CONFEDERACIÓN CANARIA DE EMPRESARIOS
CEOE CEPYME

Financiado por:

Gobierno de Canarias
Consejería de Economía, Conocimiento y Empleo

Pasos prácticos para la implementación de un **sistema de gestión en privacidad de la información**

BASADO EN LA NORMA **ISO/IEC 27701**

FECHA DE EDICIÓN: 31 DE DICIEMBRE DE 2019

Financiado por:

CONFEDERACIÓN CANARIA DE EMPRESARIOS
CEOE CEPYME

Gobierno de Canarias
Consejería de Economía, Conocimiento y Empleo

Pasos prácticos para la implementación de un **sistema de gestión en privacidad de la información**

BASADO EN LA NORMA **ISO/IEC 27701**

Este manual ha sido elaborado por la **Confederación Canaria de Empresarios** en el año 2019, en el marco de las diferentes actuaciones de Participación Institucional que desempeña esta Institución, financiado por la **Consejería de Economía, Conocimiento y Empleo del Gobierno de Canarias.**

Índice de contenidos

Introducción

La Confederación Canaria de Empresarios, como organización empresarial más representativa que ostenta la representación institucional de los empresarios ante las Administraciones Públicas y organismos en el ámbito territorial de Canarias, al amparo de lo dispuesto en el párrafo primero de la Disposición adicional sexta del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores y la Ley 10/2014, de 18 de diciembre, de participación institucional de las organizaciones sindicales y empresariales más representativas de Canarias; según el criterio constitucional de irradiación por la pertenencia a las Confederaciones nacionales CEOE y CEPYME, así como por el reconocimiento asumido por el Gobierno de Canarias, de más representativa y de participación institucional, en el Acuerdo de la VI Mesa de Concertación Social Canaria (firmada el 25 de enero de 2018), y sobre la base del reconocimiento expreso de la Dirección General de Trabajo del Gobierno de Canarias, por informe escrito de fecha 5 de abril de 2016 y en el artículo 23.4 de la Ley Orgánica 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias, tiene como objetivo prioritario la defensa de los intereses empresariales de carácter general y la prestación de servicios a todos los sectores de actividad.

La Confederación Canaria de Empresarios es una organización empresarial sin ánimo de lucro, constituida el 12 de junio de 1978 al amparo de la Ley 19/1977, reguladora del Derecho de Asociación Sindical, con más de 40 años de antigüedad, basándose en un esquema de base sectorial y territorial, ha alcanzado, un alto grado de consolidación, notoriedad, reconocimiento, desarrollo y representatividad empresarial. Representa los intereses generales y comunes de las empresas sin distinción de tamaño, sector de actividad o ubicación, a través de un sistema único de integración asociativa, de unidad de acción empresarial y de no atomización de representaciones empresariales.

En este sentido, para poder desarrollar este acompañamiento al empresario canario, la Confederación Canaria de Empresarios, además de desempeñar su papel de máximo interlocutor social en los debates de transcendencia económica, respetado y valorado por todos los estamentos públicos, asume desde hace más de 20 años la prestación de una serie de servicios: Servicio Integral de Empleo para la creación de empresas y la orientación e inserción laboral, acciones de formación, así como actuaciones en materia de prevención de riesgos laborales, que funcionan de forma coordinada y cooperantes entre sí, con el fin último de prestar un servicio integral, activo y flexible que permita mejorar, tanto cuantitativa como cualitativamente, la situación del mercado laboral.

Dentro de toda esta labor, cobra especial relevancia la realización de proyectos durante los últimos años y los que pretende acometer en lo sucesivo dicha organización empresarial para la implementación de una cultura preventiva del cumplimiento en materia de protección de datos personales por las empresas u otras organizaciones, pues la adecuada información y sensibilización constituye el primer paso imprescindible para su difusión y adopción por los empresarios canarios.

En el marco de las actuaciones de Participación Institucional que desempeña esta institución, financiadas por la Consejería de Economía, Conocimiento y Empleo del Gobierno de Canarias, la Confederación Canaria de Empresarios ha elaborado este manual con el fin de que las empresas que conforman el tejido empresarial de Canarias y el resto de organizaciones con o sin ánimo de lucro implementen un sistema de gestión de Privacidad de la Información con el fin de cumplir las exigencias establecidas en el Reglamento (UE) 2016/679 de Parlamento Europeo y del Consejo, de 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 y por el que se deroga la Directiva 95/46/CE (RGPD).

Recientemente, el pasado mes de agosto, International Organization for Standardization (ISO) publicó la norma ISO/IEC 27701 Técnicas de seguridad. Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la Gestión de la Información de Privacidad. Requisitos y directrices.

La norma ISO 27701 especifica los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión de la privacidad de la información (PIMS), basado en un aumento de los controles de la norma de gestión de la seguridad de la información ISO 27001. Por lo tanto, este estándar permitirá facilitar el cumplimiento del RGPD y de la normativa nacional en la materia, la L.O. 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

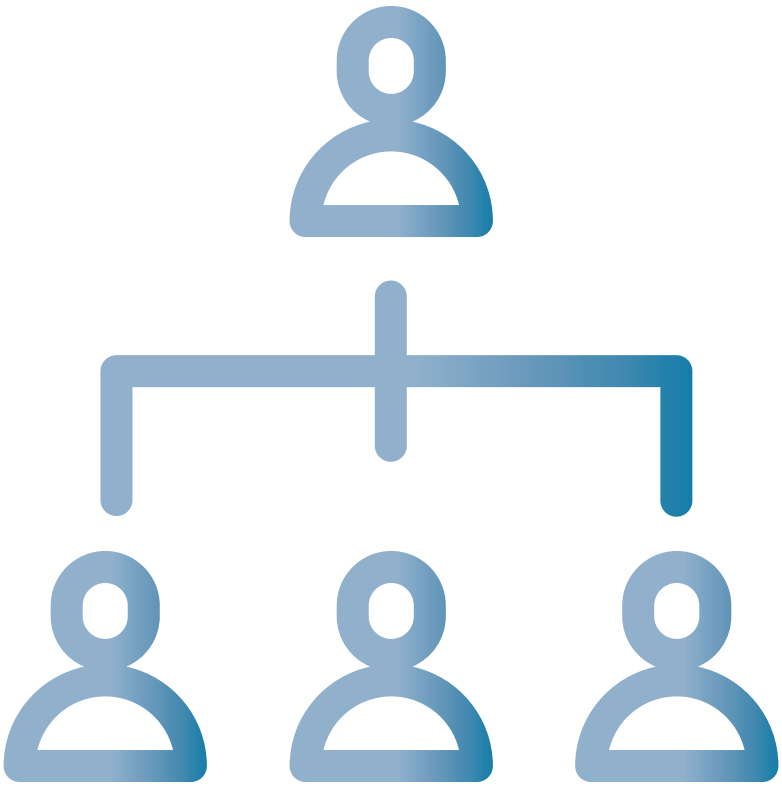
La realidad es que la implantación de un sistema de gestión de Privacidad de la Información reportará a nuestra empresa u organización importantes beneficios, entre los que destacan: la mayor confianza de la entidad ante la sociedad en general, mayor transparencia y seguridad en el tratamiento de la información, contribuye a la adopción de acuerdos comerciales con mayores garantías, se definen de forma clara los roles y responsabilidades y, además, se reduce la complejidad en su implementación al integrarse con la norma ISO/IEC 27001, que es la norma por excelencia en seguridad de la información. Así pues y ante cualquier posible inspección se tendría prueba fehaciente de estar aplicando unos controles de privacidad acorde con un estándar internacional.

Al igual que el resto de normas ISO, puede ser implementada en **cualquier tipo de organizaciones, grandes o pequeñas, incluidas empresas públicas y privadas, entidades gubernamentales y organización sin ánimo de lucro**. Sin mbargo, las organizaciones que deseen proceder a la certificación, en base a esta norma, de su sistema de gestión de Privacidad de la Información deberán disponer de un sistema de gestión de seguridad de la información ISO 27001 certificado o, en el supuesto de no contar con éste último, deberán implementar la ISO 27001 e la ISO 27701 en una auditoría integrada. De conformidad con lo anterior, la implementación del Sistema de Gestión de Privacidad de la Información no se podrá realizar de forma independiente, es decir, será necesario acreditar la existencia o desarrollo de un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme a la ISO/IEC 27001.

Por lo tanto, este manual tendrá el objeto de conseguir implementar un sistema de gestión en materia de protección de datos personales con el fin de conseguir su certificación en base a las normas descritas. Este sistema de gestión se estructurará en varias fases, la cuales serán desarrolladas en los siguientes epígrafes.

FASE I

Liderazgo y compromiso con la seguridad y la política en protección de datos



FASE I

Liderazgo y compromiso con la seguridad y la política en protección de datos

Introducción

Cualquier entidad que se ponga como objetivo la implementación de un sistema de gestión en protección de datos deberá asumir el liderazgo y el compromiso de establecer unas medidas de seguridad al tratamiento de la información que garantice su integridad y que, en todo momento, respeten las obligaciones impuestas por la normativa vigente en materia de protección de datos personales de las personas físicas.

Este compromiso no podrá quedarse en una simple manifestación de intenciones por parte de la empresa u organización. Se deberá desarrollar los procedimientos oportunos para acreditar el seguimiento y la evaluación del sistema de gestión en cada una de sus fases. Estos procesos internos deberán respetar las exigencias establecidas en la normativa desde el diseño y por defecto.

El artículo 25 RGPD determina que: *"el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*

El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento."

A continuación se establecerán las actuaciones a llevar a cabo para abordar esta primera fase de nuestro sistema de gestión.

Checklist en protección de datos personales

Antes de comenzar con el diseño de nuestro sistema de gestión en Privacidad de la Información, se plantea la necesidad de determinar el grado de conocimiento que la empresa u organización poseen en la materia y si se han abordado acciones al respecto. La herramienta para dilucidar dicho nivel de conocimiento en esta fase inicial es el "Checklist en materia de protección de datos".

Con dicho Checklist pretendemos conocer lo siguiente:

- Si existe una cultura en materia de la seguridad de la información.
- Los diferentes departamentos/empleados con acceso a datos de carácter personal.
- Finalidad del tratamiento.
- Licitud del tratamiento.
- Sistema de tratamiento (papel, digita o mixto).
- Categoría de datos personales tratados.
- Tecnología aplicada al tratamiento de datos personales.
- Formas de recogida de los datos personales.
- Método de información de derechos a los titulares de la información.
- Cesiones de datos personales.
- Sistema de archivo de la información.
- Medidas organizativas/técnicas de seguridad utilizadas.
- Procedimientos de recuperación de la información y de copias de seguridad.

Por consiguiente, esta herramienta permite un acercamiento a la realidad de aquellas en materia de protección de datos y, a su vez, sirve de hoja de ruta para el delegado de protección de datos o persona responsable a la hora de diseñar el programa específico de cumplimiento normativo.

Nombramientos del delegado de protección de datos y del responsable de seguridad

Delegado de protección de datos

El órgano de gobierno de la entidad deberá nombrar formalmente al Delegado de Protección de Datos si se encuentra en alguno de los supuestos descritos en los artículos 37 del **RGPD** y/o 34 de la **LOPDGDD**. El nombramiento se deberá recoger de forma documental y se incluirá en el clausulado las siguientes cuestiones:

- Datos identificativos del Delegado seleccionado.
- Consideraciones que apoyen su nombramiento.
- Funciones a desempeñar en su cargo.
- Obligaciones derivadas a su cargo.
- Referencias al estatuto del Delegado de Protección de Datos en el ejercicio de su cargo.
- Datos para poder contactar con el Delegado de Protección de Datos.
- Comunicación de su nombramiento a AEPD.

Responsable de seguridad

La designación de la figura del responsable de seguridad es de carácter facultativa, por lo que su nombramiento se deberá valorar por cada empresa u organización. Se trata de la persona/s que se encargarán de coordinar y controlar las medidas adoptadas en el manual de seguridad. A pesar del aumento de discrecionalidad otorgada en el RGPD a las entidades a la hora de definir sus medidas organizativas y técnicas, el nombramiento de este cargo contribuye a garantizar el principio de responsabilidad proactiva que configura la forma de proceder del Responsable del tratamiento de datos personales.

Su nombramiento, al igual que el nombramiento del Delegado, se deberá documentar:

- Datos identificativos del Responsable de Seguridad.
- Consideraciones justificativas de su nombramiento.
- Funciones y obligaciones derivadas de su cargo.

Política de protección de datos

La Política de Protección de Datos es un documento que permitirá al órgano de gobierno de la organización fijar la piedra angular de su sistema de gestión en Privacidad de la Información, definiendo las características del mismo, el alcance y sus objetivos. Además, se constituye como un documento que demuestra el compromiso de la entidad con el sistema de gestión a implementar, incluyendo las medidas de control interno que posibiliten detectar, prevenir y mitigar los posibles riesgos de incumplimiento (las medidas de control/seguridad se desarrollarán en el manual de seguridad del responsable del tratamiento que se desarrollará en una fase posterior).

Los principales aspectos a incluir en este documento son los siguientes:

Finalidad de la Política de Protección de Datos.

Ámbito de aplicación.

Recursos protegidos (definición, categoría de datos personales y categorías de tratamientos).

Principios que rigen el tratamiento de los datos personales.

Registro de actividades de tratamientos (en los supuestos en los que su confección sea obligatoria).

Identificación de la base jurídica que legitima el tratamiento de datos.

Deber de informar a las partes interesadas del tratamiento.

Acreditación del consentimiento.

Derechos de los interesados.

Medidas de seguridad.

Encargados del tratamiento.

Brechas de seguridad.

Mecanismos para llevar a cabo la implementación.

Control, evaluación y divulgación.

Anexos, en este apartado y dependiendo de la actividad ejercida se podrán incluir los siguientes:

- Política de privacidad.
- Política de cookies.
- Tratamiento de datos personales de los empleados.
- Pacto de confidencialidad para empleados.
- Cláusula de protección de datos en la firma de correos.
- Formulario de consentimiento en el tratamiento de datos personales en las entregas físicas de currículum vitae.

- Cláusula en materia de protección de datos para la recepción de currículum vitae vía e-mail.
- Cartel de videovigilancia.
- Consentimiento cesión de derechos de imagen.
- Formularios de ejercicios de derechos ARSOPOL.
- Modelos de contratos con el corresponsable y el encargado.
- Formulario web de inscripciones.
- Formulario de consentimiento del tratamiento de datos personales.

La citada política se califica como norma de ciclos, es decir, durante la vigencia de la misma se encuentra en constante monitoreo, actualización y mejora. En consecuencia, la política de protección de datos es una de las normas de carácter interno que componen el Compliance Program, entendiéndose por éste último al conjunto de normas internas establecidas en la entidad a iniciativa del órgano de administración con la finalidad de implementar en ella un modelo de organización y gestión eficaz e idóneo que le permita mitigar el riesgo de comisión de delitos y exonerar a la misma.

Compromiso de la empresa u organización

El órgano de gobierno deberá recoger en un documento su liderazgo y compromiso con el sistema de gestión de protección de datos que pretende implementar, siendo responsable de:

Establecer las medidas técnicas y organizativas a todo tratamiento de datos personales que se realice.

Adoptar, implementar y mejorar el sistema de gestión de Privacidad de la Información.

Dotar al sistema de gestión de los recursos financieros, materiales y humanos adecuados y suficientes para su funcionamiento eficaz.

Fijar y aprobar la política de protección de datos.

Asegurar que se establezcan los procedimientos para el proceso de formación de la política de protección de datos, de toma de decisiones y de ejecución de las mismas promoviendo una cultura que garantice altos estándares éticos de comportamiento.

Comunicar la política de protección de datos con un lenguaje e idioma adecuado a los miembros de la entidad.

Nombrar el Delegado de Protección de Datos en los supuestos en los que dicho nombramiento sea obligatorio de conformidad con la normativa que regula la materia.

Asegurarnos de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión en materia de protección de datos y de su mejora continua, incluyendo todas las no conformidades relevantes, promoviendo activamente una cultura de información completa y transparente.

Tener conocimiento de los resultados de las auditorías.

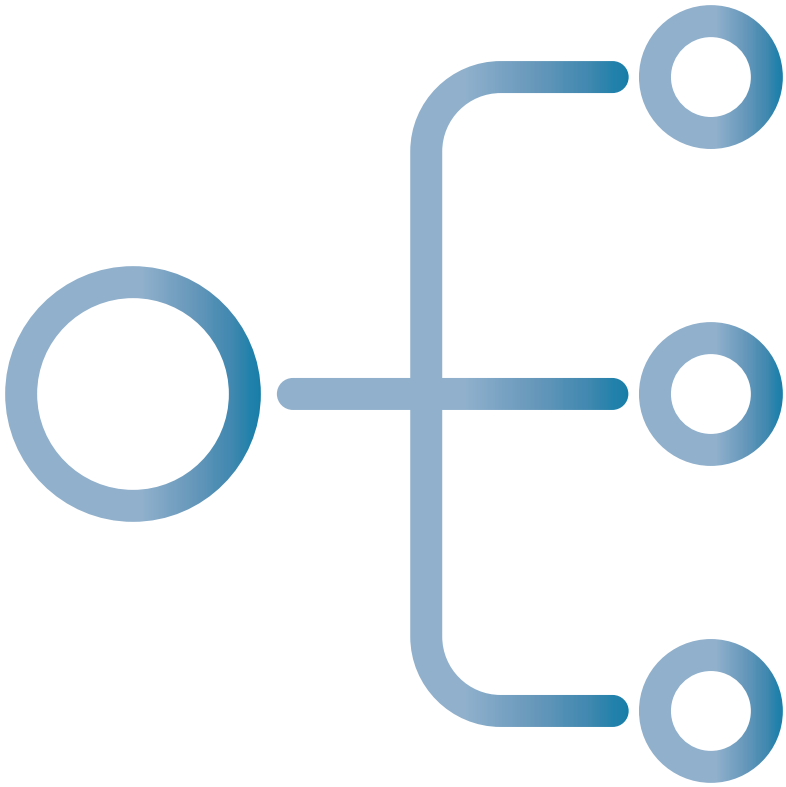
Recibir copia de las revisiones del sistema de gestión de la Seguridad y Privacidad de la Información realizadas por los órganos competentes, así como la documentación de la evidencia de los resultados obtenidos.

Examinar periódicamente el sistema de gestión de gestión en Privacidad de la Información.

Por lo tanto, el presente documento se configura como el compromiso formal para la implementación de nuestro sistema de gestión en materia de protección de datos.

FASE II

Circunstancias propias de cada empresa u organización



FASE II

Circunstancias propias de cada empresa u organización

Introducción

En esta fase se analizarán las especificidades de cada empresa u organización con el fin de diseñar un sistema de gestión lo más adaptado posible al contexto y a las características de la misma.

El diseño de un programa de Privacidad de la Información no puede plagiarse de una entidad a otra, dado que cada una de ellas tiene una problemática y unos riesgos diferentes. Así pues y con el fin de diseñar un programa específico en la materia, se analizarán los diferentes elementos que nos permitirán contextualizar la actividad de ésta y, en consecuencia, establecer un programa de gestión lo más idóneo posible, entre ellos se encuentran:

Normativa general y específica

El entorno legislativo en el que cada empresa u organismo desarrolla sus actividades se encuentra en constante cambio, haciendo que éste cada vez sea más abundante y complejo. Es fundamental realizar la identificación de toda la normativa aplicable a la actividad de aquella para diseñar la estrategia y los procedimientos a fin de dar cumplimiento a los preceptos legales y así poder salvaguardarse ante situaciones de riesgo que podrían derivar unas consecuencias económicas que podrían afectar a su estabilidad e incluso a su continuidad.

Normativa general

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 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 y por el que se deroga la Directiva 95/46/CE.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Normativa específica

Real Decreto de 24 de julio de 1889, Código Civil.

Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Ley 58/2003, de 17 de diciembre, General Tributaria.

Ley 178/2005, 26 de julio, por el que se aprueba el Reglamento que regula la historia clínica en los centros y establecimientos hospitalarios y establece el contenido, conservación y expurgo de sus documentos.

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Real Decreto 170/2010, de 19 de febrero, por el que se aprueba el Reglamento de centros de reconocimiento destinados a verificar las aptitudes psicofísicas de los conductores.

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles.

Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

Ley 5/2014, de 4 de abril, de Seguridad Privada.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.

Roles dentro de la entidad

Deberá existir un registro de cada uno de los roles existentes en materia de protección de datos. Se deberá dejar constancia en todo momento de los posibles cambios que se puedan producir en las siguientes figuras:

Responsable del Tratamiento

La persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Encargado del tratamiento

La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Con cada uno de los encargados del tratamientos de datos existentes se deberá formalizar el pertinente **contrato de encargo**, deberá reunir la siguiente información:

Fecha de celebración.

Identificación de las partes contratantes.

Objeto del contrato.

Delimitación del acceso a los ficheros.

Duración de contrato.

Obligaciones del Encargado y del Responsable del tratamiento.

Autorización para recurrir a otros encargados auxiliares.

Responsabilidades del Encargado.

Planificación de los controles y auditorías.

Confidencialidad.

Notificaciones.

Cláusulas generales de la contratación y jurisdicción aplicable.

Recordar que la Disposición transitoria quinta de la LOPDGDD establece que los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, **hasta el 25 de mayo de 2022.**

Destinatarios

Persona física o jurídica, pública o privada u órgano administrativo, al que se revelan datos.

Corresponsable

Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento.

Entre los corresponsables se deberá formalizar el oportuno contrato que deberá reunir la siguiente información:

- Fecha de celebración.
- Identificación de las partes contratantes.
- Objeto del contrato.
- Delimitación del acceso a los ficheros.
- Duración de contrato.
- Obtención legítima de los contratos de carácter personal.
- Comunicación de datos a terceros.
- Obligaciones de los corresponsables del tratamiento.
- Planificación de los controles y auditorías.
- Confidencialidad.
- Incumplimiento y responsabilidad.
- Notificaciones.
- Información sobre protección de datos de los contratantes.
- Cláusulas generales de la contratación y jurisdicción aplicable.

Usuarios internos

Persona física ligada a la empresa u organización que tiene acceso a ciertos datos personales. Se deberá registrar la siguiente información: datos identificativos, cargo, ubicación departamento, categoría de datos a los que tiene acceso, su identificación de usuario, si ostenta permisos, etc.

Actividades de tratamientos de datos personales

Cuando nos referimos al tratamiento de datos personales nos apoyamos en la definición establecida en el artículo 4 RGPD, donde se define como *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"*.

En base a esta definición se deberá identificar cada tratamiento de datos personales llevado a cabo. Una vez identificado, se deberá describir el tratamiento en cuestión: definir los roles (responsable, encargado, destinatario, etc.) de cada tratamiento, unidad de negocio que realiza el tratamiento, la finalidad, base de legitimación, sistema de tratamiento, tecnología utilizada, duración del tratamiento, normativa aplicable, medidas técnicas y organizativas establecidas para el mismo, etc.

Identificado y descrito el tratamiento de datos, debemos realizar la misma actividad descriptiva pero centrándonos en la categoría de datos personales tratados. Se deberá especificar: la actividad de tratamiento, la categoría de datos tratados, si pertenece a los datos de categorías con una especial protección, la sensibilidad de dicha información, nivel de riesgo por categoría de datos e interesados en la información.

Por último, se deberá describir todas las transferencias internacionales de datos que se realicen en cada uno de los tratamientos. Indicar cómo se lleva a cabo la transferencia, los datos transferidos, el país al que se transfieren, si la transferencia se ha basado en garantías adecuadas, normas corporativas vinculantes (BCR) o, por el contrario, se fundamenta en alguna excepción del artículo 49 RGPD. Se deberá registrar toda la documentación referente a las transferencia internacionales, especialmente, las cláusulas contractuales tipo celebradas entre responsables de tratamientos y entre éstos y los encargados del tratamiento.

Registro de las actividades del tratamiento

Las empresas u organizaciones que empleen a menos de 250 personas no estarán obligadas a llevar un registro de las actividades del tratamiento efectuadas por las mismas, salvo que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales o datos personales relativos a condenas e infracciones penales.

El registro deberá contener la información siguiente:

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.

Los fines del tratamiento.

Una descripción de las categorías de interesados y de las categorías de datos personales.

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.

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 49.1 del RGPD la documentación de garantías adecuadas.

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

A modo de ejemplo, representamos el registro de la actividad del tratamiento de datos personales llevado a cabo en materia de videovigilancia:

TRATAMIENTO: **VIDEOVIGILANCIA**	
Responsable del tratamiento	Identidad: **Confederación Canaria de Empresarios** - NIF: **G35057595** Dirección Postal: **Calle León y Castillo 54,2º, 35003 Las Palmas de Gran Canaria** Correo electrónico: **comunicacion@ccelpa.org** Teléfono: **928 383 500**
Finalidad del tratamiento	**Seguridad de las personas y bienes**
Categoría de interesados	**Personas que accedan o intenten acceder a las instalaciones**
Categoría de datos	**Imágenes**
Categoría de destinatarios	**Fuerzas y Cuerpos de Seguridad**
Transferencias Internacionales	**No está previsto realizar transferencias internacionales**
Plazo de supresión	**Un mes desde su grabación**
Medidas de seguridad	**Las reflejadas en nuestra política de protección de datos y en el manual de medidas de seguridad del responsable del tratamiento**

En este caso se ha realizado un registro individual del tratamiento para ejemplificarlo y que sea más sencillo observar el contenido mínimo exigido. No obstante, el registro de actividades se podrá llevar acabo en un único documento especificando cada uno de los tratamientos realizados por la empresa u organización e incluyendo los datos anteriores para cada uno de éstos tratamientos.

FASE III

Evaluación de impacto

FASE III

Evaluación de impacto

Evaluación de impacto

En base al artículo 35 del RGPD, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento de datos personales cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines entrañe un alto riesgo para los derechos y libertades de las personas físicas.

La Agencia Española de Protección de Datos presentó, el pasado mes de julio, una nueva herramienta denominada **Gestiona_EIPD** a través de la cual se podrá realizar análisis de riesgos y evaluaciones de impacto en los supuestos en los que se traten datos considerados especialmente protegidos.

En líneas generales, se deberá realizar evaluación de impacto si la actividad ejercida se encuentra enmarcada en el alguna de las siguientes: sanidad, solvencia patrimonial y crédito, generación y uso de perfiles, actividades políticas, sindicales o religiosas, servicios de telecomunicaciones, seguros, entidades bancarias y similares, publicidad y videovigilancia masiva.

Las evaluaciones de impacto se deberán realizar por cada uno de los tratamientos de datos personales llevados a cabo dentro de la empresa u organización que impliquen el alto riesgo indicado anteriormente. Además, la evaluación de impacto deberá abordar los datos personales tratados, el tratamiento realizado, el responsable del tratamiento, a lo encargados si existiesen, a la finalidad del tratamiento y a la base de legitimación de dicho tratamiento.

El artículo 35.7 del RGPD determina el contenido mínimo que deberá incluir una evaluación de impacto en protección de datos (EPID), se debe incorporar:

a Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento.

b Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c Una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1.

d Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Seguidamente y a modo ejemplificativo, analizamos los cuatro apartados del precepto anterior que conforman el contenido mínimo de una EIPD:

1 Análisis de la necesidad de la EIPD

CONDUCTA	RESPUESTA / JUSTIFICACIÓN	NECESIDAD EIPD
¿Se tratan datos personales relativos a afiliación sindical, datos genéticos, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de la persona física?	Sí. Actualmente, se tratan datos de salud con la finalidad de medicina preventiva de los pacientes.	SI
¿Se tratan datos personal relativos a menores de edad?	Sí, entre nuestros pacientes se encuentran menores de edad. Sin embargo, la finalidad de dicho tratamiento es de medicina preventiva.	SI

2 Análisis de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad

CONDUCTA	RESPUESTA / JUSTIFICACIÓN
Indicar la finalidad declarada a la que se van a destinar los datos personales recogidos.	Sí. Actualmente, se tratan datos de salud con la finalidad de medicina preventiva de los pacientes.
Indicar si los datos personales recogidos se tratarán para otra finalidad	Sí, exclusivamente se van a destinar a la finalidad declarada.
Indicar si se ha respetado el principio de minimización de los datos personales.	Sí, sólo se han recogido los datos necesarios para alcanzar la finalidad trasladada.
Indicar si la tecnología empleada para llevar a cabo el tratamiento de datos garantiza la seguridad de la información.	Sí. Actualmente, los datos personales se gestionan a través de un sistema cloud delimitado al espacio de la UE y con todas las garantías para salvaguardar la seguridad de la información.
Indicar si el plazo de conservación de la información es el adecuado para garantizar la finalidad declarada.	Sí, la conservación de los datos de los pacientes respeta lo establecido en laLey 41/2002 de 14 de noviembre.

3 Evaluación de los riesgos

Con respecto a nuestro supuesto donde se tratan datos de salud, hemos identificado a modo ejemplificativo los siguientes riesgos:

RIESGO IDENTIFICADO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL
No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender.	Limitada	Máximo	**Medio**
Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos.	Limitada	Máximo	**Medio**
Fugas de información.	Significativa	Máximo	**Alto**
Violaciones de la confidencialidad de los datos personales por parte de los empleados o personal externo de la organización.	Significativa	Máximo	**Alto**

4 Medidas previstas para afrontar los riesgos detectados

RIESGO IDENTIFICADO	MEDIDAS A ADOPTAR
No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender.	Reciclaje formativo en protección de datos personales dado que este riesgo sólo se ha detectado en una ocasión este año.
Errores a la hora de recabar el consentimiento de los pacientes.	Reciclaje formativo en protección de datos personales dado que este riesgo sólo se ha detectado en una ocasión este año.
Fugas de información.	- Formación en seguridad de la información. - Revisión de los derechos de acceso de los usuarios. - Restricción de acceso a la información. - Controles de red. - Revisar las cláusulas de confidencialidad.
Violaciones de la confidencialidad de los datos personales por parte de los empleados o personal externo de la organización.	- Formación en seguridad de la información y protección de datos. - Revisar nuestro procedimiento disciplinario. - Revisar la política de control de acceso. - Revisar los derechos de acceso de los usuarios. - Retirar o adaptar los derechos de acceso.

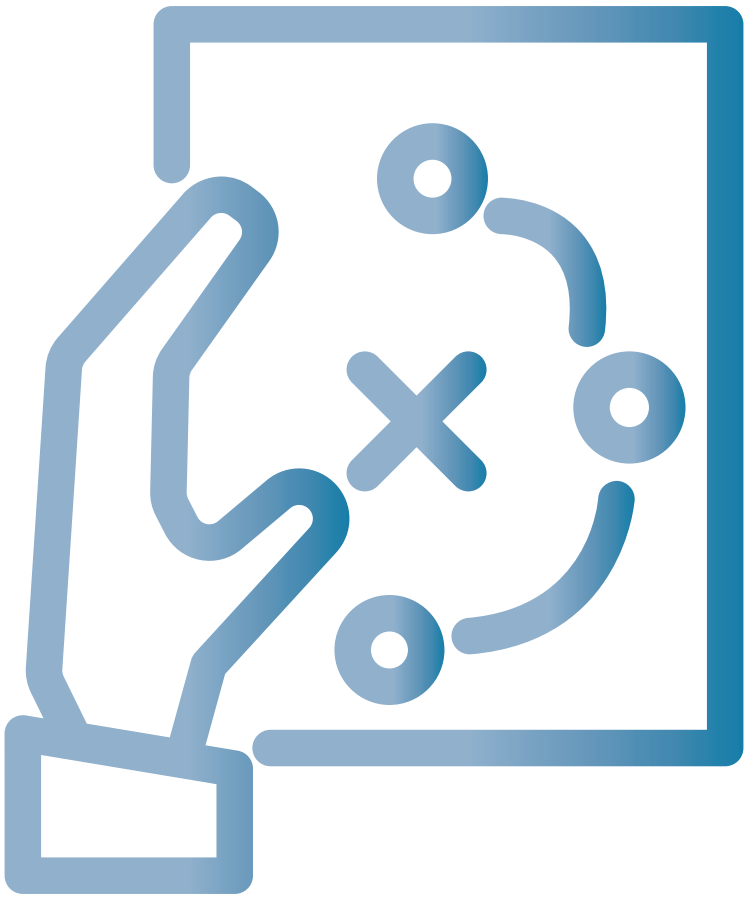
FASE IV

Gestión de riesgos y medidas de seguridad

Análisis, identificación y evaluación del riesgo potencial

Matriz de riesgo

Plan de acción



FASE IV

Gestión de riesgos y medidas de seguridad

Análisis, identificación y evaluación del riesgo potencial

Tras la correcta identificación de los posibles riesgos a los que se expone la empresa u organización, se analizarán los mismos. El análisis se realizará combinando la probabilidad de su materialización y el impacto que puede producir en ellas.

El análisis del riesgo es uno de los elementos en los que se sustenta cualquier modelo de prevención y control de la Privacidad de la Información. Su principal función es identificar las actividades que pueden entrañar un riesgo que vulnere el derecho fundamental de protección de datos de los interesados.

Identificado el riesgo se tendrá que especificar la causa de su origen y la relación de las conductas inapropiadas que lo generan.

La valoración del riesgo se realizará teniendo en cuenta los dos elementos que lo componen: probabilidad e impacto. Ambas magnitudes se valorarán en una escala del 1 al 4, siendo 4 la valoración más alta. En este punto, es fundamental introducir la siguiente leyenda para poder interpretar los valores otorgados:

PUNTUACIÓN	VALORACIÓN PROBABILIDAD E IMPACTO
1	Despreciable
2	Limitada
3	Significativa
4	Máxima

Una vez obtenido el nivel de priorización del riesgo, se procederá a la justificación de la valoración imputada a la probabilidad de que dicho riesgo se produzca y a la justificación de las consecuencias que podrían acarrear para las anteriores si se llegara a materializar el mismo.

Una vez obtenido el nivel de priorización del riesgo, se procederá a la justificación de la valoración imputada a la probabilidad de que dicho riesgo se produzca y a la justificación de las consecuencias que podrían acarrear para las anteriores si se llegara a materializar el mismo.

Matriz de riesgo

La matriz de riesgo es la representación gráfica de la información obtenida en la fase anterior de análisis de riesgos. Esta información será el punto de partida para el diseño de medidas de vigilancia y control idóneas y eficaces que permitan reducir el riesgo de posibles brechas de seguridad de la información.

MATRIZ DE RIESGO

ACTIVIDAD INAPROPIADA	PROBABILIDAD	IMPACTO	RIESGO INHERENTE	NIVEL DE RIESGO
Acceso no autorizado a datos personales	3	3	9	GRAVE
Errores al recabar el consentimiento de los usuarios	4	4	16	MUY GRAVE

Existirán los siguientes riesgos:

Riesgo muy grave: Cuando el valor obtenido del producto anterior (Probabilidad x Impacto) sea superior a 9.

Riesgo grave: Cuando el valor obtenido del producto anterior (Probabilidad x Impacto) sea superior a 6 y menor o igual que 9.

Riesgo moderado: Cuando el valor obtenido del producto anterior (Probabilidad x Impacto) sea superior a 2 y menor o igual que 6.

Riesgo Leve: Cuando el valor obtenido del producto anterior (Probabilidad x Impacto) se sitúe entre 1 y 2.

El riesgo inherente es el riesgo existente ante la ausencia de alguna acción que pueda alterar tanto la probabilidad o el impacto del mismo. Detectado el mismo, lo fundamental es confirmar si la empresa u organización era conocedora de éste y si ha implantado algún tipo de control con el fin de aminorarlo.

El resultado obtenido en la fase de análisis, y representado en la matriz de riesgo, se deberá incluir en el ***Informe de riesgo***. A través de este documento se justificará la identificación de los riesgos potenciales y el procedimiento de cómo se ha llegado a esa conclusión.

Plan de acción

Los planes de acción son documentos que especifican las actividades que se realizarán en un plazo de tiempo determinado.

Los planes se deben elaborar antes de realizar una acción determinada con el objetivo de dirigirla y encauzarla. En este sentido, el **"Plan de Acción"** nos sirve para poner en conocimiento cómo se gestionarán los riesgos identificados mediante un conjunto de acciones, las cuales deben ser aprobadas por el órgano de gobierno.

Ante cualquier riesgo existen diferentes formas de gestionarlo, entre ellas:

Evitar el riesgo, no iniciando o no continuando con la actividad que lo genera.

Aceptar el riesgo o incluso aumentarlo para aprovechar una oportunidad.

Eliminar la fuente del riesgo.

Modificar la probabilidad.

Cambiar las consecuencias.

Compartir el riesgo

Mantener el riesgo.

Establecer métodos de seguimiento, medición, análisis y evaluación para asegurar resultados válidos.

En el "Plan de Acción" es donde se recogerán los métodos de seguimiento, medición, análisis y evaluación del riesgo. Las acciones contempladas en él deberán llevarse a cabo en un período determinado de tiempo para reforzar progresivamente el sistema de gestión de protección de datos personales. En definitiva, se realizará un estudio profundo de la medida impuesta, se describirá el procedimiento empleado, se justificará la adopción de esa en lugar de otra y, por último, se valorará la eficacia del control y de la eficiencia de la implantación.

Por último, tras elaborar y aprobar el plan de acción, obtendremos el riesgo residual, es decir, el nivel de riesgo que permanece en la entidad tras mitigar el mismo con la aplicación de los controles.

Seguidamente, presentamos el contenido mínimo que se debería incluir en cualquier plan de acción para poder dejar constancia de cómo se gestionarán los riesgos identificados.

RIESGO IDENTIFICADO	NPR	RIESGO RESIDUAL	ÁREA DE NEGOCIO	TIPO DE ACCIÓN	DESCRIPCIÓN DE ACCIÓN	IMPLANTACIÓN	EVALUACIÓN	COSTE ACCIÓN
Violaciones de la confidencialidad de los datos personales por parte de los trabajadores de la empresa u organización.	8	3	RRHH	Preventiva	Formación adecuada de los empleados sobre sus obligacionesy responsabilidades respecto a la confidencialidad de la información e implantar un sistema disciplinario.	01/06/2019	01/01/2020	350€

FASE V

Medidas técnicas y de seguridad

FASE V

Medidas técnicas y de seguridad

Introducción

En esta fase se deberán identificar y procedimentar el conjunto de medidas organizativas y técnicas adoptadas por el responsable del tratamiento de conformidad con el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamientos, con el fin de garantizar un nivel de seguridad adecuado a los riesgos identificados en la fase anterior.

Manual de medidas de seguridad del responsable del tratamiento

El presente Manual tiene por objeto desarrollar las medidas de seguridad aplicables a los datos personales de los que la empresa u organización es responsable del tratamiento, con independencia del sistema de tratamiento utilizado (informático, manual o mixto), de conformidad con la normativa aplicable.

El contenido del mismo se estructurará en :

Definir el objeto del manual.

Marco legal.

Ámbito de Aplicación.

Términos y definiciones.

Políticas, procedimientos y controles de seguridad de los datos personales, entre los que podemos destacar los siguientes:

Clasificación de los datos personales.

Análisis del riesgo de los datos personales.

Inventarios de datos personales y sistemas de información.

Registro de los medios de almacenamiento de datos personales.

Identificación y Autentificación.

Gestión de soportes y criterios de archivo.

Copias de seguridad.

Confidencialidad de los datos personales.

Gestión de incidencias que afectan a los datos personales.

Violaciones de la seguridad de los datos personales.

Auditoría de las medidas de seguridad.

Revisión y actualización del documento de seguridad.

Anexos: En este apartado del manual se podrá incluir los siguientes mecanismos de control/seguridad:

Inventario de datos personales

INVENTARIO DE DATOS PERSONALES CCE			
CATEGORÍA DE DATOS TRATADOS	**EXISTENTE**	**NECESARIO TRATAMIENTO**	**NO NECESARIO TRATAMIENTO**
DATOS IDENTIFICATIVOS Y DE CONTACTO			
Nombre			
Estado Civil			
Lugar de nacimiento			
Fecha de nacimiento			
Nacionalidad			
Domicilio			
Teléfono particular			
Móvil			
Correo electrónico			
Firma autógrafa			
Firma electrónica			
Edad			
Fotografía			
DATOS CARACTERÍSTICAS FÍSICAS			
Color de piel			
Color de iris			
Color de cabello			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
DATOS BIOMÉTRICOS			
Imagen del iris			
Huella dactilar			
Palma de la mano			
DATOS LABORALES			
Cargo desempeñado			
Domicilio de trabajo			
E-mail institucional			
Teléfono institucional			
Referencias laborales			
Experiencia laboral			
Información obtenida del proceso selectivo			
DATOS ACADÉMICOS			
Trayectoria educativa			
Títulos			
Certificados			
Reconocimientos			

(sigue)

INVENTARIO DE DATOS PERSONALES CCE			
CATEGORÍA DE DATOS TRATADOS	**EXISTENTE**	**NECESARIO TRATAMIENTO**	**NO NECESARIO TRATAMIENTO**
DATOS PATRIMONIALES / FINANCIEROS			
Bienes muebles			
Bienes inmuebles			
Información Fiscal			
Historial crediticio			
Ingresos			
Cuentas bancarias			
Número de tarjetas de crédito			
Información adicional de tarjetas			
Seguros			
DATOS TIEMPO LIBRE			
Deportes			
Aficiones			
Pasatiempos			
DATOS LEGALES			
Juicios			
Procesos administrativos			
Causas pendientes			
Embargos			
Ejecución de sentencias			
DATOS ESPECIALMENTE PROTEGIDOS			
DATOS IDEOLOGÍA			
Creencias religiosas			
Creencias políticas			
Simpatizante de partidos			
Afiliación a un sindicato			
DATOS SALUD			
Estado actual de salud			
Enfermedades padecidas			
Discapacidad			
Información genética			

Registro de los medios de almacenamiento de datos personales

REGISTRO DE LOS MEDIOS DE ALMACENAMIENTO DE DATOS PERSONALES CCE			
FORMATO ALMACENAMIENTO	**FÍSICO**	**ELECTRÓNICO**	**PERSONA CON PRIVILEGIOS DE USO**
Correspondencia / email			
Formularios			
Copias de documentos de identificación			
Solicitudes de pedidos			
Facturas			
Bases de datos			
Hojas de cálculo			
Contratos			
Expedientes			
Servidor			
Discos duros			
Pendrive			
Audios / Videos			
Otros			

Inventario de soportes de almacenamiento de datos personales

INVENTARIO DE SOPORTES DE ALMACENAMIENTO DE DATOS PERSONALES CCE					
TIPO DE SOPORTE	**NÚMERO DE REGISTRO**	**FECHA DE ENTRADA**	**UBICACIÓN**	**USUARIO INICIALES**	**CARGO CCE**
PC	00001		León y Castillo, 54		
P	00002		León y Castillo, 89		
P			Pedro de Vera, 19		
P					
P					
P					
P					
P					
PC					
PC					
PC					
Pendrive					
Portátiles					

PC
Portátiles
Tablet
Móvil
Discos duros
Pendrive
Servidores

Autorización de salida de soportes con información en materia de datos personales

AUTORIZACIÓN DE SALIDA DE SOPORTES FUERA DE LAS INSTALACIONES DE LA CCE	
Sede institucional:	
Fecha de la Salida:	

Información del Soporte	
Identificación	
Contenido	
Fichero de procedencia	
Fecha de creación	

Finalidad y Destino de la Extracción del Soporte	
Finalidad	
Destino	
Destinatario	

Forma de Remisión del Soporte	
Canal de envío	
Remitente	
Observaciones de envío	

Autorización de la Extracción	
Autorizante	
Cargo en la CCE	
Observaciones	

Firma:

Modelo de registro de incidencias y formato para la notificación interna

FORMULARIO DE NOTIFICACIÓN DE INICIDENCIAS	
Sede institucional:	
Nombre del Comunicante:	
Fecha Incidencia:	
Hora Incidencia:	
Nº Registro Incidencia:	

Descripción de Incidencia

Destinatario de la Notificación

Efectos de la Brecha de Seguridad

Medidas adoptadas por el Comunicante

Medidas adoptadas por el Responsable del Tratamiento

Firma:

Listado de empleados con acceso al tratamiento de datos personales

USUARIOS CON ACCESO AL TRATAMIENTO DE DATOS PERSONALES			
RESPONSABLE DE SEGURIDAD O PERSONA QUE LE SUSTITUYA			
Apellidos y nombre	**Cargo en la CCE**	**Fecha Alta**	**Fecha Baja**

EMPLEADO CON ACCESO AL FICHERO DE DATOS PERSONALES			
Apellidos y nombre	**Cargo en la CCE**	**Fecha Alta**	**Fecha Baja**

Firma Responsable Seguridad o equivalente

Autorización para recuperación de datos

FORMULARIO DE RECUPERACIÓN DE DATOS	
Sede institucional:	
Fecha solicitud:	
Hora solicitud:	
Nº Registro Solicitud:	(a cumplimentar por el Responsable del Tratamiento o su equivalente)

Información de la Solicitud de Recuperación de Datos	
Apellidos y nombre del Solicitante	
Apellidos y nombre del Responsable del tratamiento o su equivalente	

Datos a restaurar	
Tratamiento objeto de recuperación	
Identificación del Soporte	
Datos	
Ubicación	
Servidor	

Tramitación de la solicitud

☐ **APROBACIÓN** ☐ **DENEGACIÓN**

Firma del Solicitante:

Registro de ejercicio de derechos ARSOPOL

Registro de Ejercicio de Derechos ARSOPOL						
Nº SOLICITUD	SEDE	CANAL DE RECLAMACIÓN	DIA DE ENTRADA	DERECHOS EJERCIDOS	DIA DE RESPUESTA	CANAL DE RESPUESTA

Manual de medidas de seguridad del encargado del tratamiento

En base al principio de responsabilidad proactiva y al deber de diligencia que ostenta el responsable del tratamiento a la hora de elegir a los encargados del tratamientos con los que se formalizará una relación de prestación de servicios, se exigirá al primero que adopte todas las cautelas necesarias para acreditar que el encargado seleccionado cumple con la actual normativa en materia de protección de datos. Dentro de estas medidas se encuentra la posibilidad de solicitar el acceso a su manual de seguridad para ratificar que tienen implantados protocolos de seguridad adaptados a los más exigentes estándares de seguridad de la información.

FASE VI

Canal de denuncias

FASE VI

Canal de denuncias

El canal interno de denuncia es un mecanismo que deberá ser establecido por el órgano competente de la empresa u organización, a disposición de los trabajadores o de terceros ajenos a la entidad, para facilitar la comunicación de cualquier presunta conducta contraria a la presente normativa en materia de protección de datos.

El canal de denuncias, como elemento clave de los programas de cumplimiento normativos, contribuye a:

- Prevenir conductas irregulares y/o actividades ilícitas.
- Generar una cultura corporativa basada en la integridad y la gestión responsable.
- Manifestar tolerancia cero ante cualquier práctica inapropiada o ilegal.
- Identificar posibles conflictos internos.
- Demostrar la existencia de un modelo organizativo de vigilancia y control para evitar los mismos.

La entidad definirá, en función de su estructura y de sus necesidades, el procedimiento para la recepción, clasificación y tramitación de las denuncias, así como las funciones y responsabilidades de cada una de las personas involucradas en el proceso de investigación y resolución de éstas.

Una de las cuestiones más importantes dentro del canal de denuncias es regular la protección tanto de la persona denunciante como de la persona investigada. Por lo que se garantizará, en todo momento, la presunción de inocencia, la confidencialidad y la prohibición de represalias al denunciante que actúa de buena fe.

El éxito de la implantación de un canal de denuncias radica en la comunicación y en la formación puesta a disposición del personal, consiguiendo interiorizar la importancia de poner en conocimiento las posibles acciones ilícitas o irresponsables a su responsable o coordinador.

Además, se evaluará y se realizará seguimiento al funcionamiento del sistema. Esta labor es de gran importancia dado que se obtendrá información fundamental para la compañía, entre otras:

Volumen de denuncias.

Acciones inapropiadas más habituales.

Riesgos asociados a las conductas inapropiadas.

Duración media en la tramitación de los expedientes.

Acciones realmente probadas.

Reincidentes en la comisión de acciones no apropiadas.

Por último y al igual que en el resto de fases del procedimiento de cumplimiento normativo, se deberán recabar evidencias de los esfuerzos realizados para asegurar el correcto funcionamiento del canal de denuncias, sin esta labor de seguimiento no se podrá justificar nuestra actuación preventiva al riesgo. En consecuencia, se deberá justificar en todo momento que se han llevado a cabo todas las acciones existentes a nuestro alcance para evitar cualquier brecha de seguridad que ponga en riesgo la seguridad de la información en materia de protección de datos personales.

Recientemente, se ha publicado la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. La presente Directiva tiene por objeto reforzar la aplicación del Derecho y las políticas de la Unión en ámbitos específicos mediante el establecimiento de normas mínimas comunes que proporcionen un elevado nivel de protección de las personas que informen sobre infracciones del Derecho de la Unión.

En la materia que nos ocupa en este manual, dicha directiva será aplicable a las infracciones cometidas en materia de intimidad personal, protección de datos, seguridad de las redes y los sistemas de información. **Las empresas privadas con 50 o más trabajadores** estarán obligadas a la implementación de un canal interno de denuncias, por lo que realizaremos un seguimiento a esta normativa con el fin de conocer los medios y las formas que serán empleados por nuestra autoridad nacional para alcanzar los objetivos fijados en este acto legislativo.

FASE VII

Planes de formación

FASE VII

Planes de formación

La formación del personal en materia de protección de datos y seguridad de la información se sitúa en una posición fundamental dentro del programa de Compliance de la entidad. Al diseñar el plan de acción formativa se deberá garantizar que la información facilitada provoque la reflexión y el compromiso de todos los miembros a garantizar el cumplimiento de la normativa vigente.

La formación continua es una necesidad para cumplir con los requisitos marcados para la implementación de un sistema de gestión en Privacidad de la Información. Estar actualizado en todas las novedades normativas que regulan la materia que nos ocupa es una de las principales herramientas para evitar cualquier conducta inapropiada por desconocimiento de la normativa. Además, la formación es el canal apropiado para facilitar el entendimiento de la regulación existente a todo el personal ya que todos no tendrán la condición de especialistas en protección de datos y seguridad de la información.

En la planificación de la formación tiene gran impacto el código ético, dejando constancia que la empresa u organización respeta sus principios éticos en la toma de sus decisiones. Las iniciativas de sensibilización y formación para ser más eficaces deben estar tan consensuadas como sea posible. Es imprescindible conseguir que éstas sean respetadas desde el órgano de gobierno al resto de la entidad, el hecho de que todos los miembros sean partícipes debe inspirar el programa formativo en materia de cumplimiento en protección de datos de carácter personal.

Los principales bloques de contenido en las actividades de formación y sensibilización serán:

- Referentes a nuestra política de protección de datos y a las medidas de seguridad técnicas y organizativas.
- Gobernanza y gestión del riesgo.
- Responsabilidad económica.
- Pérdida de la reputación institucional y descrédito ante la sociedad.

La metodología para impartir dicha formación podrá adecuarse a formato presencial, e-learning, coaching, folletos con mensajes directos que eviten acciones inapropiadas y avisos popups. Sin embargo y como es fundamental en todas las acciones llevadas a cabo en el programa de cumplimiento, se deberá dejar constancia de la trazabilidad de la formación impartida. En todo momento se deberá recoger evidencias de las personas que asistieron, de los materiales facilitados en la formación e incluso de los utilizados en la sesión formativa. Con estas acciones podremos conseguir la máxima trazabilidad por lo que se deberá ser riguroso con las convocatorias y el seguimiento de asistencia de las formaciones.

Bibliografía y otras fuentes de información

Agencia Española de Protección de Datos (AEPD).
Accesible online: https://www.aepd.es/

Agencia Estatal Boletín Oficial del Estado (BOE).
Accesible online: https://www.boe.es/diario_boe/

Asociación Española de Compliance (ASCOM).
Accesible online: https://www.asociacioncompliance.com/

Asociación Española de Compliance (ASCOM). "Libro blanco sobre la función de compliance". 2017.
Accesible online:
https://www.asociacioncompliance.com/wp-content/uploads/2017/08/Libro-Blanco-Compliance-ASCOM.pdf

Ayuso, S. y Garolera, J. **"Códigos éticos de las empresas españolas: un análisis de su contenido". 2011**.
Accesible online: http://mango.esci.upf.edu/DOCS/Documents-de-treball/10-Codigos-eticos.pdf

Comisión especial para el fomento de la transparencia y la seguridad en los mercados financieros y las sociedades cotizadas. "Informe de la Comisión especial para el fomento de la transparencia y la seguridad en los mercados financieros y las sociedades cotizadas". 2003.
Accesible online:https://www.cnmv.es/DocPortal/Publicaciones/CodigoGov/INFORMEFINAL.PDF

Comisión Nacional del Mercado de Valores (CNMV). "Código de buen gobierno de las sociedades cotizadas". 2015.
Accesible online: https://www.cnmv.es/docportal/publicaciones/codigogov/codigo_buen_gobierno.pdf

Confederación Española de la Pequeña y Mediana Empresa (CEPYME). "Guía de buen gobierno buen gobierno para empresas pequeñas y medianas". 2018.
Accesible online: https://www.cepyme.es/wp-content/uploads/2018/02/Gu%C3%ADa-Buen-Gobierno-Pymes.pdf

Confederación Provincial de Empresarios de Santa Cruz de Tenerife (CEOE-Tenerife).
Accesible online:https://ceoe-tenerife.com/compliance/

Consejo General de la Abogacía Española.
Accesible online: https://www.abogacia.es/

Fundación General Universidad Granada – Empresa. "La gestión documental en el entorno del compliance". 2017.
Accesible online:
http://cef-ugr.org/wp-content/uploads/2017/03/21-Jose-Antonio-Merino-b-2.pdf

Gobierno de su Majestad (Gobierno del Reino Unido). "Bribery Act 2010". 2010.
Accesible online: https://www.legislation.gov.uk/ukpga/2010/23/contents

Hermoso de Mendoza Sáinz de Ugarte, J. **"Legal Compliance: El manual de prevención de riesgos penales". 2018.**
Accesible online:https://academica-e.unavarra.es/bitstream/handle/2454/27435/114542.%20T.F.M.%20HERMOSO%20DE%20MENDOZA.pdf?sequence=1&isAllowed=y

Jiménez, A., Marín, L., y Campos, L. **"Guía práctica de autodiagnóstico y compliance para entidades sociales". 2018.**
Accesible online:https://web.icam.es/bucket/Gu%C3%ADa%20pr%C3%A1ctica%20autodiagn%C3%B3stico%20y%20compliance%20para%20entidades%20sociales%20Final.pdf

Kaptein, M. **"Business Codes of Multinational Firms: What Do They Say?" 2004.**
Accesible online:https://www.researchgate.net/publication/320597524_Business_codes_of_multinational_firms_What_do_they_say

KPMG. "Blog: KPMG cumplimiento legal".
Accesible online:https://www.tendencias.kpmg.es/blog/kpmg-cumplimiento-legal/

Lefebvre El Derecho. "Contratación pública". 2018.
Accesible online: https://www.efl.es/catalogo/ebooks-gratuitos/contratacion-publica

Lefebvre El Derecho. "UNE 19601: 2017 Sistemas de gestión de Compliance Penal. Requisitos con orientación para su uso". 2017.
Accesible online:https://www.efl.es/catalogo/ebooks-gratuitos/une-19601-2017-compliance-penal

OECD. "Ética Anticorrupción y Elementos de Cumplimiento Manual para Empresas". 2013.
Accesible online:http://www.oecd.org/daf/anti-bribery/Etica-Anticorrupcion-Elementos-Cumplimiento.pdf

OECD. "Líneas Directrices de la OCDE para Empresas Multinacionales". 2011.
Accesible online: http://www.oecd.org/daf/inv/mne/MNEguidelinesESPANOL.pdf

Pacto Mundial de las Naciones Unidas. "10 principios".
Accesible online: https://www.pactomundial.org/category/aprendizaje/10-principios/

Ribas y Asociados. "Códigos éticos y líneas rojas penales". 2015.
Accesible online: https://xribasdotcom.files.wordpress.com/2015/04/estudio-cc3b3digos-c3a9ticos-ibex-35.pdf

Thomson Reuters " Practicum Compliance 2018"

Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (Sepblac).
Accesible online:https://www.sepblac.es/es/sobre-el-sepblac/

Departamento de Justicia del Gobierno de los Estados Unidos. "Evaluation of Corporate Compliance Programs".
Accesible online:https://www.justice.gov/criminal-fraud/page/file/937501/download

Wolters Kluwer.
Accesible online: http://guiasjuridicas.wolterskluwer.es/Content/Inicio.aspx

CONFEDERACIÓN CANARIA DE EMPRESARIOS

ceoe CEPYME

Financiado por:

Gobierno de Canarias
Consejería de Economía, Conocimiento y Empleo