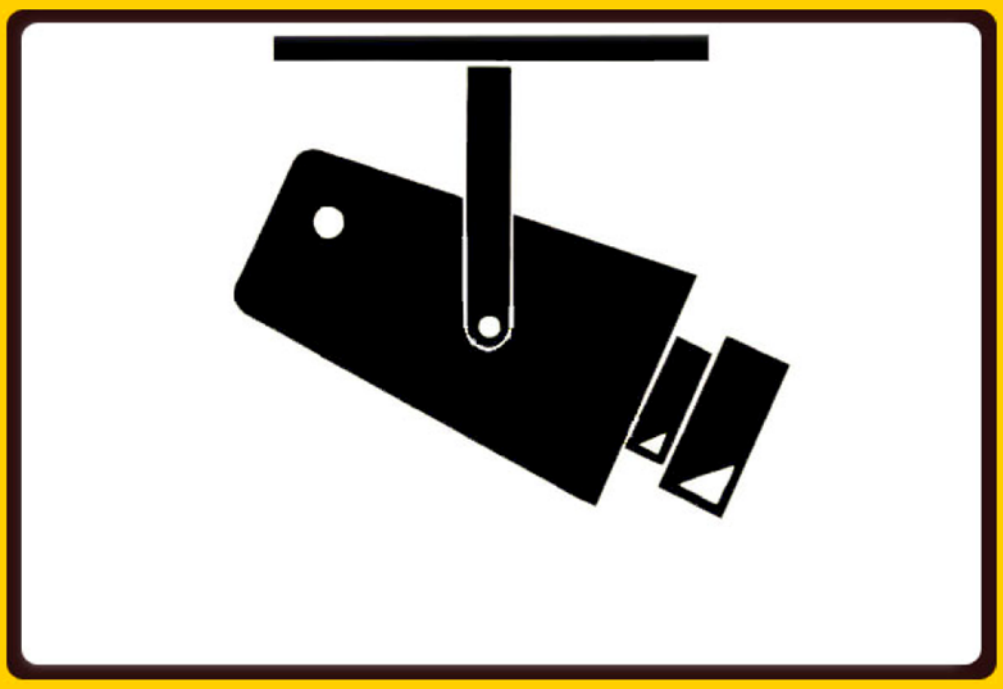
agencia española protección datos

RGPD HERRAMIENTA PARA TRATAMIENTOS DE EMPRENDEDORES EMPRENDE

Documentación

Distintivo informativo de zona videovigilada
Cláusulas informativas y Política de Privacidad
Contratos con encargados del tratamiento
Registro de actividades de tratamiento
Directrices para la atención de solicitudes de ejercicio de derechos
Recomendaciones sobre videovigilancia
Indicaciones en materia de gestión de riesgos
Estrategias de privacidad y medidas de seguridad
Directrices para la gestión de brechas de seguridad
Indicaciones y directrices con relación a las actividades que desarrolla
Recomendaciones de prevención del acoso digital

ZONA VIDEOVIGILADA



RESPONSABLE:

TELEMAN COMUNICACIONES S.L - B30695951

PUEDE EJERCITAR SUS DERECHOS DE PROTECCIÓN DE DATOS ANTE:

TELEMAN COMUNICACIONES S.L
Calle Manzano n7 30593 La Palma Cartagena Murcia
Correo electrónico: calle Manzano n7

MÁS INFORMACIÓN SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES:

Finalidad del tratamiento: Seguridad de las personas, bienes e instalaciones
Interesados: Personas que acceden a las instalaciones
Destinatarios: Fuerzas y Cuerpos de Seguridad
Plazo de conservación: 1 mes desde la captación

DOCUMENTACIÓN A REVISAR

Este documento, resultado de haber ejecutado la herramienta FACILITA EMPRENDE, tiene por objetivo ofrecerle material de apoyo en el cumplimiento de la normativa vigente en materia de protección de datos. En este sentido, incluye

1 un ejemplo de política de información en dos niveles, compuesta por las cláusulas informativas a proporcionar en el momento de la recogida de datos y que deberán ser enlazadas al documento de política de privacidad que también se proporciona.

2 si su empresa utiliza cookies o tecnologías equivalentes en la página web, un ejemplo de aviso de uso de cookies que deberá ser enlazado al documento de política de cookies que se incluye.

3 las cláusulas contractuales, en materia de protección de datos, a anexar a cada uno de los contratos de prestación de servicios que suscriba con los encargados de tratamiento.

4 el Registro de Actividades de Tratamiento precumplimentado.

5 un modelo de ficha de anotación de incidentes de seguridad para componer el registro de incidentes que debe mantenerse en cumplimiento del artículo 33.5 del Reglamento

6 un conjunto de directrices a seguir a la hora de atender las solicitudes de ejercicio de derechos en materia de protección de datos que pueda recibir de los interesados cuyos datos son objeto de tratamiento por parte de su organización.

7 un conjunto de recomendaciones para un correcto tratamiento de las imágenes captadas por las cámaras de videovigilancia junto con el cartel informativo para señalizar la zona videovigilada, ya cumplimentado con los datos del responsable del tratamiento.

8 unas indicaciones respecto a sus obligaciones en materia de gestión de riesgos condicionadas por las características de los tratamientos que esté realizando.

9 un conjunto de recomendaciones en materia de privacidad y seguridad que debe tener en cuenta al desarrollar y prestar servicios a terceros que hagan uso de los datos personales de estos.

10 una serie de recomendaciones para la prevención del acoso digital.

La documentación generada está adaptada a la información facilitada para cada uno de los tratamientos que ha seleccionado al cumplimentar la aplicación. No obstante, **la obtención de estos documentos no implica, de por sí, el cumplimiento automático de las obligaciones impuestas por la normativa**. Es obligación del responsable, y en su caso del encargado, revisar cuidadosamente el documento resultante para adaptarlo y actualizarlo a la situación concreta y específica de los tratamientos que se lleven a cabo en su entidad en cada momento.

Cláusulas informativas y Política de Privacidad

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) establece en su artículo 11 relativo a la "Transparencia e información al afectado" la posibilidad de que el responsable dé cumplimiento al deber de informar facilitando al interesado la información básica relativa al tratamiento e indicando una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. Es decir, se promueve el uso de declaraciones o avisos de privacidad por niveles; mostrando la información más relevante relativa a la identidad del responsable, la finalidad del tratamiento y el modo de ejercer los derechos en una primera capa, para remitir a un segundo nivel o capa, disponible en un único lugar claramente identificado, donde se proporcione el resto de información, de forma detallada, que permita al interesado conocer las características exactas del tratamiento al que están sometidos sus datos.

En este apartado del documento se proporcionan las cláusulas informativas del tratamiento que deberá incluir en los formularios electrónicos o impresos en papel que utilice para recabar datos personales de los distintos interesados vinculados a alguna de las actividades de tratamiento de las que es responsable, así como el modelo de política de privacidad que deberá estar accesible para su consulta en un lugar fácilmente identificable de su página web.

No olvide revisar los textos automáticamente generados y realizar los cambios necesarios para que las cláusulas de información y la política de privacidad respondan con exactitud a la realidad del tratamiento de los datos realizado.

Cláusula informativa de la actividad de tratamiento de empleados

Datos del responsable del tratamiento:

Titular: TELEMAN COMUNICACIONES S.L - NIF: B30695951
Domicilio social: Calle Manzano n7 30593 La Palma Cartagena Murcia
Teléfono: 691231544 - Correo electrónico: info@radiounion.es
Página web: www.radiounion.es
//Sólo si hay DPD: Datos de contacto del DPD: Email DPD

"Los datos proporcionados serán tratados por TELEMAN COMUNICACIONES S.L con la finalidad de mantener la relación laboral. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante TELEMAN COMUNICACIONES S.L, Calle Manzano n7 30593 La Palma Cartagena Murcia o en la dirección de correo electrónico calle Manzano n7, adjuntando copia de su DNI o documento equivalente. Puede ampliar esta información en relación con el tratamiento de sus datos personales consultando nuestra Política de privacidad."

AVISO1: Si del análisis realizado se desprende que su empresa debe tener contratado un Delegado de Protección de Datos, no olvide consignar la dirección de correo electrónico en la que los interesados pueden ponerse en contacto con él.

AVISO2: Recuerde que una vez haya concluido la relación laboral y no haya ninguna obligación legal para mantener los datos, deberá proceder a su bloqueo sin darles uso más allá de su conservación y mantenerlos en este estado mientras puedan ser necesarios para el ejercicio o defensa de reclamaciones o pudiera derivarse algún tipo de responsabilidad que tuviera que ser atendida. Transcurridos los plazos legales para el ejercicio de reclamaciones los datos deberán ser eliminados.

AVISO3: No olvide publicar el documento de política de privacidad en un lugar visible de su página web y enlazarlo desde esta cláusula informativa (o indicar la dirección de la página web en el caso de formularios impresos) para que sea fácilmente accesible para el interesado.

Política de Privacidad

TELEMAN COMUNICACIONES S.L pone a su disposición a través de la página web www.radiounion.es la presente política de privacidad con la finalidad de informarle, de forma detallada, sobre cómo tratamos sus datos personales y protegemos su privacidad y la información que nos proporciona. En caso de introducir modificaciones en un futuro sobre la misma se lo comunicaremos a través de la página web o a través de otros medios de modo que pueda conocer las nuevas condiciones de privacidad introducidas.

En cumplimiento del Reglamento (UE) 2016/679, General de Protección de Datos y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales le informamos de lo siguiente:

Responsable del Tratamiento

Titular: TELEMAN COMUNICACIONES S.L - NIF: B30695951
Domicilio social: Calle Manzano n7 30593 La Palma Cartagena Murcia
Teléfono: 691231544 - Correo electrónico: info@radiounion.es
Página web: www.radiounion.es
/*Sólo si hay DPD
Si tiene cualquier tipo de consulta, duda o sugerencia con relación a cómo usamos sus datos personales puede dirigirse al Delegado de Protección de Datos a través de la dirección de correo electrónico Email DPD***/**

¿Con qué finalidad tratamos sus datos personales?

En TELEMAN COMUNICACIONES S.L recabamos y tratamos su información personal con carácter general para gestionar la relación que mantenemos con Ud. siendo las principales finalidades que tenemos identificadas las siguientes:

- Gestión y contratación de los productos y servicios ofrecidos por nuestra empresa
- Canalizar las solicitudes de información, sugerencias y reclamaciones que nos pueda hacer llegar
- Mantenerle informado sobre eventos, ofertas, productos y servicios que puedan resultar de su interés a través de distintos canales de comunicación siempre y cuando Ud. haya prestado su consentimiento.
- Gestión de la relación laboral, en el caso de nuestros empleados.
- Gestión de la relación comercial mantenida con nuestros proveedores

¿Cómo recabamos su información?

Recabamos su información personal a través de diferentes medios, pero siempre será informado en el momento de la recogida mediante cláusulas informativas sobre el responsable del tratamiento, la finalidad y la base legal del mismo, los destinatarios de los datos y el periodo de conservación de su información, así como la forma en que puede ejercer los derechos que le asisten en materia de protección de datos.

En general, la información personal que tratamos se limita a datos identificativos (nombre y apellidos, fecha de nacimiento, domicilio, DNI, teléfono y correo electrónico), servicios contratados y datos de pago y facturación.

En los casos de gestión y selección de personal recogemos los datos académicos y profesionales para poder atender a las obligaciones derivadas del mantenimiento de la relación laboral o en su caso, entrar a formar parte de nuestra plantilla.

TELEMAN COMUNICACIONES S.L utiliza redes sociales y esta es otra forma de llegar a usted. La información recogida a través de los mensajes y comunicaciones que publica puede contener información personal que se encuentra disponible online y accesible al público. Estas redes sociales cuentan con sus propias políticas de privacidad donde se explica cómo utilizan y comparten su información, por lo que TELEMAN COMUNICACIONES S.L le recomienda que las consulte antes de hacer uso de estas para confirmar que está de acuerdo con la forma en que su información es recogida, tratada y compartida.

Responsabilidad del usuario

Al facilitarnos sus datos a través de canales electrónicos, el usuario garantiza que es mayor de 14 años y que los datos facilitados a TELEMAN COMUNICACIONES S.L son verdaderos, exactos, completos y actualizados. A estos efectos, el usuario confirma que responde de la veracidad de los datos comunicados y que mantendrá convenientemente actualizada dicha información de modo que responda a su situación real, haciéndose responsable de los datos falsos e inexactos que pudiera proporcionar, así como de los daños y perjuicios, directos o indirectos, que pudieran derivarse.

¿Cuánto conservamos su información?

En TELEMAN COMUNICACIONES S.L sólo conservamos su información por el periodo de tiempo necesario para cumplir con la finalidad para la que fue recogida, dar cumplimiento a las obligaciones legales que nos vienen impuestas y atender las posibles responsabilidades que pudieran derivar del cumplimiento de la finalidad por la que los datos fueron recabados.

En todo caso, y por regla general, mantendremos su información personal mientras exista una relación contractual que nos vincule o usted no ejerza su derecho de supresión y/o limitación del tratamiento, en cuyo caso, la información será bloqueada sin darle uso más allá de su conservación, mientras pueda ser necesaria para el ejercicio o defensa de reclamaciones o pudiera derivarse algún tipo de responsabilidad que tuviera que ser atendida.

¿A quién comunicamos sus datos?

En general, en TELEMAN COMUNICACIONES S.L no compartimos su información personal, salvo aquellas cesiones que debemos realizar en base a obligaciones legales impuestas.

Asimismo, su información personal estará a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de posibles responsabilidades nacidas del tratamiento.

Transferencias internacionales de datos

No existen transferencias internacionales de sus datos a países fuera del Espacio Económico Europeo (EEE).

¿Cuáles son sus derechos con relación al tratamiento de sus datos y cómo puede ejercerlos?

La normativa en materia de protección de datos permite que pueda ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando proceda.

Estos derechos se caracterizan por lo siguiente:

- Su ejercicio es gratuito, salvo que se trate de solicitudes manifiestamente infundadas o excesivas (p. ej., carácter repetitivo), en cuyo caso TELEMAN COMUNICACIONES S.L podrá cobrar un canon proporcional a los costes administrativos soportados o negarse a actuar
- Puede ejercer los derechos directamente o por medio de tu representante legal o voluntario
- Debemos responder a su solicitud en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo en otros dos meses más.
- Tenemos la obligación de informarle sobre los medios para ejercitar estos derechos, los cuales deben ser accesibles y sin poder denegarle el ejercicio del derecho por el solo motivo de optar por otro medio. Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que nos solicite que sea de otro modo.
- Si TELEMAN COMUNICACIONES S.L no da curso a la solicitud, le informará, a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control

A fin de facilitar su ejercicio, le facilitamos los enlaces al formulario de solicitud de cada uno de los derechos:

Formulario ejercicio del derecho de acceso

Formulario de ejercicio del derecho de rectificación

Formulario de ejercicio del derecho de oposición

Formulario de ejercicio del derecho de supresión (derecho "al olvido")

Formulario de ejercicio del derecho a la limitación del tratamiento

Formulario de ejercicios del derecho a la portabilidad

Formulario de ejercicio a no ser objeto de decisiones individuales automatizadas

Para ejercer sus derechos TELEMAN COMUNICACIONES S.L pone a su disposición los siguientes medios:

1. Mediante solicitud escrita y firmada dirigida a TELEMAN COMUNICACIONES S.L, Calle Manzano n7 30593 La Palma Cartagena Murcia Ref. Ejercicio de Derechos LOPD.

2. Enviando formulario escaneado y firmado a la dirección de correo electrónico calle Manzano n7 indicando en el asunto Ejercicio de Derechos LOPD.

En ambos casos, deberá acreditar su identidad acompañando fotocopia o en su caso, copia escaneada, de su DNI o documento equivalente para poder verificar que sólo damos respuesta al interesado o su representante legal, debiendo aportar en este caso documento acreditativo de la representación.

Asimismo, y especialmente si considera que no ha obtenido satisfacción plena en el ejercicio de sus derechos, le informamos que podrá presentar una reclamación ante la autoridad nacional de control dirigiéndose a estos efectos a la Agencia Española de Protección de Datos, C/ Jorge Juan, 6 – 28001 Madrid.

¿Cómo protegemos su información?

En TELEMAN COMUNICACIONES S.L nos comprometemos a proteger su información personal.

Utilizamos medidas, controles y procedimientos de carácter físico, organizativo y tecnológico, razonablemente fiables y efectivos, orientados a preservar la integridad y la seguridad de sus datos y garantizar su privacidad.

Además, todo el personal con acceso a los datos personales ha sido formado y tiene conocimiento de sus obligaciones con relación a los tratamientos de sus datos personales.

Todas estas medidas de seguridad son revisadas de forma periódica para garantizar su adecuación y efectividad.

Sin embargo, la seguridad absoluta no se puede garantizar y no existe ningún sistema de seguridad que sea impenetrable por lo que, en el caso de cualquier información objeto de tratamiento y bajo nuestro control se viese comprometida como consecuencia de una brecha de seguridad, tomaremos las medidas adecuadas para investigar el incidente, notificarlo a la Autoridad de Control y, en su caso, a aquellos usuarios que se hubieran podido ver afectados para que tomen las medidas adecuadas.

AVISO1: Si del análisis realizado se desprende que su empresa debe tener contratado un Delegado de Protección de Datos, no olvide consignar la dirección de correo electrónico en la que los interesados pueden ponerse en contacto con él.

AVISO2: Si utiliza cookies, no olvide enlazar al documento de Política de Cookies en el apartado ¿Cómo recabamos su información?

AVISO3: No olvide definir un plazo máximo de conservación de los CV de los candidatos e incluirlo en la política de privacidad en el apartado ¿Cuánto conservamos su información?

AVISO4: No olvide definir un plazo máximo de conservación de los datos de los potenciales clientes e incluirlo en la política de privacidad en el apartado ¿Cuánto conservamos su información?

AVISO5: Si los tratamientos que realiza bajo las tecnologías seleccionadas presentan alguna característica particular no contemplada en esta Política de Privacidad en relación con finalidades, datos tratados, categorías de interesados, comunicaciones de datos o plazos de conservación de la información, deberá actualizar el contenido de los apartados correspondientes y hacer referencia explícita a esas singularidades.

Cláusulas contractuales para encargados de tratamiento

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) regula en su artículo 33 el rol del encargado del tratamiento, entendido este como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El artículo 28 del RGPD, entre otras cuestiones, determina que el responsable del tratamiento deberá escoger únicamente aquellos encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento realizado sea conforme a los requisitos del Reglamento y garantice los derechos y libertades de las personas. Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

La relación entre responsable y encargado deberá formalizarse mediante contrato u acto jurídico que les vincule y en el que se establezca, como contenido mínimo, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos y las categorías de interesados cuyos datos son tratados, la obligación del encargado de tratar los datos personales únicamente siguiendo las instrucciones documentadas del responsable, el destino de los datos una vez finalizada la prestación del servicio así como otras obligaciones del encargado en materia de subcontratación y asistencia al responsable del tratamiento.

En este apartado se recogen los modelos de cláusulas contractuales que deberá incorporar a los contratos firmados con los proveedores de servicio y encargados del tratamiento con los que el responsable haya establecido una relación contractual y que tienen acceso a los datos tratados y a los sistemas de información en los que el responsable realiza el tratamiento de datos (proveedores de hosting, prestadores de servicio de correo, mantenimiento informático,…) además de la cláusula de confidencialidad dirigida a aquellas empresas que sólo tienen acceso accidental a los datos y deben de mantener el deber de secreto de aquella información que pudieran llegar a conocer (empresas de servicio de limpieza, empresas de mantenimiento, …)

AVISO1: No olvide cumplimentar el plazo de duración para cada uno de los contratos suscritos.

AVISO2: No olvide firmar la última hoja de cada uno de los contratos obtenidos.

AVISO3: Repase detalladamente el contenido de las cláusulas generadas para verificar que tanto el objeto del mismo como la información de carácter personal afectada se ajustan a la realidad exacta del encargo de tratamiento.

AVISO4: En el caso de proveedores de servicio y encargados de tratamiento genéricos con acceso a datos personales, ya sea este accidental o accesorio o directamente derivado de la gestión de los sistemas de información, se generan tanto las cláusulas

contractuales como las cláusulas de confidencialidad. Seleccione aquellas que procedan de acuerdo con las características del servicio prestado y el tipo de acceso a los datos personales que se produzca.

Registro de Actividades del Tratamiento

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) establece en su artículo 31 relativo al "Registro de Actividades del Tratamiento" la obligación de responsables y encargados de mantener el registro de actividades del tratamiento al que se refiere el artículo 30 del RGPD. Sin corresponderse exactamente con el mapa de procesos de la organización, los tratamientos identificados deben estar integrados en este, mostrando las interrelaciones y dependencias que mantienen con el resto de procesos que se desarrollan dentro de la entidad.

De acuerdo con este artículo, el responsable del tratamiento deberá especificar en este registro las actividades de tratamiento llevadas a cabo junto con información relativa a:

- El nombre y los datos de contacto del responsable y del delegado de protección de datos si existe obligación de nombramiento.
- Las finalidades del tratamiento realizado
- La descripción de las categorías de los interesados cuyos datos son tratados, así como de las categorías de datos.
- Las categorías de destinatarios a los que se comunican los datos, incluidos los destinatarios de terceros países.
- En su caso, las transferencias de datos a terceros países u organizaciones internacionales junto con la identificación de estos y el detalle de las garantías adecuadas.
- Los plazos previstos de conservación de los datos o los criterios para determinarlos.
- Una descripción general de las medidas técnicas y organizativas adoptadas para garantizar la seguridad y la privacidad de los datos personales tratados.

En el caso de que actúe como encargado del tratamiento, también deberá contar con un registro de actividades en el que se especificará:

- El nombre y datos del encargado y de cada responsable por cuenta del cuál actúe el encargado, así como del delegado de protección de datos si existe obligación de nombramiento.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- En su caso, las transferencias de datos a terceros países u organizaciones internacionales junto con la identificación de estos y el detalle de las garantías adecuadas.
- Una descripción general de las medidas técnicas y organizativas adoptadas para garantizar la seguridad y la privacidad de los datos personales tratados

No olvide revisar los textos automáticamente generados y realizar los cambios necesarios para que el registro de actividades de tratamiento responda con exactitud a los datos recogidos, las finalidades definidas, las comunicaciones realizadas, si está prevista o no la realización de transferencias internacionales de datos y demás circunstancias particulares de cada uno de los tratamientos realizados.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE EMPLEADOS

a) Responsable del tratamiento	Identidad: TELEMAN COMUNICACIONES S.L - NIF: B30695951 Dirección postal: Calle Manzano n7 30593 La Palma Cartagena Murcia Correo electrónico: info@radiounion.es Teléfono: 691231544
b) Finalidad del tratamiento	Gestionar la nómina
c) Categorías de interesados	Empleados: Personas que trabajan para el responsable del tratamiento y con las que mantiene una relación laboral
d) Categorías de datos	Los necesarios para el mantenimiento de la relación laboral. Datos de identificación (nombre, apellidos, NIF, número de la Seguridad Social, dirección postal, teléfono, email)
e) Categorías de destinatarios	Instituto Nacional de la Seguridad Social
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

REGISTRO DE ACTIVIDADES SI ACTÚA COMO ENCARGADO DEL TRATAMIENTO

a) Encargado del tratamiento	Identidad: TELEMAN COMUNICACIONES S.L - NIF: B30695951 Dirección postal: Calle Manzano n7 30593 La Palma Cartagena Murcia Correo electrónico: info@radiounion.es Teléfono: 691231544
b) Responsables del tratamiento por cuenta de quienes actúa	[Listado de los responsables del tratamiento para los que presta servicio]
c) Categorías de tratamientos realizados	[Listado del par responsable – tratamiento en líneas diferentes]
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

AVISO1: Deberá incluir la relación de responsables a los que presta servicios en el apartado b) Responsables del tratamiento por cuenta de quienes actúa.

AVISO2: Para cada uno de los responsables del tratamiento consignados en el apartado anterior, deberá especificar en el apartado c) Categorías de tratamientos realizados cuál es el tipo de tratamiento que realiza en el marco del servicio prestado.

Directrices de atención a las solicitudes de ejercicio de derechos

El responsable del tratamiento informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) y teniendo en cuenta lo siguiente:

- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento y, cuando proceda, el derecho a no ser objeto de decisiones individuales automatizadas. El ejercicio de los derechos es gratuito.
- El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida y de forma concisa, transparente, inteligible, con un lenguaje claro y sencillo y conservar la prueba del cumplimiento del deber de responder a las solicitudes de ejercicio de derechos formuladas.
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Las solicitudes deben responderse en el plazo de 1 mes desde su recepción, pudiendo prorrogarse en otros dos meses teniendo en cuenta la complejidad o el número de solicitudes, pero en ese caso debe informarse al interesado de la prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.
- Si no se da curso a la solicitud del interesado, el responsable del tratamiento le informará, sin dilación y a más tardar transcurrido un mes desde la recepción de esta, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos y de ejercitar acciones judiciales.

En este sentido y como garantía de cumplimiento y ejercicio de responsabilidad proactiva, es recomendable que el responsable del tratamiento implemente mecanismos efectivos de registro y atención de las solicitudes recibidas en relación al ejercicio de derechos en materia de protección de datos de modo que esté en disposición de realizar una gestión eficiente de las dichas peticiones, garantizar la trazabilidad del tratamiento dado a estas y cumplir con los plazos de respuesta estipulados por la normativa.

DERECHO DE ACCESO: En el derecho de acceso se facilitará a los interesados copia de los datos personales de los que se disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación previstos o el criterio utilizado para determinarlo, la existencia del derecho a solicitar la rectificación o supresión de datos personales así como la limitación o la oposición a su tratamiento, el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos y si los datos no han sido obtenidos del interesado, cualquier información disponibles sobre su origen. El derecho a obtener copia de los datos **no puede afectar negativamente** a los derechos y libertades de otros interesados.

- Formulario para el ejercicio del derecho de acceso.

DERECHO DE RECTIFICACIÓN: En el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento. El interesado deberá indicar en la solicitud a qué datos se refiere y la corrección que haya de realizarse, aportando, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la rectificación de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio del derecho de rectificación

DERECHO DE SUPRESIÓN: En el derecho de supresión se eliminarán los datos de los interesados cuando estos manifiesten su negativa al tratamiento y no exista una base legal que lo impida, no sean necesarios en relación con los fines para los que fueron recogidos, retiren el consentimiento prestado y no haya otra base legal que legitime el tratamiento o éste sea ilícito. Si la supresión deriva del ejercicio del derecho de oposición del interesado al tratamiento de sus datos con fines de mercadotecnia, pueden conservarse los datos identificativos del interesado con el fin de impedir futuros tratamientos. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la supresión de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio del derecho de supresión.

DERECHO DE OPOSICIÓN: En el derecho de oposición, cuando los interesados manifiesten su negativa al tratamiento de sus datos personales ante el responsable,

este dejará de procesarlos siempre que no exista una obligación legal que lo impida. Cuando el tratamiento esté basado en una misión de interés público o en el interés legítimo del responsable, ante una solicitud de ejercicio del derecho de oposición, el responsable dejará de tratar los datos salvo que se acrediten motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado o sean necesarios para la formulación, ejercicio o defensa de reclamaciones. Si el interesado se opone al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para estos fines.

- Formulario para el ejercicio del derecho de oposición.

DERECHO DE PORTABILIDAD: En el derecho de portabilidad, si el tratamiento se efectúa por medios automatizados y se basa en el consentimiento o se realiza en el marco de un contrato, los interesados pueden solicitar recibir copia de sus datos personales en un formato estructurado, de uso común y lectura mecánica. Asimismo, tienen derecho a solicitar que sean transmitidos directamente a un nuevo responsable, cuya identidad deberá ser comunicada, cuando sea técnicamente posible.

- Formulario para el ejercicio de la portabilidad de los datos.

DERECHO DE LIMITACIÓN AL TRATAMIENTO: En el derecho de limitación del tratamiento, los interesados pueden solicitar la suspensión del tratamiento de sus datos para impugnar su exactitud mientras el responsable realiza las verificaciones necesarias o en el caso de que el tratamiento se realice en base al interés legítimo del responsable o en cumplimiento de una misión de interés público, mientras se verifica si estos motivos prevalecen sobre los intereses, derechos y libertades del interesado. El interesado también puede solicitar la conservación de los datos si considera que el tratamiento es ilícito y, en lugar de la supresión, solicita la limitación del tratamiento, o si aun no necesitándolos ya el responsable para los fines para los que fueron recabados, el interesado los necesita para la formulación, ejercicio o defensa de reclamaciones. La circunstancia de que el tratamiento de los datos del interesado esté limitado **deberá constar claramente en los sistemas** del responsable. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la limitación del tratamiento de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio de la limitación del tratamiento.

DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS: Este derecho permite a los interesados solicitar no ser objeto de una decisión basada únicamente en el tratamiento de tus datos, incluida la elaboración de perfiles, que produzca sobre ellos efectos jurídicos o que le afecten significativamente de forma similar. Afecta a cualquier forma de tratamiento de datos personales que evalúe aspectos personales, en particular si analiza o predice aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, fiabilidad o el comportamiento. Este derecho no es aplicable cuando el tratamiento sea necesario para la celebración o ejecución de un contrato entre él y el responsable o si el tratamiento se fundamente en un consentimiento prestado previamente, aunque en estos casos el responsable debe garantizar el derecho del interesado a obtener la intervención humana, a que exprese su punto de vista y a que impugne la decisión. No obstante, estas excepciones no son de aplicación sobre las categorías especiales de datos, salvo que el interesado diera su consentimiento explícito al tratamiento o este sea necesario por razones de un interés público esencial recogido en una norma y con garantías específicas para proteger los intereses y derechos fundamentales de los interesados afectados.

- Formulario para el ejercicio del derecho a no ser objeto de decisiones individuales automatizadas.

Recomendaciones sobre videovigilancia

La imagen de una persona, en la medida que la identifique o la pueda identificar, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras para garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines como el control de la prestación laboral de los trabajadores. A continuación, se incluyen las directrices básicas a respetar para que el tratamiento de las imágenes obtenidas a partir de cámaras de videovigilancia sea conforme a la normativa de protección de datos. No obstante, se recomienda la consulta de la Guía sobre el uso de videocámaras para seguridad y otras finalidades para un conocimiento más exhaustivo de las obligaciones que conlleva este tipo de tratamiento o acceder al apartado específico de videovigilancia de la web de la AEPD.

- **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, así como la captación de la vía pública si se utilizan cámaras exteriores, estando únicamente permitido la captación de la extensión mínima imprescindible para preservar la seguridad de las personas, bienes e instalaciones.

- **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas sólo accederá el personal autorizado.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que acrediten la comisión de actos que atenten contra la integridad de personas, bienes e instalaciones. En ese caso las imágenes deben ser puestas a disposición de la autoridad competente en un plazo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo colocado en un lugar suficientemente visible donde se identifique, al menos, la identidad del responsable y la posibilidad de los interesados de ejercer sus derechos en materia de protección de datos. En el propio pictograma se podrá incluir también un código de conexión o dirección de internet en la que se muestre esta información. Dispone de modelos, tanto del pictograma como del texto, en la página web de la Agencia.
    - Modelo de cartel de aviso de zona videovigilada.

- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral, según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador y a sus representantes sindicales, por cualquier medio que garantice la recepción de la información, acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados a las grabaciones del sistema de videovigilancia se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado para comprobar su identidad, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se le facilitará un documento en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guía y las fichas de videovigilancia y los informes jurídicos publicados por la Agencia Española de Protección de Datos en la sección de Videovigilancia.

Estrategias de privacidad y medidas de seguridad

El artículo 5.1.f del Reglamento General de Protección de Datos (en adelante, RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, su destrucción o daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas apropiadas encaminadas a asegurar la integridad y confidencialidad y, en general, de acuerdo al artículo 32 del Reglamento, un nivel de seguridad adecuado al riesgo. Adicionalmente, también es obligación del responsable del tratamiento, según establece el artículo 25 de la norma, implementar las estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto desarrollado, ya sea una aplicación, sistema, producto o servicio, desde su concepción hasta su retirada, de modo que la protección de datos esté presente desde las primeras fases de desarrollo y forme parte integral de la naturaleza de dicho objeto.

ESTRATEGIAS DE PRIVACIDAD DESDE EL DISEÑO

Tradicionalmente, el diseño de sistemas seguros y confiables se ha centrado en analizar los riesgos y dar respuesta a las amenazas que afectan a los objetivos de la seguridad que están más orientados a la privacidad: confidencialidad, evitando los accesos no autorizados a los sistemas; integridad, protegiéndolos de modificaciones no autorizadas de la información y disponibilidad, garantizando que los datos y los sistemas están disponibles cuando es necesario.

Sin embargo, aunque el acceso y la modificación no autorizada de los datos personales puede llegar a ser un aspecto crítico que amenace la privacidad de los individuos, existen otros factores de riesgo que pueden aparecer durante un procesamiento autorizado de los datos y que deben ser identificados durante la evaluación de riesgos para los derechos y libertades de los sujetos de los datos asociada al tratamiento. Por ello, es preciso ampliar el marco de análisis tradicional para que este cubra tanto los riesgos derivados de su tratamiento no autorizado como aquellos que pueden surgir de un procesamiento planeado y permitido de la información quedando así determinados los requisitos que deberá satisfacer cualquier sistema, producto, aplicación y servicio y que han de servir como entrada a los procesos de diseño de la privacidad.

En la práctica, supone tener en consideración, desde las primeras etapas de concepción de los sistemas y a lo largo de todo su ciclo de vida, un conjunto de diferentes estrategias de privacidad que ayuden a incorporar salvaguardas y medidas de protección en las operaciones y procedimientos de tratamiento de los datos personales, consiguiendo que los resultados finales tengan en cuenta los requisitos de privacidad identificados a raíz de la gestión del riesgo y dirigidos a garantizar los derechos y libertades de las personas cuyos datos son objeto de tratamiento. En concreto, estas estrategias se resumen en lo siguiente:

- **Minimizar** la cantidad de datos que son tratados, tanto en volumen de información recopilada como en el tamaño de la población objeto de estudio así como a lo largo de las diferentes etapas del tratamiento.

- **Agregar** los datos personales en la medida de lo posible para reducir al máximo el nivel de detalle que es posible obtener.
- **Ocultar** los datos personales y sus interrelaciones para limitar su exposición y que no sean visibles por partes no interesadas.
- **Separar** los contextos de tratamiento para dificultar la correlación de fuentes de información independientes, así como la posibilidad de inferir información.
- **Informar** a los interesados, en tiempo y forma, de las características y condiciones de su tratamiento para fomentar la trasparencia y permitir a los interesados tomar decisiones informadas sobre el tratamiento de sus datos.
- Proporcionar medios a los interesados para que puedan **controlar** cómo sus datos son recogidos, tratados, usados y comunicados a terceras partes mediante la implementación de mecanismos que permitan el ejercicio de sus derechos en materia de protección de datos.
- **Cumplir** con una política de privacidad compatible con las obligaciones y requisitos legales impuestos por la normativa.
- **Demostrar**, en aplicación del principio de responsabilidad proactiva, el cumplimiento de la política de protección de datos que se esté aplicando, así como del resto de requisitos y obligaciones legales impuestos por el Reglamento, tanto a los interesados como a las Autoridades de Supervisión.

Estas estrategias se concretan en técnicas específicas como las que se muestran a continuación:

MINIMIZACIÓN
Eliminación temprana de los datos no necesarios. Minimización de los datos recogidos y tratados en cada etapa del tratamiento. Minimización de la frecuencia de recogida de los datos, por ejemplo, en lecturas de consumo, de geolocalización, etc. Reducción de la precisión/granularidad de recogida de los datos, por ejemplo, información de ocurrencia de eventos, posición, etc. Limitación de la accesibilidad de bases de datos a través de la red Anonimización temprana Seudonimización de los datos almacenados. Seudonimización de los datos en alguno de los subprocesos del tratamiento
AGREGACIÓN
Generalización de datos personales Agregación de registros Reducción de la precisión/granularidad de recogida de los datos, por ejemplo, información de ocurrencia de eventos, posición, etc. Aplicación de diferenciales de privacidad en la difusión/acceso a los resultados del tratamiento
OCULTACIÓN
Anonimización temprana Seudonimización de los datos almacenados. Seudonimización de los datos en alguno de los subprocesos del tratamiento Introducción de medidas perturbativas en los datos de origen Control de la privacidad de los metadatos en las comunicaciones electrónicas Uso de credenciales basadas en atributos

Cifrado de la información almacenada o en tránsito
SEPARACIÓN
Compartimentación del acceso a los datos en el tiempo Compartimentación del acceso a los datos entre tratamientos. Particionamiento por atributos de las bases de datos Bloqueo de los datos Separación física de las fuentes de datos.
INFORMACIÓN
Transparencia de la extensión del tratamiento para el sujeto de los datos. Transparencia sobre el momento en el que se está realizando una recogida de datos
CONTROL
Control del usuario de la recogida de sus datos personales Control del usuario del tratamiento de sus datos Cifrado de la información extremo-extremo
CUMPLIMIENTO
Fijar requisitos de privacidad en los productos/servicios adquiridos o encargados para su desarrollo. Incorporar en el proceso de desarrollo de tratamientos que involucran datos personales los requisitos de privacidad en las primeras fases del ciclo de vida. Implementar procedimientos para garantizar la autenticidad o calidad de datos Implementación de medidas físicas para limitar la recogida de datos, como máscaras físicas de privacidad en cámaras, pestañas en webcams, etc. Configuraciones de privacidad máximas por defecto Especial atención a las circunstancias de sujetos en situación de especial riesgo o vulnerabilidad Limitación de tratamientos automáticos de datos que impliquen decisiones automatizadas
DEMOSTRACIÓN DEL CUMPLIMIENTO
Documentación de todas las decisiones tomadas en relación al tratamiento. Auditar el cumplimiento del RGPD en productos/servicios/componentes adquiridos o procesos llevados a cabo por terceros Adherirse a códigos de conducta o mecanismos de certificación. Medidas para garantizar la equidad en decisiones automatizadas

Tal y como establece el artículo 25 del RGPD, la obligación de implementar la protección de datos desde el diseño y por defecto es aplicable a todos los responsables del tratamiento con independencia de su tamaño, el tipo de datos tratados, la naturaleza del tratamiento o el tipo de tecnologías utilizadas, así como sea cual sea la forma de desarrollo, adquisición o subcontratación del sistema, producto o servicio. Es por ello que la protección de datos desde el diseño se proyecta sobre otros actores participantes en el tratamiento de datos personales como son los proveedores y prestadores de servicios, desarrolladores de productos y aplicaciones o fabricantes de dispositivos en tanto que deben tener en cuenta el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones y así poder ofrecer garantías al responsable del tratamiento en el cumplimiento de esta obligación.

Puede obtener más información consultando la guía de privacidad desde el diseño publicada por la Agencia Española de Protección de Datos.

MEDIDAS DE SEGURIDAD

La adopción de medidas de seguridad, tanto de índole técnica como organizativa, que garanticen la confidencialidad, la integridad y la disponibilidad de la información son claves a la hora de garantizar el derecho fundamental a la protección de datos.

El artículo 32 del RGPD establece que estas medidas, que deben ser apropiadas para garantizar un nivel de seguridad adecuado al riesgo, se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas. Es decir, no se establecen un catálogo de medidas de seguridad estáticas, sino que, en respuesta a un enfoque de gestión continua del riesgo, corresponde al responsable del tratamiento determinar aquellas medidas de control y seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Esta aproximación a la gestión del riesgo es común a todos los responsables con independencia del tamaño, las características o la disponibilidad de recursos de la organización, por lo que, de manera similar a las grandes organizaciones, también las pequeñas empresas, startups y emprendedores tienen que identificar el nivel de riesgo al que están sometidos sus tratamientos y adoptar las medidas necesarias para garantizar que los tratamientos se realizan en condiciones de seguridad y privacidad.

Es habitual que, en el caso de pequeñas y medianas empresas, parte de estos controles de seguridad y privacidad estén implementados como parte de los productos o appliance adquiridos o de los servicios prestados por fabricantes y prestadores de servicio tecnológicos. En todo caso, y en particular, en el supuesto de desarrollos cerrados llave en mano o de servicios prestados por cuenta de terceros que exijan el acceso a los datos personales tratados por el responsable, este velará porque el encargado implemente las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de dichos sistemas y servicios de acuerdo con nivel de riesgo detectado.

Aunque el global de los controles que se seleccionen, y que deberán ser formalmente definidos y aceptados como parte de un plan de acción que vendrá condicionado por el resultado de la evaluación de riesgos que realice, las medidas de seguridad mínimas que deberían tenerse en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

Medidas de gestión de la seguridad de la información

- **Definición de una política de seguridad y los procedimientos de protección de los datos personales.**

  En esta política, se deben establecer los principios básicos para garantizar la seguridad y la protección de datos personales dentro de la organización. Basada en esta política, se desarrollarán procedimientos específicos, como la gestión de recursos o el control de accesos, en cuyo marco se implementen las medidas técnicas y organizativas necesarias.

- **Definición de una política de control de acceso**.

  Basándose en las funciones y responsabilidades de cada usuario con acceso a datos de carácter personal, debe establecerse una política de control de acceso a los sistemas en los que se realiza el tratamiento en base al principio de *"need to know"* de modo que cada rol o usuario únicamente tenga el acceso y los

permisos estrictamente necesarios para el desarrollo de las tareas y funciones que desarrolla.

- **Gestión de recursos y gestión de los cambios.**

  La adecuada gestión de los medios del tratamiento, ya sean activos hardware, software o recursos de red, es una pieza clave para garantizar la seguridad de los datos personales, al igual que todo cambio producido en estos y que debe estar perfectamente sincronizado, controlado y supervisado para que, de modo accidental, no derive en una revelación, modificación o pérdida no autorizada de los datos personales tratados.

- **Relación con los encargados del tratamiento**.

  De acuerdo al artículo 28 del RGPD, cuando el tratamiento se realice por cuenta del responsable del tratamiento, este sólo elegirá a aquellos encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento y garantice la protección de los derechos del interesado, quedando regulada esta relación mediante un contrato o acto jurídico equivalente. Además, el encargado deberá actuar bajo las instrucciones del responsable e implementar las medidas de seguridad, técnicas y organizativas, necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento de los datos personales de acuerdo con nivel de riesgo detectado.

Medidas en materia de personal

- **Deber de confidencialidad del personal con acceso a datos personales.**

  El responsable del tratamiento debe adoptar las garantías necesarias para asegurar que el personal involucrado en el tratamiento de datos personales ha sido informado y conoce sus obligaciones con relación a los tratamientos de datos personales y en concreto el deber de confidencialidad y secreto que persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- **Formación.**

  Para una efectiva implantación de las medidas técnicas y organizativas, el personal de la organización debe recibir formación periódica y actualizada en relación a los procedimientos de protección de datos personales y seguridad definidos y, en particular, los relativos a las restricciones en la comunicación y divulgación de datos personales, la protección del acceso a estos por parte de terceros no autorizados mediante medidas de almacenamiento seguro, bloqueo de sesiones, cierre de despachos, etc. así como la destrucción segura de documentos y soportes.

Medidas de respuesta ante incidentes y continuidad de negocio

- **Gestión de incidentes y brechas de seguridad.**

En el caso de que se produzca una brecha de seguridad, el responsable debe valorar si esta supone *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*. Todos los empleados deben poner en conocimiento del responsable del tratamiento aquellas brechas de seguridad que afecten a datos personales para que este pueda notificarla a la Agencia Española de Protección de Datos, y en su caso a los interesados, en los términos descritos en el apartado **Directrices para la gestión de brechas de seguridad** de este documento. Además, y de forma independiente a la notificación de brechas, el responsable deberá implementar los mecanismos necesarios de registro, documentación y gestión de incidentes.

- **Definición de un plan de continuidad de negocio.**

  La definición de un plan de continuidad de negocio es esencial para determinar los procedimientos y las medidas técnicas que una organización debe seguir en el caso de materialización de un incidente o una brecha de seguridad que afecte a los datos personales tratados para que, de acuerdo a lo establecido en el artículo 32 del RGPD, el responsable o el encargado del tratamiento *sean capaces de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.*

MEDIDAS TÉCNICAS

- **Control de acceso y autenticación.**

  La autenticación y el control de acceso son las medidas técnicas básicas para proteger los sistemas de información que tratan datos personales del acceso no autorizado y la implementación práctica de la política de control de acceso definida en las medidas organizativas. Para ello, se recomienda disponer usuarios distintos si un mismo sistema es accedido por varios empleados, separar los usos personales de los profesionales y configurar perfiles sin privilegios de administración para que, en caso de materialización de un incidente de ciberseguridad, el atacante no obtenga privilegios de acceso al sistema operativo. Además, es altamente recomendable definir una política de contraseñas para controlar su complejidad y cambio periódico y formar a los empleados en la importancia de garantizar su confidencialidad evitando su exposición o comunicación a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad.

- **Monitorización y registro.**

  La activación y uso de logs (registros) en los sistemas de información permite la identificación y seguimiento de las acciones desarrolladas por los usuarios cuando acceden a los equipos en los que se realiza el tratamiento de datos personales. Esta funcionalidad permite identificar potenciales intentos, tanto internos como externos, de acceso no autorizado a los sistemas de información

además de plantearse como una medida de responsabilidad proactiva en el caso de que se produzca un incidente de seguridad que derive en una pérdida, modificación o revelación no autorizada de datos personales.

- **Seguridad de los datos.**

  Gran parte de las medidas a adoptar para garantizar la seguridad de los datos y el deber de salvaguarda tienen que ver con el aseguramiento y bastionado de los sistemas, entornos y redes en los que se realiza el tratamiento de los datos personales. Para ello conviene asegurar la información mediante la seudonimización y el cifrado de los datos personales así como proteger los sistemas en los que estos se procesan mediante la actualización de sistemas operativos y aplicaciones, el despliegue de servicios perimetrales de seguridad, tales como antivirus y cortafuegos, y la implementación de políticas de seguridad que eviten que los usuarios realicen determinadas acciones que puedan comprometer la seguridad del entorno de trabajo como, por ejemplo, la desactivación del software antivirus o la instalación de determinadas aplicaciones.

- **Seguridad de las comunicaciones.**

  Debe valorarse la necesidad de asegurar las comunicaciones, tanto hacia Internet como en la interconexión con otros sistemas internos o externos, mediante la instalación de cortafuegos, sistemas de detección de intrusión, segregación de redes y la utilización de mecanismos de cifrado para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- **Copias de seguridad.**

  Las copias de seguridad o *backups* son uno de los medios más efectivos, como parte del plan de continuidad de negocio, para recuperar la información en el caso de una pérdida o destrucción de los sistemas que realizan el tratamiento de los datos personales. En función de las características del tratamiento, deberá definirse y configurarse, entre otros parámetros, la frecuencia y el tipo de copia de seguridad y así poder dar respuesta a una de las obligaciones para responsables y encargados del tratamiento establecidas en el artículo 32 del RGPD en relación a "*la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico*". Para garantizar que cumplen su objetivo, las copias de seguridad realizadas deberán almacenarse en lugar seguro, distinto de aquél en que esté ubicado el sistema con los ficheros originales objeto de salvaguarda y verificar que se realizan correctamente conforme a la programación definida.

- **Dispositivos portátiles.**

  Aunque el empleo de dispositivos y sistemas móviles permiten extender el nivel de servicio prestado por la organización, representan un riesgo adicional por la posibilidad de robo o pérdida accidental. En estos casos, deben adoptarse garantías adicionales, tanto a nivel organizativo (definición de las condiciones para su empleo y medidas de precaución a respetar) como técnicas (doble

factor de autenticación, cifrado, códigos de bloqueo, …) para asegurar que los datos que contienen no se vean comprometidos.

- **Desarrollo seguro.**

  En el desarrollo de aplicaciones, productos y servicios, ya sea por el propio responsable o a través de un tercero que actúe por cuenta de este bajo un encargo de prestación de servicios, deben tenerse en cuenta tanto los requisitos de seguridad como de privacidad desde la primeras fases de análisis y diseño de las actividades de tratamiento, así como el establecimiento de configuraciones de privacidad que sean lo más estrictas posibles, de modo que se dé cumplimiento al artículo 25 del RGPD relativo a la *protección de datos desde el diseño y por defecto*. Puede encontrar más información sobre la aplicación práctica de esta medida en la guía de Privacidad desde el Diseño publicada por la Agencia Española de Protección de Datos.

- **Destrucción de la información.**

  El fin último en la destrucción o retirada de los dispositivos y soportes que contienen datos personales es un borrado irreversible de los datos de modo que estos no puedan ser recuperados. Los métodos utilizados dependerán del tipo de soporte, incluidas las copias en papel. En todo caso, el responsable del tratamiento debe asegurarse que los datos personales contenidos en un dispositivo han sido eliminados de forma permanente y de forma previa a la retirada del soporte. En todo caso, y a fin de dar cumplimiento al artículo 5.e del RGPD relativo al plazo de conservación, en la medida de lo posible deberían implementarse políticas automáticas de borrado de la información para asegurar que los datos no se conservan más allá del tiempo necesario en relación con el propósito por el que fueron recabados.

- **Medidas de seguridad físicas.**

  Las medidas de seguridad y control de acceso físico juegan un papel tan importante como las medidas de seguridad técnicas en tanto que proteger los sistemas de un acceso físico no autorizado mediante sistemas de identificación del personal, definición de áreas de acceso restringido, sistemas de detección de intrusos o la instalación de barreras perimetrales, son la base sobre la que se apoya una estrategia global de seguridad.

Puede encontrar más información sobre estas recomendaciones de seguridad y su implementación mediante controles de seguridad específicos en el capítulo 4 del documento "Directrices para PYMES sobre la seguridad en el tratamiento de datos personales" desarrollado por la Agencia de la Unión Europa para la Ciberseguridad (ENISA).

La existencia y correcto funcionamiento de las medidas de seguridad implantadas será revisado de forma periódica. Esta revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido

le puede ocurrir a usted, por lo que es recomendable adoptar las medidas apropiadas para protegerse contra el mismo.

Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales y la información que trata su empresa, el Instituto Nacional de Ciberseguridad (INCIBE) en su página web www.incibe.es, pone a su disposición herramientas con enfoque empresarial en su sección «Protege tu empresa» donde, entre otros servicios, dispone de:

- un apartado de formación con un videojuego, retos para respuesta a incidentes y videos interactivos de formación sectorial,
- un Kit de concienciación para empleados,
- diversas herramientas para ayudar a la empresa a mejorar su ciberseguridad, entre ellas políticas para el empresario, el personal técnico y el empleado, un catálogo de empresas y soluciones de seguridad y una herramienta de análisis de riesgos.
- dosieres temáticos que se complementan con videos e infografías y otros recursos,
- guías para el empresario,

Además INCIBE, a través de la Oficina de Seguridad del Internauta, pone también a su disposición herramientas informáticas gratuitas e información adicional que pueden ser de utilidad para su empresa o su actividad profesional.

Directrices para la gestión de brechas de seguridad

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que puede ocasionar destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

El responsable del tratamiento debe estar preparado para esta posibilidad antes de que ocurra, habiendo debido determinar quién y qué acciones se ejecutarán en caso de producirse. Para ello, lo primero es ser consciente de qué datos personales se están tratando, con qué medios y los riesgos que puede haber. Así, una parte muy importante es implementar mecanismos que permitan detectar las brechas de seguridad de datos de carácter personal.

Una vez ha tenido lugar, el responsable del tratamiento debe poner en marcha el plan de actuación definido, concretando tareas específicas que permitan resolver la brecha, minimizar sus consecuencias y evitar que vuelva a suceder en el futuro.

Además, el Reglamento establece en su artículo 33.5 que el responsable deberá documentar los incidentes relacionados con cualquier violación de seguridad de los datos personales incluyendo los hechos relacionados con este, sus efectos y las medidas correctivas que haya adoptado. Es importante documentar los incidentes o brechas de seguridad que afecten o puedan afectar a la disponibilidad, integridad y confidencialidad de los datos personales pues la Autoridad de Control está facultada a verificar el cumplimiento de esta obligación de documentación de las brechas de seguridad sufridas. Por tanto, cualquier información recabada en este sentido será muy útil a la hora de decidir qué medidas tomar y qué acciones se emprenderán para cumplir los objetivos anteriores y para valorar la necesidad de notificar a la Autoridad de Control y en su caso a los afectados.

La información mínima que debe tener en cuenta es la siguiente:

- Identidad del responsable del tratamiento
- Identidad del encargado del tratamiento cuando proceda
- Identidad de las organizaciones implicadas en la brecha
- Fecha y hora en la que se produce la brecha
- Fecha y hora en la que se tiene conocimiento de la brecha
- Forma en la que se ha tenido conocimiento de la brecha
- Resumen del incidente:
- Origen del incidente (interno, externo, etc.)
- Tipo de incidente (confidencialidad, integridad, disponibilidad)
- Categorías de datos afectados

- Datos o informaciones especiales (ej. creencias religiosas, afiliación sindical, vida sexual, origen racial, opinión política, salud, genéticos, biométricos, desconocidos, etc.)
- Volumen de datos afectados, tanto en número de registros como de personas afectadas.
- Categorías de personas afectadas (clientes, usuarios, empleados, suscriptores, estudiantes, pacientes, estudiantes, menores, personas en riesgo de exclusión, etc.)
- Medidas paliativas y preventivas
- Comunicación a la Autoridad de Control (AEPD)
- Comunicación a los interesados

En este apartado se facilita un modelo de registro de incidentes para su documentación y archivo a los efectos arriba indicados.

Ante el suceso de una brecha de seguridad, el responsable de tratamiento debe valorar las posibles consecuencias sobre los afectados y su severidad. Si la brecha de seguridad constituye un riesgo para los derechos y las libertades de las personas se debe notificar ante la AEPD en un plazo máximo de 72 horas desde que se tenga constancia a través del formulario habilitado en la Sede electrónica. Para rellenar el formulario de comunicación será muy útil tener de antemano clara la información relevante para la brecha que se ha destacado anteriormente, de ahí la importancia de su documentación.

Si el incidente en cuestión entraña un alto riesgo para los derechos y libertades de los sujetos cuyos datos se han visto expuestos, deberá además comunicarlo, sin dilación indebida, a los afectados a través del medio que se suela utilizar para comunicarse con ellos, con un lenguaje claro y sencillo. Esto permitirá que los afectados puedan reaccionar cuanto antes y tomar las medidas oportunas, porque en dicha comunicación se les deberá explicar claramente lo sucedido y las medidas recomendadas para que puedan minimizar o eliminar las consecuencias negativas que pueda tener la brecha sobre ellos.

Si está actuando como encargado del tratamiento y sufre un incidente de seguridad con afectación a los datos personales, debe informar al responsable del tratamiento sin dilación para que este pueda valorar si notificar ante la AEPD y comunicar a los afectados. En todo caso, los detalles sobre las responsabilidades de responsable y encargado ante una brecha de seguridad deben quedar expresamente detalladas en el contrato mediante el cual se establece el encargo del tratamiento.

Para más información puede consultar la guía para la gestión y notificación de brechas de seguridad publicada por la Agencia Española de Protección de Datos

Modelo de hoja de registro de incidentes

HOJA DE REGISTRO DE INCIDENTES	**Nº _____**
Responsable del tratamiento:	
¿el incidente ha tenido afectación en un encargado de tratamiento?	Sí □ No □
Nombre de la organización	
Datos de persona de contacto:	
Información adicional:	
Información del incidente	
Fecha/Hora del incidente:	
Fecha/hora de detección:	
Medios de detección del incidente:	
Origen del incidente:	Interno □ Externo□
¿Se ha comunicado el incidente a la Autoridad de Control?	Sí □ No □
¿Se ha comunicado el incidente a los afectados?	Sí □ No □
Persona que realiza la comunicación:	
¿Se ha resuelto el incidente?	**Fecha/hora resolución:**
Resumen del incidente:	
Tipología del incidente:	Confidencialidad □ Integridad □ Disponibilidad □
Categoría de los datos afectados:	
Datos básicos □ Credenciales de acceso/identificación □ DNI/NIE/Pasaporte □ Datos de contacto □ Datos económicos/financieros □ Datos de localización □ Otros:	
Datos o informaciones especiales:	
Datos de religión o creencia □ Datos de salud □ Datos de opinión política □ Datos de origen racial □ Datos de afiliación sindical □ Datos sobre vida sexual □ Datos genéticos □ Datos biométricos □ Datos sobre condenas e infracciones penales □ Otros:	
Categorías de personas afectadas	
Clientes □ Usuarios □ Empleados □ Proveedores □ Potenciales clientes/usuarios □ Suscriptores □ Estudiantes □ Menores □ Personas en riesgo de exclusión □ Pacientes □: Otros:	
Volumen de datos afectados:	En nº registros _____ En nº afectado _____
Relación de medidas correctivas y preventivas adoptadas	

Indicaciones y directrices con relación a las actividades que desarrolla

A continuación, se muestran indicaciones y recursos que pueden ser de utilidad en el contexto de las actividades que desarrolla a fin de abordar las obligaciones asociadas a sus actividades de acuerdo con las previsiones de protección de datos del RGPD y la LOPDGDD.

Lo primero que deberá considerar, a fin de proteger el derecho de terceros a la protección de sus datos en cualquiera de las actividades que realice, es el principio de protección de datos desde el diseño que, como requisito legal, se traduce en la obligación de integrar todas las garantías necesarias para la protección de los derechos y libertades de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas, productos y servicios. Para ello, además de las estrategias y medidas enumeradas en el apartado anterior, la AEPD pone a su disposición la "Guía de Privacidad desde el Diseño" a fin de ayudarle a considerar la estrategia de protección de datos desde el diseño más adecuada para cada uno de los sistemas, productos o servicios que precise elaborar en el marco de sus actividades y utilice los principios de privacidad desde el diseño y seguridad desde el diseño para aumentar la calidad de los productos y servicios que desarrolle.

Siempre que los desarrollos o los servicios en los que base su negocio recopilen datos de personas deberá de aplicar el principio de minimización de datos por el que únicamente estará en condiciones de solicitar al cliente o usuario final la información mínima y necesaria para la prestación de dichos servicios. Puede consultar la web de la AEPD para encontrar más información sobre las obligaciones a las que se encuentra sujeto un responsable de un tratamiento de datos personales.

Ya sea usted responsable (determina la finalidad la para la que se utilizan los datos o informaciones de las personas, así como los medios con los que se lleva a cabo el tratamiento) o encargado del tratamiento (accede o trata los datos o informaciones personales siguiendo instrucciones del responsable) deberá de tener en cuenta las medidas de cumplimiento que le son aplicables y que se mencionan a continuación.

Existen supuestos de tratamiento, regulados por el RGPD y la LOPDGDD, en los que la designación de un Delegado de Protección de Datos encargado de supervisar el cumplimiento de la normativa en materia de protección de datos y de informar y asesorar al responsable o, en su caso, al encargado del tratamiento, es obligatoria. No obstante, si su entidad actúa como desarrollador de productos, sistemas o servicios o bajo el rol de encargado de tratamiento y no necesita contar con esta figura en su organización, es recomendable que tenga en cuenta la necesidad de consultar y obtener asesoramiento por parte del Delegado de Protección de Datos del que pudiera disponer el propio responsable del tratamiento para garantizar que el servicio que le está prestando es conforme con la normativa. Para obtener más información sobre la figura del Delegado de Protección de Datos puede consultar este enlace.

Si, en su caso, desarrolla productos, sistemas o servicios que puedan ser utilizados para el tratamiento de datos personales por parte de un posible responsable o encargado, tenga en cuenta que las recomendaciones y exigencias legales que se señalan a

continuación darán un valor añadido a sus desarrollos y, además, será un factor clave para obtener la confianza de los usuarios finales cuyos datos o informaciones personales van a ser procesados.

Valore la posibilidad de disponer de una política de seguridad que establezca fundamentos claves para llevar a cabo sus actividades o sus desarrollos. Incluya en dicha política un procedimiento para la gestión y notificación de brechas de seguridad, procedimiento que deberá de contemplar la posibilidad de que haya que notificar a los propios afectados de esa eventual brecha de seguridad a fin de que puedan tomar las medidas oportunas para protegerse en la medida que ellos consideren necesarias.

Disponga también de una política de protección de datos y privacidad para los productos y servicios que desarrolle. Será un valor añadido para el cliente destinatario de sus desarrollos que contribuirá a la obtención de la confianza de los usuarios o clientes finales.

Tenga en cuenta el conjunto de normativas generales y sectoriales que le pudieran ser de aplicación en el desarrollo de sus productos y servicios, en particular el RGPD, la LOPDGDD, la LSSI o la LPI.

En los desarrollos que lleve a cabo o de los que sea usuario como responsable de un tratamiento de datos, incluya mecanismos para el ejercicio de los derechos de los interesados. Tenga en cuenta que, como responsable, deberá de atender los derechos de aquellas personas cuyos datos son tratados y, además, deberá de demostrar que esta actividad se lleva a cabo. Se recomienda que los medios para poder realizar esta actividad estén incorporados en la plataforma que se desarrolle en cada caso como un valor añadido a los servicios o productos que integre y como mecanismo para garantizar la confianza de los usuarios o clientes finales.

Cuando sus productos o servicios utilicen recursos en la nube, tenga en cuenta que podría estar realizando una transferencia internacional de datos las cuales están sujetas al cumplimiento de las garantías que determina el RGPD.

Otro de los factores que debe tener en consideración en el diseño de los productos y servicios que utilice o que desarrolle son los principios de limitación del tratamiento y minimización de datos, muy ligados al de ciclo de vida del dato, y que vienen a determinar que sólo serán tratados los datos necesarios en cada etapa del tratamiento y que no deberán de conservarse de manera indefinida, lo que está alineado con el concepto de supresión de datos que incorpora el RGPD. Tenga en cuenta que la conservación de los datos implica siempre la existencia de riesgos para los derechos y libertades de las personas. Sobre la interpretación de este concepto y su relación con dichos riesgos puede consultar la "Guía práctica de análisis de riesgos para el tratamiento de datos personales" y la "Guía práctica para las evaluaciones de impacto en protección de datos personales".

La AEPD viene publicando habitualmente contenido técnico que podría ser de utilidad para los productos que desarrolla y que, al mismo tiempo, también podrían serle de utilidad si, en calidad de responsable, precisa llevar a cabo un tratamiento de datos personales mediante productos y servicios que precisen un desarrollo tecnológico con el objetivo de que incorpore a estos, desde las primeras etapas de análisis y diseño, los

requisitos que establece el RGPD y la LOPDGDD a fin de evitar riesgos para los derechos y libertades de las personas cuyos datos van a ser tratados con dichos desarrollos. Esta información está disponible en el área de innovación y tecnología de la AEPD, donde podrá encontrar guías, informes, estudios, notas técnicas, herramientas y enlaces de interés que le serán de ayuda para abordar los principios de protección de datos que deben cumplir dichos desarrollos.

Tenga en cuenta que, con independencia de las orientaciones mencionadas en materia de gestión de riesgos, las recomendaciones y directrices que se incluyen a continuación pueden ser de utilidad a la hora de mitigar los posibles riesgos que, para los derechos y libertades de las personas, pudieran tener las actividades que ha indicado que desarrolla:

MARKETPLACE Y/O COMERCIO ELECTRÓNICO

El éxito del desarrollo de sitios web orientados al comercio electrónico se basa, principalmente, en la confianza del cliente que se genera a través de la identidad digital corporativa de un entorno de aplicaciones. Existen algunos aspectos claves que debe de tener en cuenta con relación a la protección de datos de los clientes o usuarios finales de estos sitios web, como por ejemplo, garantizar la privacidad y la seguridad en las comunicaciones y los medios de pago, elegir un proveedor de servicio web que le garantice la seguridad, elegir sellos de confianza así como el resto de obligaciones legales a las que pueda verse sujeta su actividad comercial.

Para garantizar la consecución de los objetivos que persigue con un desarrollo orientado al comercio electrónico es fundamental garantizar la protección de los datos de los clientes y usuarios así como la seguridad del sitio web desde el diseño, como ya se ha indicado. La AEPD ha desarrollado la "Guía de Privacidad desde el Diseño" para orientarle a determinar sus objetivos con relación a este principio normativo y, por tanto, de obligado cumplimiento que establece el RGPD. Con relación al principio de seguridad de la información desde el diseño y que deberá de tener en cuenta para garantizar la integridad, la confidencialidad y la disponibilidad de los desarrollos orientados al Marketplace, puede también consultar las orientaciones de carácter general que le proporciona INCIBE para la protección de sitios web.

La AEPD pone también a su disposición la "Guía de compra segura en internet" que, si bien está orientada al consumidor final, puede ser utilizada para orientar al desarrollador o al responsable de un Marketplace para que tenga en cuenta aquellos elementos que inciden directamente en el factor de confianza del cliente o usuario final de estos desarrollos.

La identidad digital corporativa de un sitio web es clave para garantizar la confianza del consumidor. Uno de los objetivos del desarrollador o de un responsable de un Marketplace debe ser el de proteger esta identidad digital frente a las posibles amenazas de las que puede ser objeto. En este sentido, INCIBE pone a su disposición información para identificar amenazas a las que se encuentran expuestas las webs orientadas al Marketplace teniendo en cuenta que cualquier sitio web es susceptible de ver suplantada su identidad digital.

Uno de los mecanismos de suplantación de la identidad digital de un sitio web es mediante el uso de recursos varios como, por ejemplo, la utilización de dominios DNS orientados a confundir al usuario y generar desconfianza. En este sentido, preste especial atención al posible acaparamiento de dominios de internet que pudieran tener nombres similares al utilizado por los sitios web de los que es responsable y tenga en cuenta las recomendaciones de INCIBE con relación a esta amenza, que también puede suponer una amenaza a la posible propiedad intelectual de los sitios web o a situaciones de competencia desleal. Otra de las formas habituales de suplantación de la identidad digital de un sitio web es la utilización de la propia imagen del sitio web con la finalidad de obtener datos personales de los clientes de forma ilícita haciéndoles creer que están accediendo al Marketplace legítimo cuando en realidad acceden a una página web desconocida y fraudulenta en la que, posiblemente, proporcionarán su identificador de usuario y su contraseña que posteriormente podrán ser utilizadas con finalidades ilícitas.

Recuerde también la necesidad de establecer una política de privacidad en relación a sus servicios, ya tengan como base una web o una app para dispositivos móviles, que sea transparente para el cliente o usuario final. Tenga en cuenta que deberá de cumplir determinados requisitos legales generales como el RGPD, la LOPDGDD, la LSSI o la LPI, además de normativas específicas que le sean de aplicación a su sector de actividad. Esta herramienta le proporciona un modelo de cláusulas informativas, política de privacidad y política de cookies que le serán de ayuda para abordar el principio de información con relación a las normas señaladas. La AEPD también le proporciona una guía específica sobre el uso de cookies. No olvide que la transparencia y el deber de informar, además de ser requisitos legales establecidos en el RGPD, también son una pieza clave a la hora de fidelizar al usuario final o al cliente de una plataforma Marketplace.

Valore la posibilidad de establecer canales específicos para comunicar al responsable de un Marketplace la posible existencia de compras fraudulentas o de intentos de llevarlas a cabo. También puede implementar en el desarrollo de las aplicaciones y entornos web mecanismos automáticos de ayuda a la detección de posibles fraudes, como por ejemplo, el envío de un gran número de mensajes de correo electrónico a un mismo usuario o cliente en un tiempo excesivamente corto.

Tenga en cuenta que, si su Marketplace se encuentra ubicado en la nube, existen ciertas garantías legales de cumplimiento que le exige el RGPD como, por ejemplo, el hecho de que, sea cual sea la ubicación física en la que se encuentren los datos, se garantice en todo momento el derecho a la protección de datos de los usuarios o clientes. Entre estas garantías deberá también tener en cuenta la necesidad de garantizar la seguridad de la información, tanto si la información se encuentra en la nube como si se encuentra en sistemas físicos diferentes. Los países que integran la Unión Europea disponen de un nivel de seguridad y protección de datos equivalente, para el resto de situaciones posibles, puede consultar en la web de la AEPD si los países destinatarios que disponen del nivel de adecuación necesario . A falta de decisión de adecuación, en esta página podrá consultar qué otras garantías resultan válidas. Además, para completar la información aquí mostrada, la AEPD pone a su disposición guías y orientaciones con relación al uso de servicios en la nube, como la "Guía para clientes que contraten servicios de Cloud Computing" o la guía de

"Orientaciones para prestadores de servicios de Cloud Computing". Adicionalmente, y con el fin de analizar los riesgos y amenazas de los servicios de cloud que utilice, puede consultar la guía de INCIBE así como otras informaciones y orientaciones de carácter general acerca de servicios cloud.

Si lleva a cabo el desarrollo de apps integradas en el Marketplace, tenga en cuenta que deberá abordar los principios de protección de datos desde el diseño y de seguridad desde el diseño. Para ello, pueden resultarle de utilidad las recomendaciones que la AEPD publica en su área de innovación tecnológica o las recomendaciones facilitadas por INCIBE.

Valore la posibilidad de implementar un servicio de doble factor que proporcione seguridad a las transacciones mediante, por ejemplo, el envío de un SMS al terminal móvil del usuario para la validación del pago

Por último, si usted es responsable de un Marketplace o si lleva a cabo desarrollos de estas plataformas o sus entornos aplicativos, valore la posibilidad de suscribirse a un servicio de alertas como el servicio de INCIBE sobre avisos de seguridad o el servicio de alertas específico orientado al fraude online y phising ofrecido por el Centro Criptológico Nacional (CCN) y que le serán de gran ayuda para estar al corriente de las posibles vulnerabilidades que afecten a sus desarrollos o sus infraestructuras de Marketplace.

Recomendaciones de Prevención del Acoso Digital

Para contribuir a frenar y erradicar todo tipo de **violencia digital** que haga uso de los datos y ponga en peligro la dignidad, libertad y privacidad de las personas la AEPD ha elaborado un conjunto de recomendaciones específicas orientadas a erradicar el acoso laboral y el acoso por razón de género cuando este tipo de conductas se produzcan en el ámbito digital y se materialicen a través del uso y tratamiento de datos personales, instando a las empresas a que las incorpore como una dimensión más en los planes de adecuación y cumplimiento a la normativa de protección de datos.

Estas recomendaciones parten de una **declaración de compromiso**, por parte del responsable, de prevenir y erradicar el acoso digital, de modo que la empresa impulse una cultura de respeto a la intimidad de las personas y de concienciación en el empleo de los datos personales en el contexto de las TIC.

Una vez definida la postura de la empresa ante este tipo de conductas resulta fundamental la **adopción de medidas concretas orientadas a la prevención** del ciberacoso que eviten el tratamiento ilícito de los datos de los empleados por parte de otros empleados con un claro objetivo de causar daño. En este sentido son clave la **información** con relación a qué tipo de conductas son inadecuadas en el empleo de las nuevas tecnologías y la **formación** a los empleados para que tomen conciencia de los riesgos que un tratamiento ilícito de datos personales puede entrañar para la intimidad y privacidad de las personas y conozcan las consecuencias, penales y administrativas en su caso, en que pueden incurrir.

Por último, además de la prevención, es importante implementar **medidas orientadas a la erradicación** del acoso digital a través de un firme compromiso por parte de la empresa que ha de ir presidido por el deber de colaboración con las autoridades competentes, la puesta en marcha de mecanismos de actuación previstos en las políticas de prevención del acoso y el desarrollo de cauces especiales para los supuestos en que el acoso se materialice a través de tratamientos ilícitos de datos personales.

Puede ampliar esta información consultando las recomendaciones publicadas por la Agencia Española de Protección de Datos en relación al uso de la protección de datos como garantía en las políticas de prevención del acoso y, a modo de ejemplo, los protocolos de actuación frente al acoso laboral y de actuación frente al acoso sexual y por razón de sexo en la AEPD. En esta línea, la AEPD ha puesto dispone de un canal prioritario para la retirada de contenidos especialmente sensibles que sean objeto de difusión ilegítima en medios electrónicos, puede acceder a este canal a través de la sede electrónica de la AEPD.