Propuesta para la organización y gestión de un servicio de seguridad de la información en pymes

Francisco Javier de la Fuente Cagigós
Grado de Ingeniería Informática

José Rafael Alcalá Gómez

Junio de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	Propuesta para la organización y gestión de un servicio de seguridad de la información en pymes
Nombre del autor:	Francisco Javier de la Fuente Cagigós
Nombre del consultor:	José Rafael Alcalá Gómez
Fecha de entrega (mm/aaaa):	06/2020
Área del Trabajo Final:	Aprovisionamiento de sistemas de información
Titulación:	Grado de Ingeniería Informática

Resumen del Trabajo:

Aunque existe actualmente una sensibilización por parte de las pymes en materia de Seguridad de la Información, mayoritariamente desconocen cómo deben proceder para poder dar respuesta a estas nuevas necesidades.

El presente trabajo tiene como objetivo principal el facilitar a las pymes una definición con las características que debe tener un servicio de gestión de la seguridad, teniendo en cuenta preservar la confidencialidad, la integridad y la disponibilidad de los datos personales, de los clientes y la información estratégica de las pymes.

El trabajo ayudará a definir una estrategia de Seguridad de la Información alineada con las necesidades de negocio y que aportará, entre otros beneficios, aumentar la confianza con clientes o no estar expuestos ante posibles sanciones por la pérdida o mal uso del tratamiento de datos.

Siguiendo las mejores prácticas y recomendaciones de normativas y estándares, se definen para el servicio de Seguridad las tareas que deben realizarse, cómo acometerlas y cómo medirlas.

Además, se detalla cómo debe ser la estructura organizativa, así como la relación de Seguridad con el resto de las áreas de la empresa y, su relación con los proveedores de servicios en cuanto a nivel de cumplimiento normativo y de Seguridad de la Información.

Abstract:

Under the consideration that nowadays there is awareness by SME regarding information security, mostly are unacquainted how to proceed in order to answer these new demands.

The main objective of the following paper is to facilitate to SMEs a definition with all the characteristics regarding a Security Management System, considering confidentiality, integrity and availability preservation for both personal and client data, moreover company's strategic information.

This paper will help Information Security Strategy definition aligned with business needs that will contribute with benefits such as: increasing client satisfaction, non-exhibition to possible sanctions due to loss or misuse of data treatment.

Ensuring best practices and recommendations from standards, follows definitions for Security Systems: which tasks to perform, how to perform and measure them.

Furthermore, an organization structure is included, detailing the proper relationship between Security and the rest of the business areas, and relation with service providers as far as regulation and information security compliance.

Palabras clave (entre 4 y 8):
Servicios, Seguridad, Aprovisionamiento, Security, Services, Ciberseguridad, Cybersecurity, Provisioning

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del trabajo

La sensibilidad actual que existe relacionada con la protección de la información afecta, no solamente a las grandes organizaciones sino también a las medianas y pequeñas empresas que ven cómo sus clientes requieren que sus datos se traten y almacenen de forma segura y se cumpla con las legislaciones en materia de protección de datos. La posición mayoritaria de las pymes es positiva pero no sin algunos riesgos manifiestos. [1]

El incremento del número de ciberataques (*Un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red* [2]) ha ido en aumento en estos últimos años, y las pérdidas económicas ascienden al 0,8% del PIB mundial (74,15 billones de euros). [3]

En general, se detecta una elevada preocupación en relación con la protección de los datos y de las medidas de seguridad que se aplican para impedir la exposición de estos y se eviten posibles ataques sobre los servicios contratados. Según informe de *Consumer Loss Barometer de KPMG*, el 81% de los consumidores españoles muestra su preocupación sobre este tema. [4] [5]

El tema se considera relevante por varios motivos:

- Posible impacto en la sensación de confianza de los clientes actuales, pudiendo provocar impacto en la pérdida de clientes y reputación de la marca o la empresa.
- Una posible denuncia por parte de alguno de los clientes y que puede llevar a la investigación por parte de la Agencia Española de Protección de Datos (AEPD) y posteriores sanciones.
- La creciente preocupación por parte de los clientes hace que el trabajo del área de fuerza de ventas tenga mayor dificultad a la hora de comercializar los servicios si la empresa no tiene una clara estrategia en materia de protección de datos y medidas de seguridad apropiadas.

La confianza ante los clientes pasa por introducir en los procesos de negocio medidas para controlar que los datos personales y sensibles no se expongan. Las empresas deben conocer los datos que manejan, su criticidad y los activos que deberán estar disponibles para dar continuidad al negocio.

Las pequeñas y medianas empresas no cuentan con los recursos dedicados necesarios que permitan gestionar temas relacionados con la Seguridad de la Información y la protección de los datos, dificultando posibles acciones. "*Las pymes se dedican a su negocio y dejan muchas veces la ciberseguridad a un lado*", según indica *Deepak Daswani*, experto en ciberseguridad en entrevista al diario online finanzas.com. [6]

El presente trabajo pretende dar solución al sector de las pymes, definiendo las características que debe tener un servicio de seguridad que permita gestionar los temas relacionados en materia de protección de datos, cumplimiento normativo y Seguridad de la Información (Ciberseguridad).

1.2 Objetivos del trabajo

El presente trabajo tiene como objetivos:

- Definir las características, estructura y gestión que debe tener un servicio de Seguridad que permita preservar la confidencialidad, la integridad y la disponibilidad de los datos de los clientes.
- Definir cómo debe ser la relación con el resto de las áreas de la empresa.
- Definir una estrategia de relación con servicios de terceros en cuanto a nivel de cumplimiento (RGPD) y en materia de Seguridad de la Información.

Estos objetivos tienen como finalidad mejorar la confianza de los clientes, conseguir un mayor nivel de fidelización y aumentar la competitividad de las pymes.

Limitaciones de alcance a considerar:

- Considerando que el área de la Seguridad de la Información puede cubrir tanto peligros naturales como errores humanos o la propia seguridad física [7], el trabajo se centra en una de sus partes: la Ciberseguridad.

A lo largo del trabajo se utilizará el termino Seguridad de la Información, aunque nos centremos en la Ciberseguridad, por lo tanto, no se tendrá en cuenta los peligros naturales o la seguridad física y únicamente englobará a la digital.

- En materia de protección de datos (cumplimiento con el RGPD), con el objeto de limitar el alcance, el ámbito de actividad se centrará en empresas privadas, no relacionadas con entidades públicas y que ofrezcan servicios digitales y traten datos no sensibles (DNI, email, dirección, imágenes, etc.).

1.3 Enfoque y método seguido

Se define de forma clara y concisa el problema a resolver, el trabajo a realizar para darle solución y se definen las tareas para alcanzar los diferentes hitos requeridos para la elaboración del trabajo.

Durante las fases del trabajo se cuenta con la colaboración del consultor asignado por la UOC, que realiza las funciones de asesoramiento y seguimiento.

Las tareas, cuentan con la estimación en tiempo y recursos apropiados teniendo en cuenta la fecha fin de entrega (16/06/2020) y el número de horas, 300.

El proyecto sigue las recomendaciones de la metodología definida en *The PMBOK guide* (*Inicio, Planificación, Ejecución, Seguimiento y control, Cierre*) según la describe *Rita Mulcahy* [8], no aplicando el uso de metodologías ágiles.

Durante toda la etapa, se cuenta con las tareas de seguimiento y control, con el fin de tomar acciones correctivas, gestionar los cambios y medir el rendimiento según la línea base del proyecto.

En una *primera fase* se analizan las diferentes propuestas para servicios de TI (Tecnología de la Información), de gestión y normativas. Se definen los objetivos del servicio, las tareas a realizar y la relación con las áreas internas de la empresa.

En *fases posteriores* se definen la relación con terceros, los indicadores del servicio, la política interna de protección de datos y la de seguridad.

1.4 Planificación del Trabajo

Para el desarrollo de la planificación se tiene en cuenta las siguientes premisas:

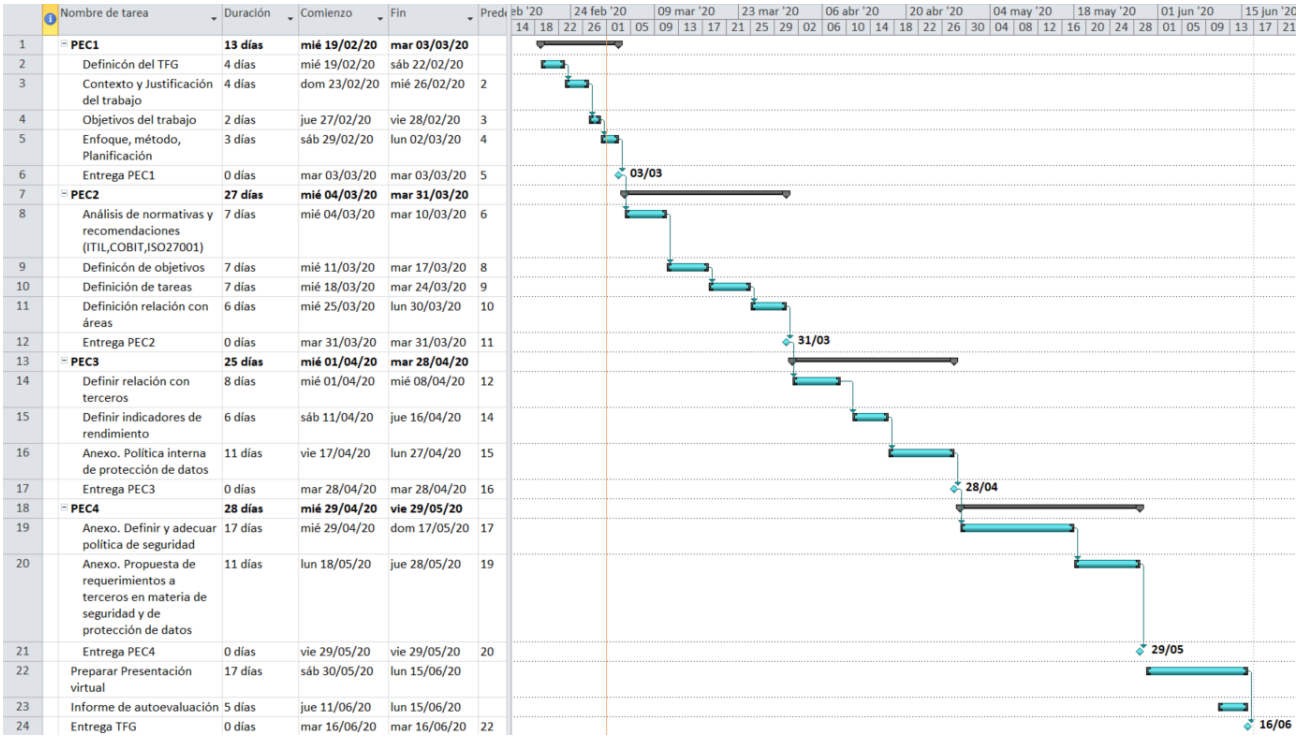
- El proyecto se realiza por un único recurso con disponibilidad de lunes a viernes, de 2 horas al día.
- El recurso cuenta con una mayor dedicación los fines de semana: 3 horas. Supone un total de 16 horas semanales.
- Se tiene en cuenta no trabajar los días festivos, señalados debidamente en el diagrama de Gantt.

Durante las diferentes fases del proyecto (entregas parciales, PEC) se realiza el seguimiento del cumplimento de las tareas planificadas y en caso de ser necesario, se revisa la planificación por si hubiera que realizar algún tipo de reajuste, sin impactar en la fecha final de entrega, 16/06/2020.

Los principales hitos de entrega del proyecto son:

- PEC1: Entrega 03/03/2020
- PEC2: Entrega 31/03/2020
- PEC3: Entrega 28/04/2020
- PEC4: Entrega 29/05/2020
- Entrega TFG: 16/06/2020

A continuación, se muestra la planificación detallada:



	Nombre de tarea	Duración	Comienzo	Fin	Predi
1	**PEC1**	**13 días**	**mié 19/02/20**	**mar 03/03/20**	
2	Definicón del TFG	4 días	mié 19/02/20	sáb 22/02/20	
3	Contexto y Justificación del trabajo	4 días	dom 23/02/20	mié 26/02/20	2
4	Objetivos del trabajo	2 días	jue 27/02/20	vie 28/02/20	3
5	Enfoque, método, Planificación	3 días	sáb 29/02/20	lun 02/03/20	4
6	Entrega PEC1	0 días	mar 03/03/20	mar 03/03/20	5
7	**PEC2**	**27 días**	**mié 04/03/20**	**mar 31/03/20**	
8	Análisis de normativas y recomendaciones (ITIL,COBIT,ISO27001)	7 días	mié 04/03/20	mar 10/03/20	6
9	Definicón de objetivos	7 días	mié 11/03/20	mar 17/03/20	8
10	Definición de tareas	7 días	mié 18/03/20	mar 24/03/20	9
11	Definición relación con áreas	6 días	mié 25/03/20	lun 30/03/20	10
12	Entrega PEC2	0 días	mar 31/03/20	mar 31/03/20	11
13	**PEC3**	**25 días**	**mié 01/04/20**	**mar 28/04/20**	
14	Definir relación con terceros	8 días	mié 01/04/20	mié 08/04/20	12
15	Definir indicadores de rendimiento	6 días	sáb 11/04/20	jue 16/04/20	14
16	Anexo. Política interna de protección de datos	11 días	vie 17/04/20	lun 27/04/20	15
17	Entrega PEC3	0 días	mar 28/04/20	mar 28/04/20	16
18	**PEC4**	**28 días**	**mié 29/04/20**	**vie 29/05/20**	
19	Anexo. Definir y adecuar política de seguridad	17 días	mié 29/04/20	dom 17/05/20	17
20	Anexo. Propuesta de requerimientos a terceros en materia de seguridad y de protección de datos	11 días	lun 18/05/20	jue 28/05/20	19
21	Entrega PEC4	0 días	vie 29/05/20	vie 29/05/20	20
22	Preparar Presentación virtual	17 días	sáb 30/05/20	lun 15/06/20	
23	Informe de autoevaluación	5 días	jue 11/06/20	lun 15/06/20	
24	Entrega TFG	0 días	mar 16/06/20	mar 16/06/20	22

Ilustración 1. Planificación de proyecto TFG

1.4.1 Seguimiento

- PEC1: Entrega 03/03/2020. Entregado en fecha.

  Se han cumplido las tareas según planificación, definido el alcance, los objetivos, metodología y la propia planificación.

- PEC2: Entrega prevista 31/03/2020. Entrega real 01/04/2020.

  Según planificación se han realizado todas las tareas, pero debido a la situación actual de Estado de Alarma por el COVID-19 y a la carga de trabajo que esto ha supuesto en el día a día en casa, se ha solicitado al tutor retrasar la entrega para poder revisar y cumplir con la calidad esperada en la entrega.

  No se contempla que este día de retraso afecte a la planificación del resto de entregas.

- PEC3: Entrega prevista 28/04/2020. Entregado en fecha.

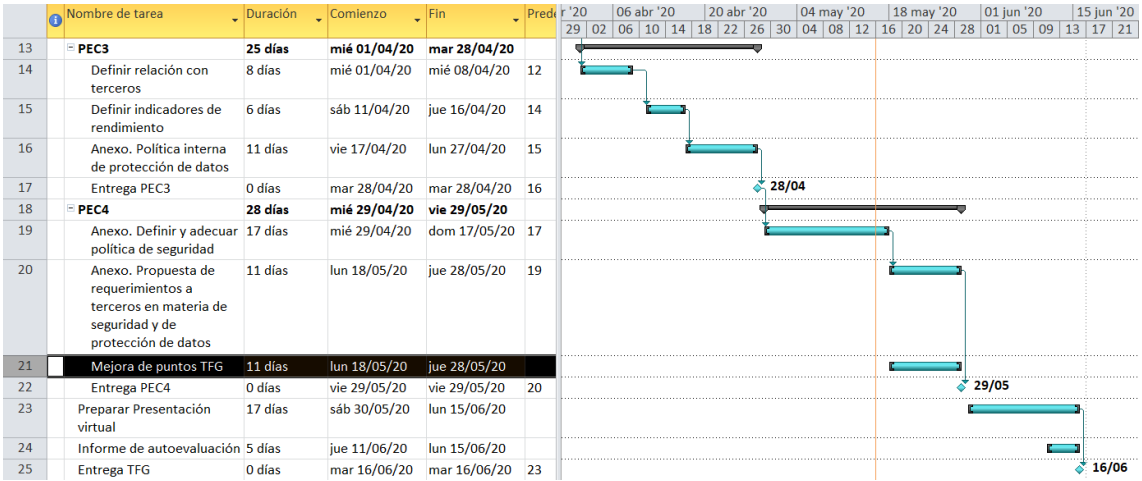
  Según planificación se han realizado todas las tareas en tiempo y se han entregado revisiones parciales al consultor, incorporando las recomendaciones que ha ido aportando.

- PEC4: Entrega prevista 29/05/2020. Entregado en fecha.

  Se ha detectado que en la entrega de la PEC3 se ha hecho parte de las tareas planificadas para la PEC4 (*tarea 20 – Anexo. Propuesta de requerimientos a terceros*) por lo que la carga de trabajo en esta fase se ha visto disminuida. El tiempo se ha invertido en mejorar la bibliografía y algunos de los puntos con menor contenido.

  La entrega se ha realizado en tiempo y se han entregado revisiones parciales al consultor, incorporando las recomendaciones que ha ido aportando.

  A continuación, se muestra cómo ha quedado la planificación tras añadir la tarea de revisión sin afectar al resto de tareas y los hitos del proyecto.



	Nombre de tarea	Duración	Comienzo	Fin	Pred
13	**PEC3**	**25 días**	**mié 01/04/20**	**mar 28/04/20**	
14	Definir relación con terceros	8 días	mié 01/04/20	mié 08/04/20	12
15	Definir indicadores de rendimiento	6 días	sáb 11/04/20	jue 16/04/20	14
16	Anexo. Política interna de protección de datos	11 días	vie 17/04/20	lun 27/04/20	15
17	Entrega PEC3	0 días	mar 28/04/20	mar 28/04/20	16
18	**PEC4**	**28 días**	**mié 29/04/20**	**vie 29/05/20**	
19	Anexo. Definir y adecuar política de seguridad	17 días	mié 29/04/20	dom 17/05/20	17
20	Anexo. Propuesta de requerimientos a terceros en materia de seguridad y de protección de datos	11 días	lun 18/05/20	jue 28/05/20	19
21	Mejora de puntos TFG	11 días	lun 18/05/20	jue 28/05/20	
22	Entrega PEC4	0 días	vie 29/05/20	vie 29/05/20	20
23	Preparar Presentación virtual	17 días	sáb 30/05/20	lun 15/06/20	
24	Informe de autoevaluación	5 días	jue 11/06/20	lun 15/06/20	
25	Entrega TFG	0 días	mar 16/06/20	mar 16/06/20	23

Ilustración 2. Planificación de proyecto TFG. Revisión final

1.5 Breve sumario de productos obtenidos

El desarrollo del presente trabajo generará los siguientes productos:

1. Una propuesta de cómo debe ser la organización y la gestión de un servicio de seguridad de la información en pymes, la relación con terceros y con las áreas internas de la empresa; así como adaptación para el cumplimiento en materia de protección de datos.

2. Anexo, propuesta de política interna en materia de protección de datos.

3. Anexo, propuesta de política interna en materia de seguridad.

4. Anexo, propuesta (para anexar a contrato) de requerimientos a terceros en materia de seguridad y de protección de datos.

1.6 Breve descripción de los otros capítulos de la memoria

La memoria está dividida en los siguientes capítulos:

1. **Introducción**. Se identifica el contexto, justificación del trabajo, los objetivos, la planificación y la metodología utilizada.

2. **Aspectos generales que deben considerarse**. Se hace un análisis de la situación actual de las pymes y un breve resumen de las normativas y estándares considerados para la elaboración de este trabajo.

3. **Definición del servicio**. Se definen los objetivos, área de aplicación.

4. **Definición de las características. Tareas.** Se definen las principales tareas a realizar en relación con la Seguridad de la Información, las métricas, indicadores de rendimiento, relación con resto de áreas.

5. **Relación con proveedores**. Se describe como debe ser las relaciones con los proveedores de servicios en relación con los requisitos de Seguridad y de Protección de Datos.

6. **Indicadores de rendimiento**. Se describen las acciones para poder definir indicadores que permitan a la pyme conocer su estado y evolución.

7. **Conclusiones**. Descripción de las conclusiones del trabajo, breve descripción de lecciones aprendidas y reflexión crítica sobre los logros obtenidos.

8. **Glosario**. Términos y siglas utilizados con breve definición de estos.

9. **Bibliografía**. Referencias de trabajos, publicaciones, contenido online y libros consultados.

10. **Anexos**. Documentación adicional que, por su extensión o carácter auto contenido, se incluye por separado.

2. Aspectos generales que deben considerarse

2.1 Situación actual de las empresas (pymes) en materia de seguridad

Para definir de forma acertada las características y necesidades de un servicio de seguridad acorde a las necesidades de las pymes, es importante analizar la situación y el contexto de estas.

En España el total de empresas superan los 2,8 millones, de las cuales las pymes representan cerca del 99,8% del total y cerca del 93,5% pertenecen a empresas de menos de 10 empleados o sin asalariados en plantilla (autónomos). [1]

Al igual que las grandes empresas, las pymes necesitan de una mayor presencia en la vida digital con el fin de ser competitivas. Esto hace que sean un blanco fácil para la ciberdelincuencia ya que carecen de los recursos que las grandes empresas dedican para protegerse.

En entrevista para la revista Expansión, Rosa Díaz, directora de INCIBE (Instituto Nacional de Ciberseguridad) asegura que "*Las pequeñas y medianas empresas tienden a pensar que los ciberdelincuentes no se van a fijar en ellas y por eso muchas veces no toman las precauciones necesarias. Pero lo cierto es que, como proveedores, son objetivo de ataques para acceder a empresas más grandes*". [9]

La relación con proveedores, el marketing, la producción, la atención al cliente, etc. Todo está basado en sistemas de información interconectados y en muchos casos, accesibles desde distintas ubicaciones, con diferentes tecnologías y a través de distintos medios (correo electrónico, redes sociales, página web, etc.)

Según el observatorio para empresas de Vodafone[2], el 73% de las empresas tiene como prioridad, además de la conectividad a la red y entre dispositivos, la inversión en sistemas de seguridad.

---

[1] Datos proporcionados por el Ministerio de Trabajo, Migraciones y Seguridad Social sobre las empresas inscritas en la Seguridad Social en enero de 2019.

[2] Estudio de digitalización del Observatorio Vodafone de la empresa 2018.

"*La mayoría de las pymes no gestionan la seguridad y únicamente cuentan con un antivirus o un cortafuegos para protegerse*", según palabras de Raúl Fernández, socio de ABF Sistemas en entrevista para CincoDías en su edición online. [10]

Esta situación, unida a las necesidades ya comentadas en la introducción, como son la de mejorar la confianza de los clientes o la obligación del cumplimento regulatorio en materia de protección de datos, hace necesaria una estrategia en materia de gestión de la seguridad que ayude a las pymes.

2.2 Análisis de normativas y recomendaciones

Para decidir el mejor enfoque y definir las características de cómo debe ser un servicio de seguridad, ser gestionado y ser medido, se ha analizado entre otras normativas y estándares, las siguientes que se detallan a continuación:

ITIL v4	Describe un conjunto de mejores prácticas y recomendaciones para la gestión de servicios de TI.
COBIT 5	Marco de trabajo creado por ISACA para la gestión y la gobernanza de TI. Plantea la seguridad como algo transversal que afecta a todas las actividades y procesos de la empresa.
ISO 27001	Norma internacional que define, para ayudar a las empresas, las mejores prácticas en materia de Seguridad de la Información. Está compuesto en su última revisión por 114 controles pensados para mejorar la Seguridad de la Información. La aplicación de estos controles obliga a medirlos, establecer responsabilidades para gestionarlos y definir acciones correctivas.

Tabla 1. Normativas y estándares consultados relacionados con procesos, gestión de servicios y Seguridad de la Información

No es objetivo del TFG la aplicación de ninguna de las normas, pero sí el conocerlas para tenerlas como marco de referencia.

ITIL, COBIT e ISO, son algunas de las recomendaciones y normativas de mayor reconocimiento y adopción por parte de las empresas, y el uso de cualquiera de ellas aporta un marco común con el que medirse respecto a la competencia y mayor flexibilidad para adaptarse al ritmo de las tendencias. Además, cualquiera de ellas por separado o en conjunto pueden ser aplicadas.

De una forma resumida:

- La normativa ISO 27001 tiene como enfoque principal evaluar la eficacia con la que se realizan las tareas o servicios, evaluando el rendimiento.

- ITIL, proporciona la base para la gestión de servicios de TI y ayuda a definir los servicios alineándolos con las necesidades del negocio. Ayuda a justificar los costes y la gestión de riesgos. Además, tiene como foco al cliente interno.

- COBIT es el que mayor enfoque tiene sobre las necesidades de negocio y define cómo deben ser las relaciones con el resto de las áreas garantizando un modelo operativo alineado y, garantizando que las tareas se ejecuten de acuerdo con las obligaciones legales y regulatorias.

Si recordamos los objetivos definidos en el TFG:

- Definir las características que debe tener un servicio interno de Gestión de la Seguridad que permita preservar la confidencialidad, la integridad y la disponibilidad de los datos de los clientes.

- Definir cómo debe ser la relación con el resto de las áreas de la empresa.

- Definir una estrategia de cómo debe ser la relación con los proveedores en cuanto a nivel de requisitos de seguridad como de cumplimiento (RGPD).

COBIT es el marco de referencia que mejor se adapta para poder cumplir los objetivos del trabajo y será tenido en cuenta en caso de ser necesario. En su versión 5, se enfoca a la Seguridad de la Información y la contempla como algo transversal, por lo que aplica a todas las actividades y procesos, lo que permite alinear la seguridad con los objetivos de la empresa.

Respecto a los controles e indicadores de rendimiento, aunque no se hará uso directo de la normativa ISO-27001[3], sí que estará presente como referencia en a cómo está organizado (dominios) y sus controles; así como, la ISO-27002[4] (recomendaciones de las mejores prácticas en la gestión de la seguridad de la información) y la ISO-27004[5] (métricas para la gestión de la seguridad de la información).

[3] UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

[4] UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de Seguridad de la Información".

[5] ISO/IEC 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.

3. Definición del servicio

La definición pasa por conocer los objetivos que se quieren lograr; así como los beneficios una vez conocidas las necesidades y lo que nos aportan las normativas y buenas prácticas.

La participación de la dirección es importante para ayudarnos a definir el servicio y conseguir de esta forma el apoyo en la toma de decisiones.

Las tareas [6] en las que se estructura la definición del servicio son:

- Dar soporte al negocio.
- Promover un comportamiento responsable en Seguridad de la Información y en materia de protección de datos.

Llegados a este punto es importante conocer qué se entiende por Seguridad de la Información. Para ello, ISACA en COBIT 5, la define como algo que: "*Asegura que, dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad)*".

3.1 Objetivos del servicio

Se persigue definir y establecer medidas y controles para garantizar la seguridad sobre los activos de valor y de forma particular:

- *Proteger de forma generalizada los datos, servicios e infraestructuras*.

  Además, de aplicar políticas y buenas prácticas que los empleados y los servicios de TI deben cumplir, es muy importante definir la forma de trabajar en relación con el diseño, desarrollo e implantación de los servicios e infraestructuras.

- *Preservar la confidencialidad de los datos*.

  Se deben definir políticas y buenas prácticas para proteger el acceso no autorizado o la divulgación de los datos. Además, se debe

[6] Definidas en el 2010 por ISACA, ISF e (ISC)[2]

definir una política de clasificación de la información dependiendo del tipo de dato y su sensibilidad, requisitos legales o criticidad para la empresa, se aplicarán distintas medidas de seguridad.

- *Preservar la integridad de los datos*.

  Se deben definir políticas de acceso (registrar y controlar) a los datos, políticas de cifrado, uso de firmas digitales, etc.

  Es muy importante preservar la integridad de los datos (*se garantiza que los datos enviados o guardados no han sido manipulados, ya sea de forma accidental o intencionada*) puesto que puede ser el primer paso para que un ataque tenga éxito y ponga en peligro la disponibilidad o la confidencialidad de los servicios.

- *Asegurar la disponibilidad*.

  Se deben definir las políticas de copias de seguridad y de alta disponibilidad (redundancia) de los servicios o sistemas críticos para asegurar que los datos no se eliminen o modifiquen de forma accidental o malintencionada.

  Es este punto es importante el contar con una gestión de la configuración que garantice los cambios sobre los servicios y sistemas.

  Así mismo, la empresa debe contar con la definición detallada de un plan de continuidad de negocio.

- *Cumplir con las obligaciones legales (cumplimiento de RGPD – Reglamento General de Protección de Datos) y contractuales con los proveedores y clientes*.

  Se deben definir las políticas en materia de protección de datos e identificar el nivel de estos con el fin de prevenir y mitigar los riesgos y garantizar el cumplimiento.

  Así mismo, se deben definir los roles necesarios para el cumplimiento según se define en el RGPD y las medidas a aplicar deben ser monitorizadas con el fin de poder demostrar su aplicación.

  En el caso del RGPD, el reglamento obliga a las empresas a aplicar el principio de responsabilidad proactiva, por lo que es necesario tener conocimiento de los activos críticos y gestionar en base a los riesgos.

- *Concienciar a los empleados en materia de seguridad*.

  La mayoría de las situaciones que afectan a la seguridad de la empresa se deben a las acciones, sin intención, que llevan a cabo los empleados y que a diario trabajan desde distintos dispositivos (móvil, ordenador), ubicaciones (sede de la empresa, teletrabajo, etc.) y plataformas (nube, SaaS, etc.).

  Las empresas deben tener definido un plan de concienciación y formar a los empleados, de manera que sean capaces de detectar posibles incidentes (Ej. intento de robo de información o una suplantación de identidad) y el cómo deben actuar ante ellos.

- *El servicio debe ser escalable como medida de adopción para las distintas sedes o empresas de un grupo de empresas*.

  Es importante que la definición del servicio de seguridad pueda ser aplicado a distintas sedes de las empresas sin tener que invertir tiempo en redefinirlo.

  Igualmente, el servicio debe permitir su adaptación a las nuevas necesidades por parte de las empresas. Las pymes están en constante evolución y el servicio debe evolucionar con ellas.

3.2 Beneficios del servicio

- *Proporcionar un método sistemático y repetitivo en el tiempo para evaluar los activos críticos de la empresa.*

- *Prevenir la pérdida de datos.*

  Aplicar medidas de seguridad, ya sea por la definición de políticas, por la implantación de un aplicativo o un equipo dedicado (cortafuegos, proxy de navegación, etc.), o por la concienciación de los empleados, que dificultarán la pérdida de datos.

  El no perder los datos, entre otras cosas, garantiza a la empresa una competitividad empresarial (por ejemplo, no se filtran datos de propiedad intelectual), refuerza la imagen de confianza que los clientes tienen de la empresa (no afecta a la reputación de marca) y, disminuye el riesgo de una pérdida de ingresos por incumplimiento legal (posibles sanciones económicas).

- *Garantizar la confidencialidad de los datos*.

  Garantizar la confidencialidad aumenta la confianza de los clientes, aumenta la ventaja competitiva y disminuye el riesgo derivado de posibles acciones legales por cumplimiento de reglamentos (Ejemplo, el RGPD – Reglamento General de Protección de Datos).

- *Garantizar la integridad de los datos.*

  Dificultará la pérdida de disponibilidad (*capacidad de estar accesible un servicio, un sistema o un dato siempre que lo requiera el usuario*) y mejorará la imagen que tengan de nuestros servicios los clientes, tanto internos como externos.

- *Fortalecer la confianza de los clientes.*

  La aplicación de medidas en los procesos internos de la empresa mantendrá seguros los sistemas internos y permitirá que los clientes confíen en la empresa para contratar los servicios.

  Transmitir tranquilidad y seguridad, que redundará en fortalecer la confianza con los clientes.

- *Cumplimiento de reglamento relacionado con la protección de datos.*

  La aplicación de medidas de seguridad relacionadas con el cumplimiento del reglamento de protección de datos mejorará el conocimiento que la empresa tiene sobre los datos que trata (tipo de datos, dónde se ubican, quién los trata, quién es el responsable, etc.).

  Además, se evitarán posibles sanciones por incumplimiento.

- *Aumentar el nivel de seguridad de los datos, los sistemas y las aplicaciones.*

4. Definición de las características. Tareas.

Las características se adaptarán según las necesidades, los objetivos definidos y considerando el contexto empresarial, teniendo en cuenta aspectos como[7]:

- Ética y cultura relativas a la Seguridad de la Información.
- Leyes, regulaciones y políticas aplicables.
- Regulaciones contractuales aplicables.
- Políticas y practicas existentes.
- Nivel de madurez de la Seguridad de la Información actual.
- Las capacidades de la Seguridad de la Información y recursos disponibles.
- Practicas de la industria.
- Estándares obligatorios y marcos de trabajo existentes respecto a la seguridad de la información.

4.1 Tareas

Cada empresa debe ser consciente de los riesgos que conlleva su actividad, y debe conocer los planes y medios de los que dispone para poder defenderse de un ataque informático.

A continuación, se detallan las tareas de seguridad que deberán ser gestionadas y que, como mínimo, son necesarias para conseguir los objetivos definidos (*ver apartado 1.2 Objetivos del trabajo*).

Todas las tareas serán definidas, implantadas y gestionadas por el Servicio de Gestión de la Seguridad.

4.1.1 Definir los principios y códigos de conducta en materia de seguridad.

Definir las políticas es la primera tarea que deberá acometer la gestión de seguridad. En ellas se definirán de forma detallada cómo poner en práctica los principios y los aspectos claves que deberán estar bajo control.

[7] Definición según se describe en COBIT 5 para Seguridad de la Información. Sección III. Capítulo 2. Implementación de iniciativas de Seguridad de la Información. 2012. Ed. ISACA

Las políticas tendrán en cuenta la situación específica de la empresa, tales como el contexto y el entorno en el que opera, adaptándose a las necesidades. Así mismo, las políticas siempre estarán en continua evolución.

Deben ser publicadas de forma que sean accesibles a los empleados y se debe definir por cada una de ellas quién es el responsable de mantenerla. Las políticas, en caso de ser necesario, también se facilitarán a los proveedores externos.

En el caso de definir una política que no afecte de forma genérica a toda la empresa, se deberá indicar el área o áreas a las que aplica la política.

Es muy importante que todas las políticas estén aprobadas con el apoyo de la alta dirección de la empresa. Esto facilitará que la implantación de la política se haga con éxito.

La política no debe considerarse como algo estándar, no indica cómo se realiza una tarea de forma específica y no indica las tecnologías que deben usarse. Las políticas deben ser generales y definir los objetivos a cumplir por parte de la empresa.

La siguiente tabla enumera las políticas y las normativas recomendadas que debe tener una empresa, detallando su descripción y algunos de los controles que pueden aplicarse.

Política	Descripción	Controles
Política general de Seguridad	Es la principal junto con la general de protección de datos y en las que el resto de las políticas deberán basarse. La política debe ir alineada con otras de alto nivel ya existentes y se debe comunicar la importancia de esta para la empresa. Se establecerán los requisitos que hay que cumplir para considerar que se da cumplimiento a la política. Se establecerán las directrices que un usuario deberá conocer y aplicar. Si se definen políticas más	• Auditorías externas periódicas • Revisiones internas periódicas • Grado de cobertura y adopción de la política.

Política	Descripción	Controles
	concretas, aplicará esa política y en caso de duda, será la general de Seguridad la que deba aplicarse. Se definirá qué es la Seguridad de la Información para la empresa y se definirán las metas que se quieren alcanzar y las métricas a aplicar. Se definirán aspectos de como debe realizarse la gestión de datos, la evaluación de riesgos de la información y el cumplimiento de las obligaciones legales, reglamentarias y contractuales. Se definirán los roles y responsabilidades para la Seguridad de la Información.	
Política general de protección de datos	Junto con la general de Seguridad, es la política en la que el resto de las políticas deberán basarse. La política debe ir alineada con otras políticas de alto nivel ya existentes y se debe comunicar la importancia de ésta para la empresa. Se establecerán los requisitos que hay que cumplir para considerar que se da cumplimiento a la política. La política deberá definirse teniendo en cuenta los requisitos del marco regulatorio del actual Reglamento Europeo de Protección de datos (RGPD[8]). Se definirán los principios del tratamiento de datos personales y las actividades para las que estos datos pueden ser tratados. Se definirán las funciones clave y las responsabilidades de los principales interesados. Entre estas responsabilidades se definirán las funciones el DPD (Delegado de Protección de Datos).	• Auditorías externas periódicas • Revisiones internas periódicas • Grado de cobertura y adopción de la política.
Normativa de Contraseñas	Las contraseñas son la llave de acceso a los servicios y por tanto son uno de los aspectos más importantes	• Revisiones internas periódicas

[8] Reglamento 2016/679 del 27 de abril del 2016 y que entró en vigor el 25 de mayo de 2018.

Política	Descripción	Controles
	de la seguridad de cara a impedir el acceso no deseado. Se establecerán las buenas prácticas de uso de las contraseñas indicando al usuario cómo debe comportarse ante los distintos escenarios que se puedan dar. La normativa contemplará, orientado a los servicios de atención al usuario, cómo generar, modificar y revocar una contraseña. Se establecerá el patrón que debe cumplirse a la hora de generar la contraseña (mayúsculas, minúsculas, caracteres especiales, etc.) y el periodo de vigencia de estas. Se establecerán las medidas de seguridad para su almacenamiento seguro.	
Normativa de control de accesos	Se establecerá quien, cómo y en qué circunstancias pueden acceder a los activos de la empresa y, cómo se registrarán las evidencias del acceso. La normativa definirá cómo crear los grupos y usuarios en los distintos servicios o aplicaciones; así como, los perfiles (roles) y la forma de realizar la eliminación/baja de un usuario. Se establecerá cómo debe ser la asignación de permisos, crear una cuenta con privilegios de administración y cuales son los mecanismos de autenticación.	• Revisión de los permisos de forma periódica • Revisión de los *logs* de acceso y de eventos. • Revisión periódica de eliminación de cuentas
Normativa de actualización de software	El software debe ser actualizado con el fin de corregir los errores y agujeros de seguridad que los fabricantes detecten. Se establecerá qué software debe ser actualizado (sistema operativo, navegadores, antivirus, etc.). Se establecerá sobre qué activos aplicará la política y la periodicidad con la que se revisarán y aplicarán las actualizaciones.	• Revisiones internas periódicas • Revisiones del estado de las actualizaciones por sistema (servidores, equipos personales, etc.)

Política	Descripción	Controles
	Se establecerá un ciclo de prueba de las actualizaciones para verificar su correcto funcionamiento. Se establecerá un sistema de alertas para recibir avisos y notificaciones sobre actualizaciones.	
Normativa de uso de los equipos de trabajo	Se establecerá el procedimiento de solicitud y asignación de un equipo. Se establecerán las responsabilidades del propietario, que será el que deba garantizar un correcto uso del equipo y del tratamiento de la información. Se establecerá también el cómo actuar ante la pérdida o robo de un equipo y, así cómo ante una infección. Se establecerán las limitaciones de uso tanto en el ámbito laboral como en el ámbito personal en caso de permitirse.	• Revisiones internas periódicas • Revisar privilegios de los empleados en los equipos • Revisión periódica de software instalado
Normativa de clasificación de la información	La información debe ser clasificada con el objetivo de poder aplicar medidas de seguridad según el impacto que tendría para el negocio si esta se difundiera de forma no autorizada o accidental. La normativa debe definir los criterios de clasificación y los activos de la empresa sobre los que aplicará. Se establecerán y definirán los tipos de clasificación, que como mínimo contará con los de confidencial, privado y público. Se establecerá por cada tipo de clasificación el tratamiento a dar (cifrado, limitar su difusión, etc.)	• Grado de cobertura y adopción de la política.
Normativa de copias de seguridad	De cara a la continuidad del negocio se definirá sobre que activos (software, datos) y con que periodicidad se realizarán copias de seguridad. Se establecerán los criterios de acceso a las copias de seguridad.	• Revisiones internas periódicas • Ejecutar de forma periódica restauración de servicios críticos

Política	Descripción	Controles
	Se establecerá el periodo de conservación de la copia de seguridad en función de la necesidad de negocio o por motivos legales. Se establecerá el periodo máximo en el que deben realizarse las pruebas de restauración de los activos más críticos.	
Normativa de uso de dispositivos móviles	Se establecerá el procedimiento de solicitud y asignación de un dispositivo. Se establecerán las responsabilidades del propietario, que será el que deba garantizar un correcto uso del dispositivo y del tratamiento de la información. Se establecerá también el cómo actuar ante la pérdida o robo de un dispositivo y, cómo actuar ante una infección.	• Revisiones internas periódicas • Revisión periódica de software instalado

Tabla 2. Definición de las políticas y normativas mínimas recomendadas a definir por una empresa

De forma generalizada, todas las políticas y normativas que se definan deben contar con un apartado de sanción en caso de incumplimiento y ésta, tendrá que ser acorde a la magnitud o reiteración de la falta.

4.1.2 Definir los activos críticos de la empresa.

Un activo es un recurso (servicios, datos que se manejan, aplicaciones, equipos informáticos, personal interno y externo, redes de comunicaciones, soportes de información o equipamiento auxiliar)[9] que tiene algún valor para la empresa y por tanto debe protegerse de potenciales riesgos.

Los activos de la empresa deben cumplir con los requisitos que defina Seguridad de la Información y que están presentes en la Política General.

[9] Activos según se define en la metodología MAGERIT v3 para el Análisis y Gestión de Riesgos de los Sistemas de Información. En ella se definen 8 tipos de grupos de activos, no aplicando en el presente trabajo que Seguridad de la Información gestione tareas referentes a la seguridad física.

De cara a identificar y clasificar los activos críticos, se realizarán entrevistas con personas que representen a todas las áreas y roles de la empresa.

La Dirección, junto con Seguridad y las áreas que se estimen, definirán cuales son finalmente los activos críticos para asegurar el correcto funcionamiento del negocio.

Según la norma ISO/IEC 27002:2013 en el punto 8.2.1. Directrices para la clasificación, "*Es conveniente que la información se encuentre clasificada en términos de su valor, requerimientos legales, sensibilidad y la criticidad para la organización*".

Siguiendo la recomendación de la norma, se clasificarán los activos teniendo en cuenta el valor económico del activo o asignando una calificación (bajo, medio, alto) a cada uno siguiendo un criterio homogéneo en base a la integridad, confidencialidad y disponibilidad.

Se elaborará un árbol de dependencias entre activos donde se podrá ver la relación existente entre todos los activos de la empresa de cara a facilitar decisiones.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles/métricas:

- Porcentaje de activos que cumplen las políticas de Seguridad.
  - *Objetivo de cumplimiento*: 100% de los activos en producción. No se consideran entornos de desarrollo o pruebas.
  - *Umbral de aceptación*: 70% de los activos en producción. No se consideran entornos de desarrollo o pruebas.

- Porcentaje de activos críticos que cumplen las políticas de Seguridad para mitigar riesgos de seguridad.
  - *Objetivo de cumplimiento*: 100% de los activos identificados como críticos.
  - *Umbral de aceptación*: 70% de los activos críticos.

4.1.3 Gestionar en base a riesgos.

ISACA[10], define el riesgo de TI como un riesgo de negocio, específicamente "*como el riesgo de negocio asociado con el uso, la*

[10] COBIT 5 for Risk. A Powerful Tool for Risk Management (elaborado y editado por ISACA).

propiedad, la operación, el involucramiento, la influencia y la adopción de TI dentro de una empresa”.

Es vital para la empresa conocer los riesgos a los que se enfrenta, con el fin detectar y responder de forma eficaz a los posibles incidentes que se den de seguridad (malware, ataques, robo de datos, etc.).

En términos de Seguridad, el activo a proteger es la información de la compañía, incluyendo la de los clientes; así como el resto de los recursos involucrados (servicios, datos que se manejan, aplicaciones, equipos informáticos, redes de comunicaciones, soportes de información, etc.).

La seguridad de la información no es un problema de TI sino también de carácter estratégico y de gestión de riesgos. Debe proteger los riesgos asociados a la integridad, confidencialidad y disponibilidad de la información.

En base a los activos críticos, se deben analizar los riesgos (¿Qué puede pasar? ¿Cuándo y dónde? ¿Cómo y por qué?) a los que se enfrenta el negocio con el objetivo de dar soporte a la toma de decisiones. Es importante asegurarse reducir el número de escenarios a un conjunto manejable.

Para analizar el riesgo (calificarlo para priorizar esfuerzos) se aplicará la siguiente fórmula:

Riesgo = Impacto x Probabilidad (*)

(*) ISO/IEC 73

Donde, **Impacto** es un porcentaje que estima la degradación de un activo (100% representa la pérdida total del servicio) y **Probabilidad** es la posibilidad de ocurrencia de un suceso o amenaza en base a datos de histórico o de opiniones de los expertos.

El impacto, se valora en términos de costes derivados de los activos afectados y de los daños producidos por el propio activo (daños personales, reputación de marca, pérdida del rendimiento, pérdida del servicio).

La empresa deberá establecer un umbral de riesgo que esté dispuesto a soportar, y la gestión de riesgos debe mantener el nivel de éste siempre por debajo del umbral.

Una vez valorados los impactos, la probabilidad y establecidos los umbrales de riesgo, es una buena práctica el elaborar una tabla donde se vean reflejados los valores.

		IMPACTO		
		Bajo	**Medio**	**Alto**
PROBABILIDAD	**Baja**	*Muy bajo*	Bajo	Medio
	Media	Bajo	Medio	*Alto*
	Alta	Medio	*Alto*	*Muy alto*

Tabla 3. Propuesta de estimación de evaluación del riesgo <<probabilidad x impacto>> en base a propuesta de INCIBE. [11]

Donde Probabilidad e Impacto pueden valorarse teniendo en cuenta los siguientes criterios:

Probabilidad	Valor	Consideraciones
Baja	1	No suele darse en nuestra empresa o sector. La frecuencia es anual o superior.
Media	2	Ha ocurrido alguna vez en nuestra empresa o sector. La frecuencia es inferior al año.
Alta	3	Ocurre con frecuencia en nuestra empresa o sector. La frecuencia es mensual o inferior a un mes.

Tabla 4. Probabilidades para evaluar riesgos

Impacto	Valor	Consideraciones
Bajo	1	No existe impacto económico y afecta mínimamente al activo. No afecta a la reputación o imagen de la empresa. No hay pérdida o exposición de los datos.
Medio	2	Impacto en el negocio con pérdidas financieras que suponen tomar medidas y se puede ver comprometida la reputación e imagen de la empresa. La pérdida del activo puede ser superior a 24 horas. Hay pérdida o exposición de los datos no sensibles.
Alto	3	Impacto en el negocio con pérdidas financieras que pueden poner en peligro la continuidad del negocio y se puede ver comprometida la

Impacto	Valor	Consideraciones
		reputación e imagen de la empresa. La pérdida del activo puede ser superior a 72 horas. Hay pérdida o exposición de datos sensibles.

Tabla 5. Impacto para evaluar riesgos

Seguridad deberá tratar los riesgos bien evitando o eliminando el riesgo o, reduciendo el riesgo (impacto o probabilidad) para que esté por debajo del umbral definido por la empresa y tendrá en cuenta las vulnerabilidades y medidas aplicadas actuales que mitiguen el riesgo.

El riesgo puede ser también aceptado, asumirlo o puede ser asignado a un tercero con capacidad para reducir y gestionar el riesgo.

Finalmente, se elaborará una política de gestión de riesgos donde se explicarán los motivos para llevar a cabo la gestión de riesgos, los objetivos, las responsabilidades, los recursos disponibles, la medición del desempeño y el compromiso de revisión de la política.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles/métricas:

- Porcentaje de activos críticos que cumplen las políticas de Seguridad para mitigar los riesgos y mantener los riesgos en niveles aceptables según el umbral definido.

    - *Objetivo de cumplimiento*: El 100% de los activos críticos deben estar dentro de los niveles aceptables según el umbral definido.
    - *Umbral de aceptación*: Cumplimiento en activos con el riesgo más alto (probabilidad e impacto altos).

- Porcentaje de áreas para las cuales se ha implantado una estrategia global para mantener los riesgos de Seguridad de la Información por debajo del umbral definido.

    - *Objetivo de cumplimiento*: Implantación de la estrategia global en el 100% de las áreas de la empresa.
    - *Umbral de aceptación*: Implantación de la estrategia global en las áreas identificadas con mayor riesgo, bien por tratar con información estratégica o bien por el uso de información sensible.

4.1.4 Preparar un plan de respuesta ante incidentes de seguridad[11].

El plan tiene como objetivo minimizar el tiempo de respuesta ante un incidente de seguridad, contener los daños y buscar una solución persistente en el tiempo, no temporal.

Basándose en el estándar ISO 27000[12], se considera un incidente de ciberseguridad como un "*evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información*".

El plan deberá ser conocido por los empleados de la empresa y deberá ser comunicado a los proveedores de servicios con los que se tenga algún tipo de acuerdo. Además, deberá ser revisado anualmente, y actualizado si procede, y siempre tras un cambio significativo en los sistemas de la empresa.

Se establecerá un Equipo de Respuesta ante Incidentes de Seguridad, compuesto por el personal de Seguridad de la Información (Ciberseguridad), quien coordinará las acciones necesarias para gestionar los incidentes.

Entre otras cosas, el plan definirá que es un incidente de seguridad para la empresa, la tipología y la criticidad respecto a las necesidades de negocio. Así mismo, establecerá el mecanismo de comunicación de incidentes (por *Service Desk*, etc.) y la información mínima y necesaria acerca del incidente.

De forma generalizada el plan de respuesta debe conseguir identificar un incidente, cómo recuperarse de él, las acciones para mitigar las posibles consecuencias, así como el proceso de adquisición y análisis de evidencias.

A continuación, se muestra un flujo general como posible adopción por parte de las empresas.

[11] Conocido también como SIRP (*Security Incident Response Plan*)
[12] ISO/IEC 27000:2018. Publicada por ISO en https://www.iso.org/standard/73906.html

Ilustración 3. Etapas de plan de respuesta de incidentes de seguridad

La fase de **Detección** considera que el incidente puede ser detectado por un sistema de monitorización o alarma que la empresa tenga instalado, por un empleado interno de la empresa, un cliente, un tercero (proveedores de servicios, fabricante, etc.) o un organismo público (CERT).

Durante la fase de **Evaluación Inicial** el equipo de Respuesta ante Incidentes de Seguridad con la información disponible realizará un breve análisis con el fin de definir el tipo de incidente, realizar una primera valoración del impacto y gravedad y, decidir cuáles serán las primeras medidas de contención y notificación (necesidad de implicar a otras áreas, dirección o notificar a un organismo competente[13]).

Se tratará de **clasificar** el incidente, pero esta clasificación podrá variar si en el transcurso del proceso de su gestión se modificasen las circunstancias o conocimiento que se tiene del incidente.

La fase de **Contención y Mitigación** tiene como objetivo limitar en la medida de lo posible la propagación del incidente y minimizar sus efectos.

Dependiendo del tipo de incidente y de los servicios o aplicaciones, afectados, se pondrán en marcha las acciones de contención especificadas en los procedimientos definidos para cada caso.

Estas acciones de contención y mitigación pueden ser, finalmente, las mismas que se establezcan en la fase de remediación.

En la fase de **Remediación y Recuperación** se llevarán a cabo las acciones necesarias para devolver el nivel de operación a su estado

[13] INCIBE-CERT o AEPD (Agencia Española de Protección de Datos)

normal y que las áreas de negocio afectadas puedan retomar su actividad.

La fase de **Mejora Continua** tiene como objetivo aprender de lo sucedido, tomar decisiones para evitar que una situación similar se pueda repetir y detectar mejoras en las medidas de actuación.

La fase de **Registro y Recogida de Evidencias** se inicia desde la detección del incidente, transcurriendo en paralelo al resto de las fases del presente plan. Se guardará cronológicamente y con el máximo detalle, toda la información que se ha ido analizando.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles/métricas:

- Número de incidentes, su gravedad y estado.

    - *Objetivo de cumplimiento*: Tener en estado de resueltos el 90% de los incidentes, independientemente de su gravedad.
    - *Umbral de aceptación*: Tener en estado de resueltos el 70% de los incidentes identificados como graves.

- Número de incidentes que afectan a la Protección de Datos y estado.

    - *Objetivo de cumplimiento:* Cero incidentes comunicados a la Agencia de Española de Protección de Datos. Internamente, tener en estado de resueltas el 90% de las incidencias.
    - *Umbral de aceptación:* Cero incidentes comunicados a la Agencia de Española de Protección de Datos ya que al igual que en el objetivo de cumplimiento, un solo caso que afecte a la investigación por parte de la Agencia puede acarrear graves consecuencias. Internamente, tener en estado de resueltas el 70% de las incidencias.

- Número de llamadas al servicio de atención al usuario (Service Desk) relacionadas con la Seguridad y estado.

    - *Objetivo de cumplimiento*: Tener en estado de resueltas el 90% de las incidencias abiertas por Service Desk.
    - *Umbral de aceptación*: Tener en estado de resueltas el 70% de las incidencias abiertas por Service Desk.

- Número de llamadas al servicio de atención al cliente (SAC) relacionadas con la Seguridad y estado.

    - *Objetivo de cumplimiento*: Tener en estado de resueltas el 90% de las incidencias abiertas por las llamadas al SAC.
    - *Umbral de aceptación*: Tener en estado de resueltas el 70% de las incidencias abiertas por las llamadas al SAC.

- Porcentaje de empleados que han sido notificados.

    - *Objetivo de cumplimiento*: Tener notificados del plan al 100% de los empleados.
    - *Umbral de aceptación*: Tener notificados del plan a los empleados de las áreas más críticas y sensibles (Dirección, Recursos Humanos, Financiero, etc.).

- Porcentaje de proveedores que han sido notificados.

    - *Objetivo de cumplimiento*: Tener notificados del plan al 100% de los proveedores.
    - *Umbral de aceptación*: Tener notificados del plan a los proveedores que traten información sensible o en nombre de la empresa ofrezcan un servicio a un tercero.

4.1.5 Cumplimiento normativo, legal y regulatorio.

Es tarea de Seguridad junto con las áreas de Auditoría, Jurídico y *Compliance* el identificar las regulaciones y normativas que aplican a la Seguridad de la Información según la actividad o sector de la empresa.

Seguridad debe ayudar a implementar las mejores practicas internacionales (ITIL, COBIT, ISO 27001, ISO 27002, etc.) en sistemas de gestión y a cumplir con las obligaciones legales (RGPD/LOPDGDD, ENS, Infraestructuras criticas, etc.) y contractuales para desarrollar el negocio con las máximas garantías.

Se realizan acciones para identificar riesgos técnicos, legales y de gestión relacionados con la privacidad y áreas donde se estén realizando interpretaciones erróneas en el tratamiento de los datos o en el mal uso de los activos.

Se ayudará a definir políticas corporativas y legales e implementar estructuras de privacidad y controles para gestionar los riesgos relacionados con la privacidad en el contexto de la empresa y sus riesgos de negocio.

Se definirá e implementará una monitorización en base a los controles establecidos.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles/métricas:

- Porcentaje de sistemas y aplicaciones para los que han sido identificados sus responsables y han aceptado sus responsabilidades.

    - *Objetivo de cumplimiento*: Tener identificados a los responsables y aceptadas sus responsabilidades del 75% de los activos (sistemas y aplicaciones) tanto críticos (100% de los críticos) como no críticos.
    - *Umbral de aceptación*: Tener identificados a los responsables y aceptadas sus responsabilidades del 100% de los activos (sistemas y aplicaciones) críticos.

- Porcentaje de sistemas y aplicaciones que contienen datos sensibles y sobre los que se han aplicados medidas de Seguridad recomendadas (cifrado, etc.).

    - *Objetivo de cumplimiento*: El 90% de los activos (sistemas y aplicaciones) que tratan datos sensibles deben cumplir con las medidas.
    - *Umbral de aceptación*: El 70% de los activos (sistemas y aplicaciones) que tratan datos sensibles deben cumplir con las medidas.

4.1.6 Concienciación.

La concienciación en materia de Seguridad de la Información es una de las principales carencias en las empresas. Las personas somos el canal más vulnerable para lograr acceder a la empresa y esto es aprovechado por los delincuentes.

A nivel global, en las pymes el impacto medio de los ataques causados por empleados descuidados o desinformados tiene un coste

de 72.000€[14], y el 52% de las empresas señalan las acciones descuidadas de los empleados como el mayor problema en su estrategia de seguridad[15].

La concienciación no es una materia que Seguridad deba afrontar de manera individual, se debe elaborar una estrategia conjunta con las áreas de Recursos Humanos y Formación.

Es muy importante que las tareas de concienciación se realicen de forma constante con el objetivo de desarrollar las habilidades de los empleados en materia de Seguridad de la Información.

Las acciones que se tomen deben lograr la involucración del empleado. Este debe conocer las implicaciones de tratar la información sensible, evitar la fuga de información, cómo actuar ante un correo no deseado y como detectar las técnicas de ingeniería social o el intento de robo de información.

Se establecerán objetivos por roles, siendo diferente la concienciación que debe recibir un operario, un desarrollador o un cargo directivo.

Algunas de las acciones básicas de concienciación y fácilmente aplicables son:

- Hacer uso de contenido audiovisual con mensajes muy concretos. Ejemplo: navegación segura, buenas prácticas en la gestión de contraseñas, uso responsable de los dispositivos móviles, etc.
- Comunicados, al estilo píldoras informativas con mensajes claros y concisos.
- Charlas a los empleados, en grupos reducidos y muy orientadas a tratar un mensaje concreto que se quiera reforzar.

Los materiales anteriormente citados deben ser completos y realistas con los riesgos. Además, deben ser comprensibles y adaptados al entendimiento de todos los empleados.

[14] “Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within”, Kaspersky Lab y B2B International, junio de 2017.

[15] Cálculos basados en el informe "Cost of Phishing and Value of Employee Training" de Ponemon Institute, agosto de 2015.

Para las empresas que tengan un nivel de madurez en concienciación es recomendable fomentar la participación de los empleados exponiéndoles a situaciones de aprendizaje reales, como puede ser, la de recibir un mensaje de *phishing*.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles o métricas:

- Porcentaje de empleados que han sido formados mediante alguna charla.
    - *Objetivo de cumplimiento*: El 70% de los empleados han sido formados o han asistido a alguna charla de Seguridad de la Información.
    - *Umbral de aceptación*: El 55% de los empleados han sido formados o han asistido a alguna charla de Seguridad de la Información.

      El 100% de los empleados considerados como personal de riesgo por el tipo de información que tratan debe haber asistido como mínimo a una charla o recibido algún tipo de formación de Seguridad de la Información.

- Número de comunicados emitidos.
    - *Objetivo de cumplimiento*: Se ha emitido a los empleados mensualmente un mínimo de un comunicado con información de concienciación en materia de Seguridad.
    - *Umbral de aceptación*: Se ha emitido a los empleados de forma trimestral un mínimo de un comunicado con información de concienciación en materia de Seguridad.

- Si se realizan cursos, el estado del seguimiento en porcentaje de empleados que los han completado.
    - *Objetivo de cumplimiento*: El 70% de los empleados han recibido o están cursando actualmente formación de Seguridad de la Información. Incluye a los empleados considerados de alto riesgo (el 100% debe cumplirlo) por el tipo de información que tratan.
    - *Umbral de aceptación*: El 55% de los empleados han recibido o están cursando actualmente formación de Seguridad de la Información.

      El 100% de los empleados considerados como personal de riesgo por el tipo de información que tratan debe

haber asistido y finalizado algún tipo de formación de Seguridad de la Información.

4.1.7 Monitorización de las medidas.

Tan importante es implantar medidas como verificar su efectividad, por ello Seguridad debe realizar seguimiento, reportar el desempeño e identificar áreas de mejora o problemas.

Para poder realizar estas tareas, se apoyará en la monitorización de las medidas, los activos y en la definición de métricas. Una buena monitorización puede anticipar posibles incidentes.

Seguridad elaborará un plan de seguimiento y control del cumplimiento de las medidas (monitorización); así como la elaboración de cuadros de mando donde se permita ver el estado actual y su evolución en el tiempo.

El cuadro de mando debe contener información operativa como las alarmas de seguridad en función de los activos (intentos de conexión no autorizados, activos con alguna vulnerabilidad conocida y no solucionada, si existen actualizaciones de seguridad para el activo, volumen de correo electrónico no deseado recibido, número de virus detectados, equipos con antivirus desactualizado, etc.). Además, debe contemplar aquellos indicadores que nos permitan visualizar la evolución, seguimiento y el cumplimiento de los objetivos.

Todos estos indicadores que forman parte del cuadro de mando son recomendables que tengan unos valores de referencia, como son el valor actual, el valor objetivo y el valor mínimo aceptable.

Por otro lado, y de forma genérica se elaborarán métricas y controles que contribuyan a conocer el estado actual y evolución de aspectos concretos.

A continuación, se detallan algunas métricas en base a las mejores prácticas recomendadas por COBIT-5 y la ISO/IEC 27002:2017[16]:

- Acceso de usuarios a recursos de red conforme a las políticas.
- Cuentas de usuario inactivas de acuerdo con las políticas.

[16] UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de Seguridad de la Información".

- Número de procesos de negocio y de TI en los que la seguridad de la información está integrada.
- Número de proyectos en los que la seguridad colabora.
- Número de brechas de seguridad de la información relativas a no conformidades con las directrices de comportamiento ético y profesional.
- Frecuencia de los informes sobre la gestión de la seguridad de la información al comité ejecutivo.
- Número de auditorias y revisiones internas/externas.
- Valor del riesgo en base al umbral definido.
- Retorno de la inversión (ROI).

Si la empresa quiere definir controles para medir la madurez en materia de Seguridad de la Información y su evolución en base a las metas que se definan, puede apoyarse en los controles definidos en la norma ISO/IEC 27002:2017 donde se describen los siguientes dominios de actuación:

- Políticas de Seguridad.
- Organización de la Seguridad de la Información.
- Seguridad de los recursos humanos.
- Gestión de activos.
- Control de accesos.
- Cifrado.
- Seguridad física y ambiental.
- Seguridad en las operaciones.
- Seguridad en las telecomunicaciones.
- Adquisición de sistemas, desarrollo y mantenimiento.
- Relaciones con los proveedores.
- Gestión de Incidentes que afectan a la Seguridad de la Información.
- Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.
- Cumplimiento.

De forma generalizada para medir el cumplimiento de esta tarea adicionalmente a las ya comentadas, se aplicarán los siguientes controles/métricas:

- Estado de la Seguridad mediante un informe global en base a los sistemas de monitorización.
    - *Objetivo de cumplimiento*: Se tiene con periodicidad mensual un informe global del estado de la Seguridad.

- *Umbral de aceptación*: Se tiene con periodicidad trimestral un informe global del estado de la Seguridad.

La monitorización de las medidas podrá complementarse con la definición de los indicadores de rendimiento (*punto 6. Indicadores de rendimiento*).

Como referencia rápida, se facilita a continuación una tabla resumen con las métricas y controles de cada tarea con sus objetivos de cumplimiento y umbrales de aceptación:

Tarea	Métrica/Control	Objetivo de cumplimiento	Umbral de aceptación
Definir los principios y códigos de conducta en materia de seguridad	El detalle de posibles métricas aplicables a cada una de las políticas está detallado en la tabla *"Tabla 2. Definición de las políticas mínimas recomendadas a definir por una empresa*". De forma generalizada a todas las políticas se pueden aplicar las siguientes:		
	Estado de revisión de las políticas	Revisión anual de todas las políticas	Revisión anual de al menos las políticas generales (seguridad y protección de datos)
	Porcentaje de áreas que conocen y aplican las políticas	100% de las áreas de la empresa	100% de las áreas que traten algún activo identificado como crítico
Definir los activos críticos de la empresa	% de activos que cumplen las políticas de Seguridad	100% de los activos en producción	70% de los activos en producción
	% de activos críticos que cumplen las políticas de Seguridad	100% de los activos en críticos	70% de los activos críticos
Gestionar en base a riesgos	% de activos críticos que cumplen las políticas de Seguridad para mitigar los riesgos y mantener los riesgos en niveles aceptables según el umbral definido	El 100% de los activos críticos deben estar dentro de los niveles aceptables según el umbral definido	Cumplimiento en activos con el riesgo más alto (probabilidad e impacto altos).
	% de áreas para las cuales se ha implantado una estrategia global para mantener los riesgos de Seguridad de la Información por debajo del umbral definido	Implantación de la estrategia global en el 100% de las áreas de la empresa	Implantación de la estrategia global en las áreas identificadas con mayor riesgo bien por tratar con información estratégica o bien por el uso de información sensible
Preparar un plan de respuesta ante incidentes de seguridad	Número de incidentes, su gravedad y estado	Tener en estado de resueltos el 90% de los incidentes, independientemente de su gravedad	Tener en estado de resueltos el 70% de los incidentes identificados como graves
	Número de incidentes que afectan a la Protección de Datos y estado	Cero incidentes comunicados a la Agencia de Española de Protección de	Cero incidentes comunicados a la Agencia de Española de Protección de

Tarea	Métrica/Control	Objetivo de cumplimiento	Umbral de aceptación
		Datos. Internamente, tener en estado de resueltas el 90% de las incidencias	Datos. Internamente, tener en estado de resueltas el 70% de las incidencias
	Número de llamadas al servicio de atención al usuario (Service Desk) relacionadas con la Seguridad y estado	Tener en estado de resueltas el 90% de las incidencias abiertas por Service Desk	Tener en estado de resueltas el 70% de las incidencias abiertas por Service Desk
	Número de llamadas al servicio de atención al cliente (SAC) relacionadas con la Seguridad y estado	Tener en estado de resueltas el 90% de las incidencias abiertas por las llamadas al SAC	Tener en estado de resueltas el 70% de las incidencias abiertas por las llamadas al SAC
	Porcentaje de empleados que han sido notificados	Tener notificados del plan al 100% de los empleados	Tener notificados del plan a los empleados de las áreas más críticas y sensibles
	Porcentaje de proveedores que han sido notificados	Tener notificados del plan al 100% de los proveedores	Tener notificados del plan a los proveedores que traten información sensible o en nombre de la empresa ofrezcan un servicio a un tercero
Cumplimiento normativo, legal y regulatorio	Porcentaje de sistemas y aplicaciones para los que han sido identificados sus responsables y han aceptado sus responsabilidades	Tener identificados a los responsables y aceptadas sus responsabilidades del 75% de los activos tanto críticos (100%) como no críticos	Tener identificados a los responsables y aceptadas sus responsabilidades del 100% de los activos críticos
	Porcentaje de sistemas y aplicaciones que contienen datos sensibles y sobre los que se han aplicados medidas de Seguridad recomendadas (cifrado, etc.)	El 90% de los activos que tratan datos sensibles deben cumplir con las medidas	El 70% de los activos que tratan datos sensibles deben cumplir con las medidas
Concienciación	% de empleados que han sido formados mediante alguna charla	El 70% de los empleados han sido formados o han asistido a alguna charla de Seguridad	El 55% de los empleados han sido formados o han asistido a alguna charla de Seguridad. El 100% de los empleados considerados como personal de riesgo
	Número de comunicados emitidos	Se ha emitido a los empleados mensualmente un mínimo de un comunicado con información de concienciación en materia de Seguridad	Se ha emitido a los empleados de forma trimestral un mínimo de un comunicado con información de concienciación en materia de Seguridad

Tarea	Métrica/Control	Objetivo de cumplimiento	Umbral de aceptación
	Si hay cursos, estado del seguimiento en porcentaje de empleados que los han finalizado	El 70% de los empleados han recibido o están cursando actualmente formación de Seguridad de la Información. Incluye a los empleados considerados de alto riesgo (el 100% debe cumplirlo) por el tipo de información que tratan	El 55% de los empleados han recibido o están cursando actualmente formación de Seguridad de la Información. El 100% de los empleados considerados como personal de riesgo
Monitorizar las medidas	Estado de la Seguridad mediante un informe global en base a los sistemas de monitorización	Se tiene con periodicidad mensual un informe global del estado de la Seguridad	Se tiene con periodicidad trimestral un informe global del estado de la Seguridad

Tabla 6. Referencia rápida de actividades y sus controles

4.2 Definición de la estructura y responsabilidades

La estrategia y gestión de Seguridad de la Información de la empresa debe estar a cargo del Responsable de Seguridad de la Información[17].

Aunque la dirección tiene la responsabilidad en la toma de decisiones, incluyendo la seguridad de la información, la responsabilidad puede y debe ser delegada dentro de la empresa. En caso contrario, se puede exponer al consejo directivo a las reclamaciones por negligencia por parte de los reguladores o de otros grupos de interés, si ocurre un incidente.

Organizativamente el cargo de Responsable de Seguridad de la Información puede estar ubicado según varios modelos, tal y como se describe en el Libro Blanco del CISO[18]:

- Como subárea de Tecnología, dentro de Infraestructuras.
- Como un área específica de Tecnología, al mismo nivel que Infraestructuras.
- Fuera de Tecnología reportando al Responsable de Operaciones (COO) o de Riesgos (CRO).
- En la alta dirección, reportando directamente al CEO.

[17] En empresas grandes esta figura está representada por el CISO (*Chief Information Security Officer*).
[18] ISMS Forum. Libro Blanco del CISO.

Las responsabilidades de Seguridad de la Información deben estar alineados con los objetivos (*definidos en punto 3.1 Objetivos del servicio*). El mínimo de responsabilidades exigibles es:

- Gestión de la operativa de Seguridad de la Información (internamente o mediante servicios externos).
- Alinear la estrategia de Seguridad de la Información con los objetivos de negocio y estratégicos de la empresa.
- Definir las políticas y procedimientos de Seguridad de la Información.
- Asegurar el cumplimiento de normativas y regulaciones que apliquen a la empresa.
- Establecer medidas para gestionar el riesgo en los activos de la empresa.
- Establecer un plan de respuesta de incidentes de Seguridad de la Información.
- Establecer indicadores que permitan conocer el estado actual en materia de Seguridad de la Información.
- Monitorizar el cumplimiento de las medidas aplicadas.
- Concienciar y sensibilizar a la empresa.
- Promover la mejora continua en materia de Seguridad para mejorar los costes, la eficiencia y eficacia.

Todas estas responsabilidades pueden recaer en una única figura, el Responsable de Seguridad de la Información, o dependiendo de la empresa, pueden crearse roles específicos de Seguridad adicionales o complementarios, o recaer todas en un rol ya existente que además de sus actuales funciones realice todas las nuevas. Es habitual, sobre todo en pymes pequeñas, ver como el responsable de administrar los sistemas informáticos, realiza también las funciones de seguridad o de protección de datos.

Como recomendación para la empresa, además de contar con la figura del Responsable de Seguridad de la Información es recomendable que cuente también con la de experto en Cumplimiento y Auditorías de Seguridad. Este rol de experto tendría como tarea principal comprobar que las medidas de seguridad implementadas se adecuan a las políticas, normativas y regulaciones.

La empresa puede contar con su propio equipo o puede delegar subcontratando a una empresa externa tanto las funciones de Responsable de Seguridad de la Información como las de experto en Cumplimiento.

Para empresas que necesitan apostar por un mayor empuje en Seguridad de la Información, es necesaria una organización de seguridad de la información más elaborada, y se pueden añadir grupos y roles adicionales.

Según se define en COBIT 5, algunos de los roles típicos que podría la pyme incorporar en el equipo de Seguridad de la Información y bajo su criterio son:

- Administradores de Seguridad de la Información.
- Arquitectos de Seguridad de la Información.

4.3 Relación con el resto de las áreas de la empresa

Seguridad de la Información debe garantizar que los requisitos que defina se incluyan en los distintos proyectos de negocio, en la definición de nuevas arquitecturas, en el diseño de nuevos desarrollos y en la relación con proveedores de servicios.

La relación de Seguridad con el resto de las áreas de la empresa es fundamentalmente importante, y debe cubrir todas las funciones y procesos que forman parte ella, tanto internos como externos.

De cara a facilitar la relación con el resto de las áreas:

- La Seguridad de la Información se debe poner en práctica en las operaciones diarias.
- Las áreas deben respetar la importancia de las políticas y los principios de Seguridad de la Información.
- A las áreas se les debe proporcionar directrices suficientes y detalladas sobre Seguridad de la Información.

La relación con las áreas puede afectar a todos los procesos del área o únicamente a aquellos que manejen información sensible o hagan uso de activos en los que Seguridad tenga un interés.

Algunos de los procesos de otras áreas de la empresa y en los que Seguridad de la Información debe intervenir son:

- Gestión del Cambio. Los cambios sobre los activos (actualización de un aplicativo, configuración de un servicio, etc.) deben ser controlados para asegurarse que se realizan de forma correcta, según las recomendaciones, plazo y momento acordados.

Según lo define ITIL[19], un cambio es "*la adición, modificación o eliminación de un servicio, o un componente de un servicio, autorizado, planificado o soportado, y de su documentación asociada*".

- Gestión de la Configuración y Activos. Seguridad debe supervisar que todos los componentes que forman parte de un producto o un servicio se mantienen actualizados. La integridad debe estar protegida y se definirá una línea base de configuración, pudiéndose esta línea modificarse siguiendo los procedimientos de cambio formales y en los que Seguridad habrá contribuido a definir.

  Según lo define ITIL, un elemento de configuración es "*un activo, componente de un servicio u otro elemento que está (o estará) bajo el control de la Gestión de la Configuración"*.

- Pruebas (*Testing*). El aseguramiento de la calidad debe contar con la colaboración de Seguridad con el fin de cumplir con las normas, buenas prácticas y los requisitos de diseño en esta materia. Para ello Seguridad, realizará controles y pruebas de seguridad, recomendando que sean durante las fases iniciales donde el coste de resolver las posibles incidencias es menor.

- Protección de Datos. El RGPD exige a las empresas que se garantice la seguridad de los datos y especialmente cuando se trabaja con datos sensibles (ideología política, afiliación sindical, convicciones religiosas, origen racial o étnico, datos relativos a la salud, orientación sexual, dato genético, etc.).

  Seguridad será la encargada de poner las medidas de seguridad para proteger la integridad y confidencialidad de los datos según las indicaciones de la política general de Protección de Datos.

- Auditoría. Seguridad colaborará en facilitar información en las auditorías que así lo requieran y que con carácter periódico realiza esta área. Por otro lado, el propio servicio de Seguridad de la Información realizará auditorías tanto a nivel interno como externo con el objetivo de evaluar las medidas adoptadas, revisar el cumplimiento de las políticas y facilitar posibles puntos de mejora.

[19] Glosario de Términos ITIL v3 (2007)

- Definición de Productos de Negocio. Seguridad colaborará en todas las iniciativas de negocio y lo hará estrechamente para ser un facilitador hacia la innovación. Participará de forma activa y definirá los requisitos para que se cumplan las políticas, normativas y regulaciones teniendo en cuenta la protección de los activos digitales.

- Proceso de altas y bajas de Recursos Humanos. Seguridad tiene un papel importante en este proceso debido, no solamente a la sensibilidad de los datos que se manejan, sino también al conjunto de acciones a llevar a cabo cuando se incorpora (accesos, entrega de equipo de trabajo, dispositivo móvil, etc.) o deja la empresa (desactivación de la cuenta, inhabilitación de accesos, devolución de los equipos de trabajo, etc.) un empleado.

  Junto a Recursos Humanos definirán las medidas de seguridad que se deben aplicar en cada uno de los casos.

- Desarrollo. La seguridad, al igual que se diseña el software para cumplir con las funcionalidades solicitadas por los usuarios, debe formar parte integrada dentro del modelo de desarrollo. Seguridad facilitará las guías de desarrollo seguro y de las mejores prácticas para ayudar en el proceso.

  Por otro lado, Seguridad realizará inspecciones de código para validar si el desarrollo tiene errores de seguridad que podrían más adelante usarse como puerta de entrada de ataques.

  Esta práctica, en fases tempranas del desarrollo evita que los costes de solucionar una incidencia sean elevados.

- Diseño de nuevas infraestructuras. Si hay un proceso crítico y en el que Seguridad deba estar involucrado, es este. Desde que la idea se conceptualiza, Seguridad debe estar presente en el diseño.

  Seguridad asegurará que se cumplan las especificaciones del diseño, las condiciones en las que el sistema funcionará y el cumplimiento de las políticas con el fin de evitar riesgos.

5. Relación con proveedores

Dentro de las responsabilidades que debe asumirse por Seguridad está la de controlar la relación con los proveedores. Es deseable exigir que los proveedores, sobre todo los que ofrecen servicios o afectan a activos críticos para el negocio de la empresa, tengan garantías para poder ofrecer la calidad necesaria y deseable en materia de Seguridad de la Información. Una buena práctica es exigir algún tipo de certificación que lo corrobore, como la ISO 27001 de Sistemas de Gestión de la Seguridad de la Información.

La relación con proveedores es un riesgo que hay que controlar y los acuerdos o contratos que se elaboren deberán contemplar cláusulas o anexos con los requisitos de cumplimiento tanto a nivel de seguridad como de protección de datos. Como mínimo, los contratos deberán contar con estos puntos:

- Información a la que se puede acceder, cómo se accede a ella y qué mecanismos de protección se aplican.
- Definir cómo se realizará la baja de accesos, devolución de activos y las garantías de eliminación de la información sensible, una vez terminada la relación contractual.
- Incluir el derecho a poder auditar y poder hacerles seguimientos sobre los puntos acordados.
- Definir cómo gestionar las incidencias que puedan darse. Es importante en este punto tener bien definido un ANS (Acuerdo de Nivel de Servicio).
- El contrato debe incluir requisitos para el cumplimiento en materia de Protección de datos. Normalmente referentes a las responsabilidades sobre el tratamiento de los datos.

En el “ANEXO A. Requisitos en el tratamiento de datos personales”, se facilita una lista de requisitos mínimos que cualquier proveedor debería cumplir para asegurar el cumplimiento del Reglamento de Protección de Datos (RGPD).

- Si aplica, el proveedor deberá incluir las clausulas de cumplimiento de la Ley de Servicios de la Sociedad de la Información (LSSI).

Así mismo, Seguridad definirá unos requisitos a cumplir por los proveedores y que deberán ser acordes con las políticas internas de la empresa. Estos requisitos en algunos casos deberán ser cumplidos por ambas partes, tanto la empresa como el proveedor, según el tipo de servicio.

En el "ANEXO B. Requisitos de Seguridad a Proveedores", se facilita una lista de requisitos mínimos que cualquier proveedor debería cumplir para asegurar la seguridad de nuestros datos.

Debido a la evolución de la tecnología, las amenazas de seguridad y a los nuevos requerimientos legales y normativas, la empresa debe reservase el derecho a modificar cualquier acuerdo o contrato para poder incorporar medidas adicionales. En caso de cambios en los requisitos definidos en *ANEXO A. Requisitos en el tratamiento de datos personales* , o el *ANEXO B. Requisitos de Seguridad a Proveedores*, estos se divulgarán a todos los proveedores para su conocimiento.

Para medir el cumplimiento de esta tarea se aplicarán los siguientes controles/métricas:

- Proveedores que cumplen con certificaciones relacionadas con la seguridad en los servicios o sobre los activos identificados como críticos.
    - *Objetivo de cumplimiento*: Todos los proveedores con los que se trabajan cumplen con las certificaciones que se les solicita.
    - *Umbral de aceptación*: Los proveedores que tratan datos sensibles o interactúan con activos críticos, cumplen con las certificaciones que se les solicita.
- Auditorías periódicas de obligado cumplimiento por normativa o cumplimiento legal.
    - *Objetivo de cumplimiento*: Realizar una auditoría anual o según el periodo que marque el reglamento (RGPD, LSSI, etc.).
    - *Umbral de aceptación*: Realizar una auditoría anual sobre los activos críticos.
- Auditorías periódicas sobre los acuerdos y contratos con proveedores.
    - *Objetivo de cumplimiento*: Realizar una auditoría anual o según el periodo, si aplica, que marque el reglamento (RGPD, LSSI, etc.).
    - *Umbral de aceptación*: Realizar una auditoría/revisión bianual (puede ser durante el periodo de renovación) sobre los acuerdos y contratos con los proveedores de servicios que traten datos sensibles o trabajen con activos críticos.

6. Indicadores de rendimiento

De cara a una correcta gestión de un servicio es imprescindible medir el rendimiento de las tareas que se realizan, de esta forma se puede validar y mejorar los procesos y controles implantados.

Es importante tener en cuenta que la definición de los indicadores de rendimiento dependerá de los objetivos de Seguridad definidos por la empresa y de hasta dónde se quieran desarrollar. Además, el sector de actividad de la pyme puede afectar a la definición de estos.

Como primer paso y de cara a afrontar qué los indicadores deseados, se puede partir de las tareas anteriormente definidas (*ver 4.1 Tareas*), considerándolo como los indicadores principales:

- Principios y códigos de conducta en materia de seguridad.
- Seguridad en los activos críticos.
- Gestión del riesgo.
- Respuesta ante incidentes.
- Cumplimiento normativo y legal.
- Conciencia de los empleados.
- Monitorización y control de la seguridad.

Para facilitar la lectura de los indicadores se recomienda realizar una representación gráfica tal y como la que se muestra a continuación:

Ilustración 4. Propuesta gráfica de seguimiento de indicadores de rendimiento de seguridad.

Como se aprecia en la gráfica, los indicadores principales tienen valores entre 0 y 10. Estos valores pueden ser calculados en base a los controles de cada uno de los indicadores principales detallados anterioridad (*ver punto 4.1 Tareas*), dando un peso si fuera necesario a cada uno de los controles (ver *Tabla 6. Referencia rápida de actividades y sus controles*).

Como ejemplo, el indicador principal "Concienciación de los empleados" puede estar medido por los valores y pesos asignados a varios de sus controles: porcentaje de empleados que han sido debidamente formados mediante una charla, número de comunicados emitidos, estado del seguimiento de los cursos realizados por los empleados.

Si la empresa considera medir el rendimiento, como buena práctica debería automatizar la generación de las gráficas de rendimiento. De esta forma garantiza que se hace de una forma metódica y sin errores en la obtención de los valores.

La empresa puede optar por un mayor control y definir los indicadores de rendimiento teniendo en cuenta normativas como la ISO-27004[20]que incorpora las mejores prácticas en la medición de un sistema de gestión de la seguridad, y la ISO-27002[21] que dispone de controles, recomendaciones y buenas prácticas para que la empresa conozca los activos, sus responsables y las medidas de protección a aplicar.

A continuación, se detallan algunos indicadores adicionales a los principales y que pueden ser utilizados para complementar la visión general y estar presentes en un posible cuadro de mando:

- *Número de incidentes de seguridad*. Este indicador, que partirá de un histórico de incidentes previos, permitirá conocer si con las medidas de seguridad implantadas se reduce el número de incidentes. Se puede medir en porcentaje o en número total de incidentes.
- *Estado de los parches de seguridad en equipos de los empleados*. Este indicador permite conocer si se están aplicando correctamente las actualizaciones de seguridad y los equipos que están desactualizados. Esto permite conocer el riesgo general.

[20] ISO/IEC 27004:2016. Information technology. Security techniques. Information security management. Monitoring, measurement, analysis and evaluation.

[21] ISO/IEC 27002:2017. Information technology. Security techniques. Code of practice for information security controls.

- *Servidores con vulnerabilidades conocidas*. Este indicador nos permitirá conocer el estado de los activos y si actualmente tienen o no alguna vulnerabilidad pendiente de resolverse. Se puede optimizar actuando únicamente sobre los activos críticos.
- *Porcentaje de correo no deseado (SPAM) y malintencionado (Phishing, malware, etc.)*. Este indicador nos permitirá conocer el volumen de correo no deseado y cómo funcionan las distintas medidas de seguridad que están implantadas.
- *Número de robo o pérdida de dispositivos empresariales (teléfono, ordenador portátil, Tablet, etc.)*. Este indicador tiene su importancia principalmente en el ámbito de la protección de datos, ya que una posible pérdida de un equipo o robo puede exponer los datos sensibles de la empresa y nuestros clientes.
- *Número de equipos con software no permitido instalado*. Este indicador permitirá identificar los equipos que tienen software no permitido en la empresa y que pueden ser potencialmente un peligro.

7. Conclusiones

El proyecto de investigación me ha permitido **conocer de cerca el sector de las pymes y el conocimiento de estas en materia de Seguridad de la Información**, e identificar que, aunque las pymes cada vez son más conscientes de la importancia y relevancia de la Seguridad de la Información debido a su presencia digital, esto no necesariamente se ve reflejado en cómo aplicar las medidas de seguridad o saber gestionarla, lo que ha motivado la definición de los objetivos del TFG (*ver 1.2 Objetivos del trabajo*).

Como una segunda conclusión, es de resaltar la importancia que tiene el **alinear la estrategia de negocio con la de Seguridad**, ambas deben de ir de la mano.

Para los responsables de TI, sentarse a hablar con negocio y entender su estrategia les ayudará a definir las políticas de seguridad y de protección de datos, a identificar los activos que deben protegerse, a cumplir con las normativas y el marco, y a planificar un plan de respuesta de incidentes adecuado.

El responsable de Seguridad de la Información debe hablar a sus usuarios de negocio en términos de amenazas y de impactos al negocio, explicando el por qué de las medidas de seguridad, incorporando en las conversaciones el concepto de gestión de riesgos.

El modelo de gestión de la Seguridad de la Información propuesto en este trabajo permitirá a las pymes adoptar un marco de trabajo, una estructura y unos indicadores de rendimiento, dotándolas de agilidad para adaptarse rápidamente a las necesidades y a los cambios requeridos, tanto por el negocio como por las regulaciones y normativas que les apliquen.

Además, la adopción del modelo propuesto en este trabajo repercutirá en un aumento de la confianza, tanto por parte del negocio como por parte de los clientes, y en un aumento de ofrecer valor frente a la competencia.

Como una tercera conclusión, la importancia de tener como **marco de referencia** las normativas y recomendaciones ya contrastadas como son la ISO-27001 o COBIT 5. Estas normas, elaboradas expertos en el sector de la Seguridad de la Información, recogen las mejores prácticas en aspectos que son claves para la competitividad de las empresas, y su análisis ha servido como punto de referencia para desarrollar los objetivos propuestos y establecer e implementar las medidas para una correcta gestión de la Seguridad de la Información.

Otra conclusión que deriva de la elaboración del propio trabajo es la importancia de tener **una correcta gestión de la Seguridad** a la hora tanto, de trabajar con las áreas internas de la empresa, como de hacerlo con proveedores externos.

Durante el trabajo se han dado pautas de cómo debe ser esa gestión, de cómo medirla y de cómo actuar en la relación con los proveedores. Se ha dejado claro que ya sea internamente, o bien mediante la contratación de un servicio externo, la organización tiene que contar con la figura del responsable de Seguridad de la Información, que será pieza clave y velará porque la gestión sea la correcta.

Del proyecto, tal y como se planteó desde el inicio, no se deja nada sin implementar, y durante las distintas fases se ha ido dando respuesta a los objetivos definidos inicialmente (*ver 1.2 Objetivos del trabajo*).

Este TFG deja abierta la puerta a otros posibles trabajos, como pueden ser, la implementación del propio servicio de seguridad, la definición de un plan director de Ciberseguridad, la implantación para el cumplimiento de la normativa ISO 27001 o el plan de implementación del gobierno según COBIT 5.

Como recomendación a las pymes que quieran comenzar a usar el modelo propuesto, y puesto que el eslabón más débil son las personas, sugiero comenzar por definir un plan de concienciación que constituya un buen punto de partida para la gestión del cambio. Mientras, la empresa puede nombrar un responsable de Seguridad (interno o externo) que identifique las necesidades de la empresa en base a su estrategia de negocio y pueda de esa forma conocer y definir una estrategia sobre los activos afectados.

De cara a asegurar el cumplimiento normativo y legal, la empresa debe incluir también auditorías (ejecutadas por una empresa externa) de los procesos de seguridad, con carácter anual.

Por último, quiero decir que la elaboración del trabajo me ha permitido consolidar los conocimientos en el ámbito de aprovisionamiento de los sistemas de información y adentrarme en el fascinante mundo de la Seguridad de la Información.

8. Glosario

Término	Descripción
Activo	Es cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa.
Agujero de seguridad	También conocido como vulnerabilidad, es un fallo o deficiencia de un programa informático y que puede permitir que un usuario no legítimo accede a la información o lleve a cabo acciones maliciosas.
Amenazas	Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.
Antivirus	Programa informático diseñado para detectar, bloquear y eliminar código malicioso (virus, etc.) y proteger los equipos de otros programas peligrosos (*malware*).
CERT	*Computer Emergency Response Team* o Equipo de Respuesta ante Emergencias Informáticas. También conocido como CSIRT (*Computer Security Incident Response Team*).
Ciberseguridad	Es parte de la Seguridad de la Información y se encarga de la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
Cifrado	Es un mecanismo que utiliza métodos matemáticos para proteger los datos de forma que un usuario no deseado en caso de acceder a la información no pueda leer su contenido (visualiza contenido ilegible) sin conocer la clave de cifrado usada por el emisor.
Confidencialidad	Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
Copias de seguridad	También conocido como *backup*, consiste en la copia que se realiza sobre los datos, aplicaciones con la finalidad de recuperación en caso de ser necesario.
Cortafuegos	También conocido como firewall, es un sistema de seguridad situado en los puntos limítrofes de una red y que tiene como objetivo permitir y limitar, el tráfico entre los diferentes ámbitos que protege.
CSIRT	*Computer Security Incident Response Team.* *(Ver CERT)*
Disponibilidad	Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
Firma digital	Sirve para demostrar la autenticidad de un mensaje, un documento o un aplicativo.
Firewall	*(Ver Cortafuegos)*
Fuga de datos	Es la pérdida de la confidencialidad de la información privada de una persona o una empresa.

Término	Descripción
Ingeniería social	Táctica utilizada para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la victima.
Integridad	La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
Log	Es un archivo donde queda registrada la actividad de una aplicación o servicio de forma cronológica. El nivel de detalle suele ser configurado según las necesidades.
Malware	Es un tipo de software (virus, gusano, troyano, etc.) que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.
PEC (Prueba de Evaluación Continua)	Prueba definida por la metodología de trabajo de la UOC donde se evalúan, de forma periódica, las actitudes de los alumnos.
Phishing	Es la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. El estafador suplanta a una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (email, fax, SMS o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.
Proxy de navegación	Es un sistema que centraliza el acceso a internet dentro de la empresa, monitorizando lo que se hace e impidiendo que se acceda a contenido no deseado.
SaaS	*Software as a Service* (Software como servicio). Es un modelo de distribución de software donde tanto el software como los datos que maneja se alojan en servidores de un tercero (generalmente el fabricante del software) y el cliente accede a los mismos vía Internet.
Seguridad de la Información	Se refiere a la confidencialidad, integridad y disponibilidad de la información, independientemente del formato que tengan.
Servidor	Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software. Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla.
SI (Sistema de Información)	Conjunto de datos que interactúan entre sí con un fin común. Ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.
Sistema de Monitorización	Supervisar el correcto funcionamiento de una aplicación o servicio, analizando su estado y rendimiento y en caso de anomalía, alertar.
Sistema Operativo	Es un software que permite que un ordenador o dispositivo (móvil, Tablet, …) pueda ser fácilmente manejado por un usuario. Normalmente se presentan de forma gráfica. Algunos sistemas operativos conocidos son

Término	Descripción
	el de Microsoft Windows, iOS y Mac OSX de Apple, Android de Google o Linux.
TI (Tecnología de la información)	Conjunto de infraestructuras y comunicaciones para almacenar, recuperar, transmitir y manipular datos en base a los Sistemas de Información (SI).
Vulnerabilidad	*(Ver Agujero de seguridad)*

Los términos han sido consultados tomando como fuente el glosario de términos de ciberseguridad del INCIBE[22]

[22] INCIBE. Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.

9. Bibliografía referenciada

[1] AEPD y CEPYME, «Encuesta sobre el grado de preparación de las empresas españolas ante el reglamento general de protección de datos. Informe ejecutivo,» octubre 2019. [En línea]. Available: https://www.aepd.es/sites/default/files/2019-10/estudio-proteccion-de-datos-aepd-cepyme.pdf. [Último acceso: febrero 2020].

[2] N. Frett, «¿Qué es un ciberataque? Auditool. Archivado desde el original el 18 de abril de 2019,» 18 abril 2019. [En línea]. Available: https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque. [Último acceso: febrero 2020].

[3] Google and The cocktail analysis, «Panorama actual de la Ciberseguridad en España. Retos y oportunidades para el sector público y privado,» 19 octubre 2019. [En línea]. Available: https://drive.google.com/file/d/18TNjaDus-lrSl5gL5Wt-Z4DOsKXtQ46m/view. [Último acceso: febrero 2020].

[4] LEGALTODAY, «El 81% de los consumidores, preocupados por la Seguridad en sus dispositivos,» 1 octubre 2020. [En línea]. Available: http://www.legaltoday.com/actualidad/noticias/el-81-de-los-consumidores-preocupado-por-la-seguridad-en-sus-dispositivos. [Último acceso: febrero 2020].

[5] KPMG, «KPMG Consumer Loss Barometer highlights disconnect in the evento of a data breach,» 26 marzo 2019. [En línea]. Available: https://home.kpmg/xx/en/home/media/press-releases/2019/03/kpmg-consumer-loss-barometer-highlights-disconnect-in-the-event. [Último acceso: febrero 2020].

[6] M. Á. Moreno, «Diario online La Vanguardia. Las pymes dejan muchas veces la ciberseguridad a un lado, dice Deepak Daswani,» EFE, 17 octubre 2018. [En línea]. Available: https://www.lavanguardia.com/vida/20181217/453601860042/las-pymes-dejan-muchas-veces-la-ciberseguridad-a-un-lado-dice-deepak-daswani.html. [Último acceso: febrero 2020].

[7] ISACA, CSX Cybersecurity Fundamentals. Study Guide, 2nd Edition, ISACA, 2017.

[8] R. Mulcahy y L. Diethelm, Preparación para el examen PMP. 7th edición (PMBOK 4th Edition), RMC Publications, Inc, 2011.

[9] J. G. Fernández, «Incibe: "Los hackers atacan a las pymes para llegar a las grandes empresas",» Diario Expansión edición online, 1 diciembre 2019. [En línea]. Available: https://www.expansion.com/economia-digital/protagonistas/2019/12/01/5ddfc152468aebc4718b46b5.html. [Último acceso: marzo 2020].

[10] CincoDías (El País economía), «Las pymes pasan bastante de gastarse dinero en ciberseguridad,» 24 mayo 2019. [En línea]. Available: https://cincodias.elpais.com/cincodias/2019/05/23/pyme/1558612494_142435.html. [Último acceso: marzo 2020].

[11] INCIBE, «¡Fácil y sencillo! Análisis de riesgos en 6 pasos,» 16 enero 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo. [Último acceso: abril 2020].

Bibliografía consultada

ABAST GRUP, Introducción a ITIL. Gestión de la provisión y el soporte de los servicios TI. 2006, Abast Systems S.A.

Alonso Ludeña, Sergio. TFG UOC. Aprovisionamiento ServiceDesk & ITSM Quirón Salud, 16 diciembre 2019 [En línea]. Disponible en: *http://hdl.handle.net/10609/108787* [Consultado: febrero 2020]

INCIBE. Decálogo ciberseguridad empresas. Una guía de aproximación para el empresario. 3 marzo 2017 [En línea] *https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf* [Consultado: marzo 2020]

ISO, COBIT e ITIL. 6 abril 2018 [En línea] *https://www.gb-advisors.com/es/normas-y-estandares-internacionales/* [Consultado: marzo 2020]

¿Cómo se relaciona COBIT 5 y la Seguridad de la Información? 6 diciembre 2018 [En línea] *https://www.pmg-ssi.com/2018/12/como-se-relaciona-cobit-5-y-la-seguridad-de-la-informacion/* [Consultado: marzo 2020]

INCIBE. Políticas de seguridad para la pyme. [En línea] *https://www.incibe.es/protege-tu-empresa/herramientas/politicas* [Consultado: marzo 2020]

MinTIC. Gobierno de Colombia. Elaboración de la política general de seguridad y privacidad de la información. 11 de mayo de 2016 [En línea] *https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf* [Consultado: marzo 2020]

CCN (Centro Criptológico Nacional). Seguridad en el control de procesos y SCADA. Marzo de 2010 [En línea] *https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/212-ccn-stic-480b-seguridad-en-sistemas-scada-comprender-el-riesgo-del-negocio/file.html* [Consultado: marzo 2020]

MAGERIT v3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Octubre 2012 [En línea] *https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XFSfLIVKiUk* [Consultado: marzo 2020]

INCIBE. Gestión de Riesgos. Una guía de aproximación para el empresario. [En línea] *https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf* [Consultado: marzo 2020]

Punit Bhatia. Advisera - EUGDPR Academy. [En línea] *https://advisera.com/eugdpracademy/es/knowledgebase/contenido-de-la-politica-de-proteccion-de-datos-segun-el-rgpd/* [Consultado: marzo 2020]

Un vistazo general de COBIT 5 for Risk. 31 octubre 2013 [En línea] *https://www.academia.edu/31530752/COBIT_5_for_Risk* [Consultado: marzo 2020]

Olivé Vernet, Carles. Diseño de indicadores y métricas para la creación de un cuadro de mando de seguridad. Diciembre 2018 [En línea] *http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89126/7/olivernet81TFM0119memoria.pdf* [Consultado: marzo 2020]

ISMS-Forum Spain. El Libro Blanco del CISO. Año 2019 [En línea] *https://www.ismsforum.es/ficheros/descargas/ellibroblancodelciso1540377171.pdf* [Consultado: marzo 2020]

SCProgress. Ciberseguridad. Normas ISO 27001 - ISO 27002. Agosto 2017 [en línea] *https://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf* [Consultado: marzo 2020]

Oliván Huerva, Antonio. Guía de controles de Ciberseguridad para la protección integral de la PYME. Diciembre 2017 [en línea] *http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf* [Consultado: marzo 2020]

INCIBE. Relación con proveedores. Políticas de seguridad para las pymes. [En línea] *https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/relacion-proveedores.pdf* [Consultado: abril de 2020]

RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [En línea] *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es* [Consultado: abril de 2020]

LOPDGDD. Ley Orgánica 3/2018, 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. [En línea] *https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673* [Consultado: abril de 2020]

AEPD. Ejerce tus derechos. 20 de julio de 2019 [En línea] *https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos* [Consultado: abril de 2020]

INCIBE. ¿Sabes cómo se mide la Seguridad de la Información en tu empresa? 21 de septiembre de 2015 [En línea] *https://www.incibe.es/protege-tu-empresa/blog/mide-seguridad-informacion* [Consultado: abril de 2020]

ITIL V3 Glosario v2.1. Publicado en academia.edu, 30 de mayo de 2007 [En línea] *https://www.academia.edu/36543475/ITIL_V3_Glosario_v2.1_30_de_mayo_del_2007* [Consultado: abril de 2020]

ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Febrero de 2018 [En línea] Publicada por ISO en *https://www.iso.org/standard/73906.html*

INCIBE. Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. 20 de febrero de 2017 [En línea] *https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario* [Consultado: mayo de 2020]

ISOTools. Cómo alinear la estrategia y la seguridad de la información de acuerdo a ISO 27001. 26 de marzo de 2017 [En línea] *https://www.isotools.org/2017/03/26/como-alinear-la-estrategia-y-la-seguridad-de-la-informacion-de-acuerdo-a-iso-27001/* [Consultado: mayo de 2020]

García, Paloma. Impulso español a las normas internacionales de ciberseguridad. Seguritecnia, 28 de febrero de 2020 [En línea] *https://www.seguritecnia.es/tecnologias-y-servicios/ciberseguridad/impulso-espanol-a-las-normas-internacionales-de-ciberseguridad_20200228.html* [Consultado: mayo de 2020]

ISACA. COBIT 5 para Seguridad de la Información. 2012, Ed. ISACA.

10. Anexos

ANEXO A. Requisitos en el tratamiento de datos personales

Los requisitos que a continuación se definen deberán estar dentro del acuerdo o contrato que se firme con el proveedor.

Cuando se vaya a realizar un tratamiento de datos personales por cualquier proveedor por cuenta de la empresa, solo se elegirá un encargado (prestador del servicio) que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD[23] y garantice la protección de los derechos de los interesados.

Se prohibirá al encargado del tratamiento recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable, informándole de que, en caso de autorización deberá informar al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

Siempre se regulará por escrito la relación con los terceros encargados del tratamiento, mediante un contrato de encargo de tratamiento, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

El acuerdo o contrato estipulará, en particular, que el encargado:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas de la empresa, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal derecho lo prohíba por razones importantes de interés público.
b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

[23] RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

c) Tomará todas las medidas necesarias en materia de seguridad, de conformidad con el artículo 32 “Seguridad del tratamiento” del RGPD.
d) Respetará las condiciones indicadas por el responsable para recurrir a otro encargado del tratamiento.
e) Asistirá a la empresa, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.
f) Ayudará a la empresa a garantizar el cumplimiento de las obligaciones de seguridad, incluida la notificación de brechas o violaciones de seguridad a la Autoridad de Control, así como a los interesados cuando proceda.
g) A elección de la empresa, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho aplicable.
h) Pondrá a disposición de la empresa toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas anteriormente establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

ANEXO B. Requisitos de Seguridad a Proveedores

A fin de prevenir y mitigar cualquier impacto de seguridad en los sistemas y servicios involucrados en prestar a la empresa, el proveedor se compromete a cumplir con los siguientes requisitos.

Como requisito deseable, deberá contar con la certificación ISO 27001[24] (Gestión de la Seguridad de la Información) u otra que garantice la calidad y las buenas prácticas sobre la Seguridad de la Información.

En caso contrario, deberá contar al menos con las siguientes medidas, que deberá detallar para su posterior control por parte del área de Seguridad de la empresa:

a. Control de acceso.
    a. El acceso a los sistemas por parte de los empleados del proveedor está controlado como mínimo por usuario y contraseña.
    b. El proveedor tiene una política de contraseñas y un procedimiento para garantizarla.
    c. El acceso de los empleados del proveedor tanto a los servicios, servidores y la información, se limitará al mínimo imprescindible para las tareas según el rol que desempeña.
    d. La conexión a infraestructura de producción con el objeto de operar los sistemas, si se realiza por un tercero, deberá hacerse mediante conexión VPN y mediante una máquina de salto que deberá cumplir con los niveles de parcheando críticos que se conozcan, según sistema.

b. Medidas perimetrales.
    a. El proveedor implementa mecanismos de seguridad (Cortafuegos, etc.) que impidan el acceso no deseado a los sistemas y la información.
    b. Los sistemas de seguridad perimetral están actualizados.
    c. Los sistemas involucrados en el servicio están protegidos por una solución Antivirus y actualizada.
    d. El proveedor dispone de un sistema o política de parcheado periódico de las vulnerabilidades críticas de los sistemas operativos de los servidores (Linux, Windows, etc.) y de sus servicios o software base (java, PHP, OpenSSL, etc.).

c. Copias de seguridad.

[24] UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

a. El proveedor deberá realizar copias de seguridad de los sistemas y de la información afectada para ofrecer el servicio. Se debe indicar por parte del proveedor la tecnología y medidas de seguridad del sistema de almacenamiento.
b. El proveedor deberá facilitar dónde se almacenan las copias y si es infraestructura propietaria o de un tercero. En caso de ser de un tercero, en qué condiciones y si es dentro de la Comunidad Europea.
c. El acceso a las copias está controlado siguiendo las políticas de control de acceso.

d. Seguridad de equipos personales.
    a. Se hace uso de mecanismos de seguridad (Antivirus y Cortafuegos) que impidan el acceso no deseado a los sistemas o la infección por malware.
    b. Los ordenadores portátiles y sistemas de telefonía móvil o *tablets*, están cifrados.
    c. Existe una política que contempla cómo debe ser el uso de dispositivos externos (llaves USB, discos USB, etc.) para la copia de información.
    d. El proveedor dispone de un sistema o política de parcheado de las vulnerabilidades críticas de los sistemas operativos que use (OSX, Windows, Linux, etc.).

e. Tránsito de la información.
    a. El proveedor garantiza que todas las conexiones desde fuera de las oficinas y hacia su infraestructura interna, se realiza mediante el uso de VPN.
    b. El proveedor garantiza que todos los sistemas y servicios involucrados en los servicios prestados hacen uso de conexiones seguras (TLS, SFTP, HTTPS, SSH, etc.).

f. Plan de continuidad de negocio.
    a. El proveedor monitoriza los sistemas involucrados en los servicios prestados y, garantiza que cualquier incidencia que se dé, será notificada al responsable del servicio de Seguridad de la empresa.
    b. El proveedor debe contar con un plan de continuidad de negocio en caso de desastre y garantizar la continuidad de los servicios contratados.

g. Análisis de la seguridad.
    a. El proveedor realiza, de forma periódica, pruebas de penetración de los sistemas involucrados y de los servicios prestados con el fin de garantizar la seguridad.

h. Otras consideraciones:
    a. El proveedor deberá contar con su propia plataforma y en caso de ser subcontratada a un tercero, deberá detallar cómo es la conexión, con el objeto de conocer por dónde transita la información y en qué condiciones lo hace. En cualquier caso, las plataformas subcontratadas por el proveedor deberán cumplir todos los requisitos indicados en este anexo.
    b. El proveedor debe indicar si los servidores son locales (España) o están ubicados dentro del Espacio Económico Europeo (EEE).

       En otro caso, el proveedor deberá cumplir con la protección de datos del país no miembro de UE (Unión Europea), proporcionar las oportunas salvaguardas como la de incluir en el contrato clausulas del tratamiento de los datos personales, o bien, tener el consentimiento del interesado en base a motivos específicos.

ANEXO C. Política General de Protección de Datos

La política está desarrollada de forma genérica teniendo únicamente en cuenta las normativas de la Agencia Española de Protección de Datos (AEPD) y no a las propias adaptaciones de las comunidades Autonómicas (Cataluña y País Vasco).

1. Información general.

   La presente normativa es de obligado cumplimiento para todos lo empleados de la empresa.

   El incumplimiento de la normativa, medidas y procedimientos derivados de esta podrá acarrear el inicio de medidas disciplinarias y, en su caso, las responsabilidades legales correspondientes.

   La responsabilidad de la actualización de la presente normativa es del Delegado de Protección de Datos, en colaboración con los responsables de las distintas áreas y el responsable de Seguridad de la Información.

   Como apoyo a la política, se pueden consultar las definiciones que el RGPD[25] menciona en su *artículo 4*.

2. Objetivo de la normativa.

   El objeto de la presente normativa es informar a los empleados en materia de protección de datos con el fin de aplicar su contenido en el desarrollo y el ejercicio de sus funciones.

   La normativa está dirigida a todas las áreas de la empresa y, en particular, a aquellos que intervienen en el tratamiento de datos de carácter personal, así como a los responsables de los departamentos, unidades internas, al personal autorizado para acceder e informar de los mismos y para el personal de desarrollo.

[25] RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Publicado en BOE, 4/5/2016.

3. Delegado de Protección de Datos.

La empresa dispone de un delegado de protección de datos (DPD) que entre otras funciones:

a. Informa y asesora a los empleados que tratan datos personales de las obligaciones que les afecta en virtud de la normativa vigente en protección de datos.
b. Supervisa el cumplimiento de lo dispuesto en la normativa vigente y de las políticas de protección de datos de la empresa.
c. Conciencia y forma al personal que participa en las operaciones de tratamiento de datos.
d. Realiza auditorias relacionadas con el cumplimiento.
e. Coopera y actúa como punto de contacto con la autoridad de control para cuestiones relativas al tratamiento, y en concreto, con la Agencia Española de Protección de Datos.

4. Principios generales de la protección de datos.

- **Secreto profesional**. Un principio básico y personal para toda persona que intervenga en el tratamiento de datos personales es su obligación de secreto profesional respecto de dichos datos y su deber de guardarlos, subsistiendo dichas obligaciones aún después de finalizar sus relaciones con el responsable del tratamiento o, en su caso, con el encargado del tratamiento.

  Por lo tanto, queda expresamente prohibido facilitar cualquier información de carácter personal a terceras personas distintas del interesado (aun cuando exista vinculo de parentesco) salvo que se establezca por Ley o por expresa autorización del interesado.

- **Principio de lealtad**, que implica cumplir todas las normas de Derecho generales y/o sectoriales aplicables al tratamiento, así como las políticas y normas de la empresa.

- **Principio de proporcionalidad**, que implica que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

- **Principio de licitud**, que implica que, cualquier tratamiento tendrá una base jurídica como el consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines

específicos, la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales, el cumplimiento de una obligación legal aplicable al responsable del tratamiento o, la protección de los intereses vitales del interesado o de otra persona física.

- **Principio de transparencia**, que implica que el interesado será informado del alcance del tratamiento de forma leal, inequívoca, especifica y expresa.

- **Principio de finalidad y limitación de la finalidad**, que implica que el tratamiento de los datos siempre se llevará a cabo con fines explícitos, legítimos y específicos.

- **Principio de compatibilidad**, que implica que no se llevarán a cabo tratamientos de datos con fines incompatibles con aquellos que motivaron la recogida de los datos. No se considerarán en todo caso incompatibles los fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

- **Principio de minimización de datos**, que implica que, los datos sometidos a tratamiento serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados y a los mínimos datos posibles.

- **Principio de exactitud**, que implica que se someterán a tratamiento datos exactos y, si fuera necesario, actualizados; adoptando todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

- **Principio de limitación del plazo de conservación**, que implica que los datos serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento para los que fueron recogidos los datos personales.

- **Principio de integridad, confidencialidad y seguridad**, que implica que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

- **Principios de protección de datos desde el diseño y por defecto** reduciendo al máximo el tratamiento de datos personales, tanto en relación con la cantidad de datos personales recogidos, la extensión de su tratamiento, su plazo de conservación y su accesibilidad.

- **Principio de responsabilidad proactiva o diligencia debida**, que implica que el responsable y el encargado del tratamiento deben cumplir con los principios antedichos y ser capaces de demostrarlo.

5. Condiciones para el consentimiento.

Antes de dar su consentimiento, el interesado será informado de ello y tendrá derecho a retirar su consentimiento en cualquier momento. Además, deberá ser tan fácil retirar el consentimiento como darlo.

El responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos utilizando un lenguaje claro y sencillo.

Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato o prestación de servicio.

6. Categorías especiales de datos.

Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física, datos relativos a la salud o datos relativos a la vida o la orientación sexuales de una persona física, salvo cuando concurran circunstancias especiales.

7. El interesado y el tratamiento de sus datos.

Cuando los datos se obtengan del interesado directamente, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará la información indicada a continuación:

a. La identidad y los datos de contacto del responsable.
b. Los datos de contacto del delegado de protección de datos.
c. Los fines del tratamiento a que se destinan los datos personales.
   la base jurídica del tratamiento.
d. Cuando el tratamiento se base en el interés legítimo, los intereses legítimos del responsable o de un tercero.
e. Los destinatarios o las categorías de destinatarios de los datos personales.
f. La intención del responsable de transferir datos personales a un tercer país u organización internacional.
g. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
h. La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
i. Cuando el tratamiento esté basado en el consentimiento, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
j. El derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).
k. Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos.
l. La existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará además de toda la información indicada en el apartado anterior, las categorías de datos personales de que se trate y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

La información indicada en los apartados anteriores se proporcionará al interesado dentro de un plazo razonable, una vez obtenidos los datos personales y como máximo en un mes.

Si los datos personales han de utilizarse para comunicación con el interesado como máximo la información se comunicará en el momento en que se produzca la primera comunicación hacia el interesado.

8. Derechos del interesado.

El ejercicio de los derechos es gratuito y deben ser respondidas las solicitudes en el plazo de un mes, aunque se tiene en cuenta la complejidad y se puede prorrogar en dos meses más el plazo.

- **Derecho de acceso.** Es el derecho del interesado dirigirse al responsable del tratamiento para conocer si está tratando o no tus datos de carácter personal y, en el caso de que se esté realizando dicho tratamiento, obtener información de los datos personales que son objeto del tratamiento, los fines, las categorías de datos que se traten, los destinatarios, el plazo de conservación de los datos, origen de los datos en caso de no haber sido obtenidos de forma directa, la existencia de decisiones automatizadas (Ej. perfiles).

- **Derecho de rectificación**. Este derecho permite al interesado obtener la rectificación de tus datos personales que sean inexactos.

- **Derecho de oposición**. Supone que el interesado puede oponerse a que se realice un tratamiento de sus datos personales cuando sean objeto de una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles y, cuando el tratamiento tenga como finalidad la publicidad directa.

- **Derecho de supresión o derecho al olvido**. Permite al interesado solicitar la eliminación (incluyendo copias, réplicas de datos y enlaces) de los datos de carácter personal en las siguientes situaciones:

    - Los datos personales que ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
    - El interesado retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico.
    - El interesado se oponga al tratamiento por motivos relacionados con su situación particular, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con fines de publicidad.
    - Los datos hayan sido tratados ilícitamente.
    - Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de

los Estados miembros que se aplique al responsable del tratamiento.
- Los datos personales se hayan obtenido en relación con la oferta de Servicios de la Sociedad de la Información[26] cuando el interesado sea menor.

- **Derecho a la limitación del tratamiento**. El interesado tiene el derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos en los siguientes supuestos:

  - El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable su verificación.
  - El interesado se haya opuesto al tratamiento basado en motivos relacionados con su situación particular, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.
  - El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos y en su lugar solicite la limitación de su uso.
  - El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

- **Derecho a la portabilidad**. El interesado tiene derecho a recibir los datos personales que le afectan, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica y, a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se le hubiera facilitado en un principio.

- **Derecho a no ser objeto de decisiones individuales automatizadas**. Garantiza al interesado que no sea objeto de una decisión basada únicamente en el tratamiento de sus datos, incluida la elaboración de perfiles, que produzca efectos jurídicos sobre él o le afecte significativamente de forma similar.

9. Registro de actividades.

La empresa gestionará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad y que contendrá la siguiente información y según se indica el RGPD:

[26] Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Título II, Capítulo I, Artículo 8 “Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario”.

a. El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
b. Los fines del tratamiento.
c. Una descripción de las categorías de interesados y de las categorías de datos personales.
d. Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
e. En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.
f. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

10. Medidas de seguridad.

Dependiendo de los costes de aplicación y su la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

En función principalmente del análisis de riesgos que el responsable del tratamiento y en su caso el encargado realice, habrá que aplicar medidas que en su caso incluya, entre otras:

a. La Seudonimización y el cifrado de datos personales.
b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
c. La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
d. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, principalmente como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

11. Transferencia de datos internacionales.

Cualquier área que necesite transferir datos de carácter personal fuera del Espacio Económico Europeo, lo consultará previamente con el delegado de protección de datos.

Solo están permitidas las transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, tanto la empresa como los responsables y el encargados del tratamiento que intervengan en la transferencia, cumplen las condiciones establecidas en el RGPD, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Dicha transferencia no requerirá ninguna autorización específica.

Cualquier otro supuesto deberá ser gestionado y tratado por el Delegado de Protección de Datos (DPD) que actuará según se marca en el reglamento (RGPD) y que podría llegar a solicitar autorización a la AEPD para realizar la transferencia.

12. Infracciones y sanciones.

La empresa está expuesta a ser sancionada por la Agencia de Protección de Datos por el incumplimiento de la normativa.

Las infracciones menos graves se sancionan con hasta 10 millones de euros o el 2% del volumen de facturación anual de la empresa (la más alta de las dos).

Y las infracciones más graves se sancionan con multas que pueden alcanzar hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa (la más alta de las dos).

Hay que tener en cuenta que el régimen sancionador se aplica a los responsables y encargados del tratamiento.

El RGPD prevé la posibilidad de no sancionar y apercibir para que se apliquen las medidas correctoras en un plazo fijado.

13. Brechas de seguridad.

Una brecha de seguridad es un incidente (destrucción, pérdida, alteración, comunicación o acceso no autorizado) que afecta a datos de carácter personal pudiendo tener su origen accidental o intencionadamente.

La empresa tiene la obligación de notificar a la Agencia Española de Protección de Datos (AEPD) las brechas de seguridad que puedan ocasionar daños y perjuicios sobre las personas y, si son graves, comunicarlo a las personas afectadas. El plazo para notificar desde que se conoce la existencia de la brecha es de 72 horas.

14. Actuación con la AEPD.

Corresponde al Delegado de Protección de Datos (DPD) de la empresa la interlocución y el mantenimiento de las relaciones institucionales con la Agencia Española de Protección de Datos (AEPD), sin perjuicio de la colaboración de la Dirección de Servicios Jurídicos, Responsable de seguridad de protección de datos y de las áreas responsables de cada fichero.

El área que reciba aviso de inspección o solicitud de información de la AEPD lo pondrá en conocimiento inmediatamente del DPD.

ANEXO D. Política General de Seguridad de la Información

1. Información general.

   La Dirección, consciente de la importancia y exigencia que supone la correcta gestión de la Seguridad de la Información y de los servicios de TI, se ha comprometido a la implantación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información, siendo de alcance total a todas las áreas de la Organización.

   Asimismo, ha establecido un marco de estrategias de Gestión de los Servicios alineadas con el negocio, con la finalidad de mejorar continuamente el servicio prestado a los clientes, garantizando la disponibilidad de este, consiguiendo de esta manera incrementar su grado de satisfacción.

   La responsabilidad de la actualización de la presente normativa es del responsable de Seguridad.

2. Objetivo de la normativa.

   El objetivo es marcar las pautas de alto nivel necesarias para conseguir la máxima calidad en la prestación de los servicios de TI, así como la máxima seguridad en la información, consiguiendo que todos los tratamientos de información relativos a los procesos de negocio incluidos en el alcance se realicen de forma segura y únicamente por personal autorizado, protegiendo la información ante incidentes que afecten a la confidencialidad, integridad y disponibilidad de los activos del negocio.

   Todos los empleados de la organización son informados de sus roles y responsabilidades en materia de calidad del servicio y Seguridad de la Información al incorporarse en su puesto de trabajo y son responsables de cumplirlas.

3. Directrices generales de actuación.

   - Aseguramiento de la calidad en la prestación de los servicios de TI mediante la implantación y mantenimiento de un Sistema de Gestión de Servicios de TI en todas las áreas de actuación.
   - Compromiso de cumplimiento de todos los requisitos legales y reglamentarios aplicables, requisitos de negocio, así como obligaciones contractuales.

- Compromiso de mejora continua del sistema de gestión y de la eficacia y eficiencia de los procesos internos de prestación de los servicios de TI y Seguridad de la Información.
- Compromiso de satisfacción de las partes interesadas, prestando servicios de TI alineados con las necesidades de clientes, usuarios y todos los grupos de interés.
- Cumplimiento de políticas de seguridad, de gestión de la configuración, de gestión de cambios y de gestión de entregas.
- Definir una política apropiada para el propósito del proveedor del servicio.
- Crear un servicio de TI innovador, eficiente y de mínimo riesgo, que facilite la actividad de los clientes.
- Destinar los recursos necesarios para desarrollar los servicios con los niveles de calidad exigidos por nuestros clientes, manteniendo un adecuado equilibrio entre coste y beneficio.
- Asegurar la confidencialidad, integridad y disponibilidad de la información tratada.
- Reconocer la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados y otras partes interesadas.
- Evitar que la información o los servicios se vean perjudicados por incidentes de seguridad.
- Analizar la vulnerabilidad de la información y preparar una respuesta efectiva a los incidentes en Seguridad de la Información para garantizar la continuidad de los servicios prestados.
- Incluir los requisitos de Seguridad de la Información pertinentes en las ofertas y contratos correspondientes.
- Formar y concienciar a todo el personal en lo referente a gestión de servicios de TI y a Seguridad de la Información.
- Disponer de un conjunto de controles de aseguramiento y refuerzo de la seguridad.
- Gestionar adecuadamente todas las incidencias que puedan ocurrir.