parches. Normalmente, establecen en estos avisos prioridades respecto a la aplicación del parche: desde la máxima urgencia, a la posibilidad de ejecución en cualquier momento. Si recibe un aviso relativo a un parche fundamental que afecta a un programa informático del que depende su empresa, debe instalarlo a la mayor brevedad posible. La continuidad de su negocio puede depender de ello. Consulte asimismo el sitio *web* de su proveedor de software para conocer las noticias de nuevas actualizaciones.

Actualmente, la mayoría de los fabricantes de software ofrecen actualizaciones automáticas a través de Internet.

Copias de respaldo

Un *backup* es el proceso de copia de datos electrónicos, como por ejemplo de los archivos contables. ¿Qué sentido tiene? Es muy fácil que los datos electrónicos se pierdan, se

extravíen o se destruyan. Si pierde la única copia de sus cuentas electrónicas, ¿cómo gestionará su negocio mañana?

Un régimen reglado y eficaz de copias de respaldo puede evitar muchas de las amenazas naturales o involuntarias esbozadas anteriormente. Pueden copiarse los datos esenciales en:

- cinta (un método antiguo, pero que cabe aún considerar, puesto que permite su constante reutilización);
- un disco duro duplicado (preferiblemente, uno separable);
- un CD (c. 700 Mb) o un DVD (c. 4,3 Gb).

Debe considerar la realización de varias copias de respaldo de datos esenciales utilizando tres generaciones de medios. Por ejemplo, conservar los datos de "final de semana" de las tres últimas semanas en un ciclo continuo, de modo que siempre disponga de las copias de respaldo de tres semanas (o generaciones), en caso de que se necesite recrear el sistema. Un régimen adecuado de copias de respaldo para una empresa (incluso para un comerciante autónomo) sería el que sigue:

- al cierre de cada jornada: copia de seguridad de todos los archivos modificados ese día;
- al cierre de cada semana: copia de seguridad de todas las aplicaciones (cuentas, correspondencia, etc.);
- a final de cada mes: copia de seguridad del sistema operativo también.

Si tuviera que reconstruir el sistema informático después de un "fallo catastrófico", utilizará la última copia de seguridad de "final de mes" para recrear el sistema operativo. A continuación, restaurará la última copia de respaldo de aplicaciones de "final de semana".
Por último, restaurará cada una de las copias de seguridad de "final de jornada" realizadas tras el último "final de semana". De este modo, habrá reconstruido el sistema por completo. Si alguna de las copias de respaldo no pudiera leerse (un suceso sorprendentemente común con independencia del medio de respaldo utilizado), podrá volver a la copia previa de las tres realizadas y comenzar desde ésta. En este caso, es poco probable que restaure hasta el último de sus archivos de datos. Inevitablemente, algo se perderá en los medios fallidos. No obstante, es preferible a perder todos sus valiosos datos.

Este tipo de régimen de copias de seguridad se ha utilizado desde que se inventaron los ordenadores, y se ha comprobado con el tiempo que resulta fiable. Pueden utilizarse regímenes más complejos en casos en los que los datos cambian con rapidez o tienen un valor muy alto. Prepárese a cambiar si cambian los riesgos que afectan a su empresa.

Mantenga sus copias de respaldo en condiciones de seguridad. Son tan valiosas como sus datos originales, y se someten a los mismos principios de arquitectura de la información (AI). No los deje donde puedan ser robados o dañados. Tampoco los deposite encima del ordenador. Si su equipo estalla o se quema, ¿qué ocurrirá con sus copias de seguridad? Lo ideal sería que mantenga estas copias en un edificio distinto a aquél en el que se encuentra su ordenador. Si la oficina sufre un incendio, ¡no querrá que sus copias de seguridad tengan el mismo destino!

Es importante no olvidarse de etiquetar convenientemente con la fecha y el asunto las copias de seguridad. De no hacerse así, puede haber problemas cuando se necesita la copia con urgencia...

Si dispone de un gran número de copias de respaldo en diversos medios, una opción consiste en adquirir una caja de seguridad a prueba de incendios. Estas cajas pueden mantenerse en las instalaciones de la empresa, pero debe tener en cuenta que, después

de un incendio importante, pueden pasar de dos a tres días hasta que la temperatura de la caja en cuestión baje lo suficiente para que pueda abrirse.

Robo de información e identidad

Se trata de uno de los delitos de más rápido crecimiento tanto en el Reino Unido como en otros países desarrollados. Se le ha dado mucha publicidad, pero no se ha mencionado un aspecto importante. Los robos de información e identidad, además de a las personas físicas, pueden afectar a las empresas.

Para una empresa, es fundamental que la información antigua se elimine de una manera segura, tanto la que se conserva en papel como en formato electrónico. No sería la primera vez que una pequeña empresa con su propio sitio en Internet ve secuestrada su *web* por alguien que ha robado un antiguo documento con membrete y se ha encontrado con las firmas de los directivos. Éstas se utilizan para falsificar cartas dirigidas a los órganos de registro de nombres de Internet, con el fin de que el sitio *web* en cuestión sea registrado nuevamente con una nueva dirección física. De este modo se constituye una empresa fraudulenta, y se obtienen créditos para sociedades.

Las personas físicas también pueden padecer el robo de su identidad con fines fraudulentos. Aunque una persona no será responsable de un fraude claramente perpetrado por terceros, el problema después de un robo de identidad es recuperar la credibilidad ante los bancos y otras entidades financieras, y en especial, ante las agencias de calificación de la solvencia crediticia.
Algunas acciones a evitar:

- No dar nunca datos personales a través de Internet, el correo electrónico, el teléfono o por carta a nadie, salvo que tenga certeza previa de que se puede confiar en el destinatario de la información;
- Recuerde que los bancos nunca piden a sus clientes que confirmen sus contraseñas o códigos de acceso por correo electrónico, por lo que debe abstenerse de facilitar tal información;
- No se deshaga de documentos empresariales o personales confidenciales sin destruirlos antes y, si es posible, utilice una trituradora que corte en dos pasadas (en vertical y en diagonal);
- Los materiales electrónicos o magnéticos que ya no sean necesarios deben inutilizarse físicamente, de modo que no puedan volver a usarse;
- Si mantiene cuentas bancarias de empresa o líneas de crédito sin utilizar con antiguos proveedores, délas de baja, porque podrían ser explotadas con fines fraudulentos.

En cualquier caso, debe comprobar sus extractos bancarios y otros documentos financieros línea por línea tan pronto como los reciba. Todo pago o cargo que le resulte extraño debe investigarse de inmediato. A su banco no le importará que le consulte. Tienen tanto interés como usted en evitar los fraudes. Otra tarea consiste en cotejar periódicamente sus registros de crédito personal o empresarial con el fin de detectar cualquiera de los hechos imprevistos que se refieren a continuación:

- consultas acerca de su calificación de solvencia crediticia por parte de empresas con las que nunca ha tratado;
- comentarios despectivos acerca de su calificación;
- notificaciones de cambio de domicilio; o
- referencias a sentencias judiciales, etc.

Redes inalámbricas

Las redes inalámbricas (wifi para abreviar) son muy atractivas para las pequeñas empresas. Su instalación no es muy cara, resultan fáciles de configurar, ofrecen flexibilidad y atenúan la necesidad de un cableado de datos difícil y costoso. Por desgracia, también es muy sencillo crear una red wifi que permita a cualquiera acceder a los datos confidenciales de su empresa.

El mayor riesgo es que cualquiera en el área de alcance inalámbrico pueda utilizar su red wifi. Pueden utilizar su conexión a Internet de manera gratuita, acceder a su tráfico de datos, por ejemplo, a sus correos electrónicos, contraseñas, o archivos de datos de acceso en sus ordenadores, o incluso fisgonear sus datos bancarios de Internet. Una red wifi insegura plantea un gran riesgo de espionaje industrial.

El establecimiento de una red wifi en su empresa requiere una planificación cuidadosa y, probablemente, necesitará de la ayuda de expertos en el tema. La presente nota no puede constituir una guía completa para la creación de redes. Lo importante en este caso es que una red wifi puede y debe establecerse de una manera segura, de modo que sólo su personal y usted puedan utilizarla y acceder y compartir sus datos. A continuación figuran algunos consejos básicos.

En primer lugar, por desgracia, algunas notas técnicas relevantes. Todas las redes wifi deben atenerse a la norma IEEE 802.11. Existen varios subapartados de dicha norma. Los importantes para usted son los denominados 802.11G y 802.11N. "G" está aquí ya, y a "N" le queda un poco todavía para llegar. A efectos empresariales, opte ahora por "G", aunque ya están a la venta los denominados "kits pre N", porque cabe la posibilidad de que éstos no cumplan plenamente con la norma "N" definitiva. "N" ofrece velocidades de transmisión mucho más rápidas y, potencialmente, mejor seguridad. No caiga en la tentación de las variantes "A" o "B", ya obsoletas, puesto que se trata de opciones más lentas y menos seguras.

No haga caso de lo que el fabricante dice sobre las prestaciones. Lo normal es que obtenga la mitad de la velocidad de transmisión y con la mitad de distancia, a no ser que opere en condiciones de laboratorio. El tipo de construcción puede ejercer un efecto inequívoco en el rendimiento de las redes wifi, y las edificaciones en piedra son las que experimentan mayores problemas.

Necesitará:

- Un enrutador inalámbrico que transmita y reciba la emisión de señales de datos por toda la oficina. Los más sofisticados pueden ajustarse de modo que la señal se limite para cubrir únicamente su edificio;
- Una conexión de banda ancha, si no dispone ya de una;
- Un adaptador inalámbrico para cada ordenador. La mayoría de los portátiles modernos lo traen incorporado, pero los ordenadores de sobremesa necesitarán la instalación de uno. Se recomiendan los adaptadores inalámbricos que se conectan directamente en un puerto USB.

En los casos en que la empresa cuenta con un servidor central de archivos preinstalado, con una conexión a Internet establecida, el enrutador se conectará directamente a dicho servidor. Las oficinas pequeñas pueden adquirir un enrutador con un módem de banda ancha incorporado. Pueden comprarse "cajas negras" más complejas que combinan el enrutador con un cortafuegos para añadir protección. Un buen consejo es adquirir todos los dispositivos wifi al mismo fabricante. No mezcle y combine porque, si algo no funciona, los proveedores se culparán entre sí. Y, por supuesto, no compre marcas desconocidas.

Las notas técnicas que siguen son esenciales para la seguridad:

- Todas las transmisiones de datos deben cifrarse; no utilice el cifrado WEP: prefiera el WPA o WPA2;
- Utilice claves precompartidas (PSK) para crear un formulario de contraseña entre sus ordenadores y el enrutador. Se recomienda que opte por una clave larga;
- Cree una denominación única para su red wifi mediante los *Service Set Identifiers* (SSID). Cree un nombre seguro e inventado;
- Configure su enrutador wifi de modo que su SSID no se emita;
- No utilice nunca la denominación SSID por defecto del fabricante;
- Registre las direcciones MAC de los ordenadores de su oficina con el enrutador, y cree la norma de que sólo las direcciones MAC registradas puedan comunicarse con él;
- Asegúrese de que su servidor y los sistemas operativos de otros ordenadores sean compatibles con la red wifi antes de adquirir los dispositivos inalámbricos.

Si todo esto le parece un tanto difícil, no intente hacerlo por su cuenta. Solicite a un experto que le instale su red wifi. No olvide que sus datos constituyen probablemente su activo más importante, y han de protegerse con una red wifi segura. Después de todo, lo que quiere no es convertir su red en un punto de acceso público.

Terceros

Con notable frecuencia, se da intervención a terceros en diversas actividades empresariales de las PYME. Entre las relaciones más habituales figuran la consultoría sobre gestión y empresarial y marketing, así como la prestación de asistencia en materia de TI respecto a sistemas esenciales. Muy a menudo, se concede a estos agentes el acceso a información confidencial de la empresa, o a sistemas e infraestructuras de red con fines de mantenimiento. Es fundamental que las empresas garanticen la confidencialidad de esta información, tanto por contrato, como a través de un proceso adecuado de gestión del control de acceso. Como mínimo, las PYME deben pensar en los siguientes controles cuando traten con terceros:

- Suscribir un contrato de no divulgación y confidencialidad;
- dar acceso a la información sólo cuando sea necesario, en el sentido de que únicamente se concederá acceso a terceros a la información absolutamente imprescindible para realizar su trabajo;
- el acceso a los terceros encargados de tareas de asistencia en materia de TI NO debe otorgarse con carácter permanente, salvo que este tipo de privilegio se requiera de manera explícita y sea necesario; el acceso debe suspenderse de inmediato tras la finalización de las actividades necesarias; deben imprimirse y revisarse los historiales de auditoría para comprobar que las actividades realizadas se limitaron a las operaciones de mantenimiento legítimas;
- solicitar del tercero en cuestión el privilegio de auditar sus medidas de protección de la seguridad, sobre todo en los casos en que se procese información corporativa propia y confidencial en sus instalaciones.

Proveedores de servicios

Los proveedores de servicios son habitualmente PSI, ASP y proveedores de servicios de telecomunicación. Antes de seleccionarlos, los encargados de esta tarea deben informarse de la normativa establecida por los posibles proveedores; por ejemplo, si han establecido límites superiores respecto al ancho de banda, o si filtran el correo electrónico y, en tal caso, con arreglo a qué reglas.

Los proveedores suelen almacenar los datos de usuario a efectos de la facturación (nombre, dirección, ID de usuario, cuenta bancaria), así como los datos de conexión y los contenidos transmitidos (durante un período de tiempo que varía de un proveedor a otro).

Los usuarios deben preguntar a sus proveedores durante cuánto tiempo permanecerán almacenados sus datos. Al seleccionar un proveedor, debe tenerse en cuenta que los que tienen su sede en la UE han de atenerse a la normativa sobre protección de los datos personales que se aplican al tratamiento de este tipo de información.

Mediante el uso del cifrado, los usuarios pueden evitar que los proveedores lean el contenido de los datos transferidos.

Otros controles:

- ¿De acuerdo con qué criterios se ha seleccionado al proveedor?
- ¿Qué medidas de seguridad aplica el proveedor?
- ¿De acuerdo con qué criterios filtra el correo electrónico el proveedor (que presta servicios de correo electrónico)? ¿Existe personal disponible las 24 horas del día para tratar problemas técnicos? ¿Cuál es su grado de competencia?
- ¿Cuál es el grado de preparación del proveedor en caso de avería de uno o varios de sus sistemas de TI (planificación de contingencias, concepto de copias de respaldo de datos)?
- ¿Qué nivel de disponibilidad puede garantizar el proveedor (período máximo de interrupción del servicio)? ¿Comprueba regularmente el proveedor que las conexiones con los clientes se mantienen estables y, si no son apropiadas, qué medidas toma?
- ¿Qué hace el proveedor para garantizar la seguridad de sus sistemas de TI y de los de sus clientes?

Una política de seguridad de la información y unas directrices en materia de seguridad deben constituir componentes habituales de la práctica de todo proveedor. Debe existir la posibilidad de que los usuarios externos revisen las directrices de seguridad. El personal del proveedor debe tener conocimiento de los aspectos relacionados con la seguridad de las TI, y someterse a la obligación de observar las directrices en esta materia; además, se les impartirá periódicamente formación al respecto (no sólo sobre cuestiones de seguridad).

Protección de datos y secreto de la información

Aparte de los miembros de su plantilla, ¿qué considera usted que constituye un activo empresarial crítico para su organización, que pasa desapercibido, casi siempre infravalorado, que puede ser mal utilizado si cae en las manos equivocadas y se pierde de manera instantánea?

La respuesta más probable es la información. Una buena práctica en materia de seguridad de la información hace posible que la información empresarial precisa sea observada y tratada por el personal pertinente, y en el plazo en que la necesita. Actualmente, la

legislación exige que se garantice que la información sobre personas se protege de manera adecuada.

La Ley de protección de datos de 1998 entró en vigor el 1 de marzo de 2000. Protege los datos personales, es decir, la información sobre personas vivas e identificables, o "persona a quien se refieren los datos".

Los requisitos de la Ley pueden resumirse como sigue:

- Evaluación del riesgo de la información de índole personal y sensible;
- Identificación de los controles necesarios para proteger los datos y el secreto de la información;
- Formulación y ejecución de una política de seguridad de la información.

Referencias

1. The fraud advisory Panel – Cyber crime what every SME should know about
2. Jack A. Jones, CISSP, CISM, CIS - An Introduction to Factor Analysis of Information Risk (FAIR) - A framework for understanding, analyzing, and measuring information risk
3. ENISA - Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)
4. ENISA - Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
5. ISO 27001
6. DTI – Directors Guide for Information Security
7. Oxford Integrated Systems - Security in an Uncertain World SME's and a Level Playing Field
8. COMISIÓN DE LAS COMUNIDADES EUROPEAS – DIRECCIÓN GENERAL – B6: Security of Telecommunications and Information Systems -Information Technology Security Evaluation Manual (ITSEM) Version 1.0
9. UK Department of Trade and Industry, Information Technology Security Evaluation Criteria (ITSEC)
10. Leeds Council - Information Assurance Guide and Questionnaire for Small & Medium Sized Businesses (SMEs)
11. Russell Morgan - Information Security for Small Businesses
12. Network and Information Security Report – ICTSB / NISSG
13. Recomendación de la Comisión, de 3 de abril de 1996, sobre definición de las pequeñas y medianas empresas.
14. The OCTAVE (SM) Method Implementation Guide Version 2.0
15. Charles A. Shoniregun, Impacts and Risk Assessment of Technology for Internet Security – Enabled Information Small-Medium Enterprises
16. Diario Oficial de las Comunidades Europeas (20.5.2003)
17. Risk Management among SMEs Executive report of discovery research by Alpa A. Virdi (November 2005) Institute of Chartered Accountants in England and Wales
18. Reputation: Risk of risks (An Economist Intelligence Unit white paper) December 2005
19. Risk management service for SMEs (Newsletter) International Accounting Bulletin: 3, May 24, 2006. ISSN: 0265-0223, Lafferty Publications Ltd
20. Information Security Guide for Small businesses (Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), INFOSEC of the office of Government Chief Information Officer (OGCIO) and the Technology Crime Division HK Police force of the HKSAR Government.)
21. http://sme.cordis.lu/home/index.cfm (SME TechWeb)
22. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm#top (La sociedad de la información en Europa – Portal temático)