
SR
SMARTRECRUITECH

SmartRecruitech SL

SmartRecruitech SL
Plaza mayor, 4, 03630, Sax (Alicante)
Correo electrónico: info@smartrecruitech.com

Finalidad del tratamiento: Seguridad de las personas, bienes e instalaciones
Interesados: Personas que acceden a las instalaciones
Destinatarios: Fuerzas y Cuerpos de Seguridad

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 clientes/usuarios

Datos del responsable del tratamiento:

Titular: SmartRecruitech SL -
Domicilio social: Plaza mayor, 4, 03630, Sax (Alicante)
Teléfono: 675274658 - Correo electrónico: info@smartrecruitech.com
Página web: https://smartrecruitech.com

"Los datos proporcionados serán tratados por SmartRecruitech SL con la finalidad de prestarles el servicio solicitado y realizar su facturación. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante SmartRecruitech SL, Plaza mayor, 4, 03630, Sax (Alicante) o en la dirección de correo electrónico info@smartrecruitech.com, 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.

Asimismo, solicitamos su autorización para ofrecerle productos y servicios relacionados con los contratados y fidelizarle como usuario de nuestros servicios aceptando el cuadro de política de privacidad disponible en el formulario de registro."

Cláusula informativa de la actividad de tratamiento de candidatos

Datos del responsable del tratamiento:

Titular: SmartRecruitech SL
Domicilio social: Plaza mayor, 4, 03630, Sax (Alicante)
Teléfono: 675274658 - Correo electrónico: info@smartrecruitech.com
Página web: https://smartrecruitech.com

"Los datos proporcionados serán tratados por SmartRecruitech SL con la finalidad de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización y evaluar si su perfil se adapta a las características del puesto para pasar a formar parte de los posibles candidatos. Puede ejercer sus derechos de acceso, rectificación, supresión y portabilidad de datos y oposición y limitación a su tratamiento ante SmartRecruitech SL, Plaza mayor, 4, 03630, Sax (Alicante) o en la dirección de correo electrónico info@smartrecruitech.com, 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."

Política de Privacidad

SmartRecruitech SL pone a su disposición a través de la página web https://smartrecruitech.com 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: SmartRecruitech SL -
Domicilio social: Plaza mayor, 4, 03630, Sax (Alicante)
Teléfono: 675274658 - Correo electrónico: info@smartrecruitech.com
Página web: https://smartrecruitech.com

¿Con qué finalidad tratamos sus datos personales?

En SmartRecruitech SL 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
- Asignación de candidatos
- Procesos de selección
- 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
- Gestión de la selección de personal

¿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.

Derivado de la finalidad del servicio que le prestamos, del que habrá sido pertinentemente informado y en su caso, se le habrá solicitado consentimiento, podemos tratar los siguientes tipos de datos:

Currículums
Imágenes de perfil

SmartRecruitech SL 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 SmartRecruitech SL 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.

A través de nuestra página web recabamos información personal relacionada con su navegación a través del uso de cookies. Para conocer de manera clara y precisa las cookies que utilizamos, cuáles son sus finalidades y cómo puede configurarlas o deshabilitarlas, consulte nuestra Política de Cookies.

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 SmartRecruitech SL 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 SmartRecruitech SL 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 el caso de que quiera entrar a formar parte de nuestra plantilla y opte a uno de nuestros puestos de trabajo, los datos proporcionados pasarán a formar parte de nuestra bolsa de empleo y se conservarán mientras dure el proceso selectivo y por un máximo de 1 año o hasta que Ud. ejerza su derecho de supresión.

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 SmartRecruitech SL 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 SmartRecruitech SL 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 SmartRecruitech SL 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 SmartRecruitech SL pone a su disposición los siguientes medios:

1. Mediante solicitud escrita y firmada dirigida a SmartRecruitech SL, Plaza mayor, 4, 03630, Sax (Alicante) Ref. Ejercicio de Derechos LOPD.

2. Enviando formulario escaneado y firmado a la dirección de correo electrónico info@smartrecruitech.com 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 SmartRecruitech SL 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.

Política de Cookies

Texto de aviso emergente de cookies

Utilizamos cookies propias para fines funcionales dirigidos a permitir la correcta navegación por nuestra página web.

Para gestionar o deshabilitar las cookies pulse el botón "Configuración"

Para consentir su utilización y confirmar que ha leído la información proporcionada, pulse el botón "Acepto". Puede obtener más información consultando nuestra Política de Cookies.

Política de cookies

En SmartRecruitech SL utilizamos las cookies u otros archivos de funcionalidad similar (en adelante, "cookies") para saber cómo utilizas nuestros servicios y poder mejorarlos. SmartRecruitech SL es responsable de las cookies y del tratamiento de los datos obtenidos a través de estas, ya sean propias o de terceros, decidiendo sobre la finalidad, contenido y uso del tratamiento de la información recabada.

El objetivo de esta política es informarle de manera clara y detallada de qué es una cookie, cuál es su finalidad, qué tipo de cookies utilizamos y cómo configurarlas o en su caso deshabilitarlas.

Una cookie es un pequeño archivo de texto que se almacena en su navegador cuando visita nuestra página web y que guarda información sobre la navegación que realiza. Algunas cookies resultan esenciales para el buen funcionamiento de las páginas web, como es el caso de las cookies técnicas o de personalización de la interfaz de usuario, aunque otras, como las cookies de análisis o las de publicidad comportamental, requieren que le informemos y recabar su consentimiento para ser utilizadas por nuestra parte.

A continuación, y con el objetivo de que pueda prestar un consentimiento plenamente informado, le detallamos la información de en qué consiste y cuál es la finalidad de cada tipo de cookie

Las **cookies técnicas** son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan, incluyendo la gestión y operativa de la página web y habilitar sus funciones y servicios, como, por ejemplo, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, gestionar el pago, … La página web no puede funcionar adecuadamente sin estas cookies por lo que se consideran necesarias y no requieren su consentimiento.

Las **cookies de preferencias** o **personalización** permiten a la página web recordar información que cambia la forma en que la página se comporta o el aspecto que tiene de modo que el usuario acceda al servicio con determinadas características que pueden diferenciar sus opciones de uso del sitio web a las de otros usuarios, como, por ejemplo, el idioma, el número de resultados a mostrar cuando el usuario realiza una búsqueda o

la región en la que el usuario se encuentra. Si es el propio usuario quien elige esas características, por ejemplo, marcando la bandera del idioma, se considera un servicio expresamente solicitado siempre y cuando las cookies obedezcan exclusivamente a la finalidad seleccionada de personalización. Como en el caso anterior, estas cookies no requieren su consentimiento.

Las **cookies de análisis** o **medición** son aquellas que permiten comprender cómo interactúan los visitantes con las páginas web y así realizar el análisis estadístico del uso que hacen los usuarios de la web de los servicios prestados. La información recogida se utiliza en la medición de la actividad de los sitios web o aplicación con el fin de introducir mejoras en los productos y servicios ofrecidos por el responsable.

Las **cookies de marketing** o **publicidad comportamental** almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar anuncios relevantes y atractivos para el usuario individual, y por lo tanto, más valiosos para los terceros anunciantes.

SmartRecruitech SL está utilizando cookies propias de tipo técnicas, para las finalidades que a continuación se exponen en la siguiente declaración de cookies:

TIPO	FINALIDAD	CADUCIDAD	PROPIAS/TERCEROS
Técnica	Autentica-ción	Limitada	Propia

Si desactiva las cookies, podrá seguir accediendo a la web pero puede que la navegación por esta no sea óptima y alguno de los servicios ofrecidos no funcionen correctamente.

Si en un futuro SmartRecruitech SL llegara a utilizar tipos de cookies diferentes a las contempladas en esta Política de Cookies para prestar nuevos servicios o fuera necesario adaptarla a nuevas exigencias legislativas, se lo notificaremos.

Puede permitir, bloquear o eliminar las cookies instaladas en su dispositivo a través del menú de configuración de su navegador de internet, pudiendo configurarlo para que bloquee las cookies o alerte al usuario cuando un servidor quiera guardarla. Los siguientes enlaces proporcionan información en relación con cómo configurar y/o deshabilitar las cookies para cada uno de los principales navegadores del mercado a fin de que el usuario pueda decidir si acepta o no el uso de cookies.

- Microsoft Internet Explorer: menú Herramientas > Opciones de Internet > Privacidad > Configuración.
- Firefox: menú Herramientas > Opciones > Privacidad > Cookies.
- Chrome: menú Opciones > Opciones avanzadas > Privacidad.
- Safari: menú Preferencias/Privacidad.
- Safari para IOS (iPhone y iPad): Opción Ajustes > Safari
- Chrome para Android: Configuración > Configuración de sitios web > Cookies

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, …)

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.

Además, debe desarrollar unas tablas similares a las mostradas en este apartado para los siguientes tratamientos descritos que hacen uso de las tecnologías innovadoras que ha seleccionado:

Gestión de Procesos de Selección y Reclutamiento en Plataforma Colaborativa
Gestión de Procesos de Selección en Plataforma SaaS

Para cada uno de ellos deberá incluir la información exigida por el artículo 30 del RGPD arriba especificada, siendo importante, en particular, que identifique la finalidad del tratamiento, el tipo de datos tratados, la categoría de los individuos de los que proceden dichos datos, las posibles comunicaciones o cesiones de datos que realice, así como el plazo de conservación de la información.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE CLIENTES O USUARIOS

a) Responsable del tratamiento	Identidad: SmartRecruitech SL Dirección postal: Plaza mayor, 4, 03630, Sax (Alicante) Correo electrónico: info@smartrecruitech.com Teléfono: 675274658
b) Finalidad del tratamiento	Prestar un servicio Facturar un servicio Asignación de candidatos Procesos de selección
c) Categorías de interesados	Clientes o usuarios: Personas que son clientes o hacen uso del servicio prestado por su empresa
d) Categorías de datos	Los necesarios para el mantenimiento de la relación comercial. Datos de identificación (nombre, apellidos, NIF, dirección postal, teléfono, email) Datos profesionales (cargo, lugar de trabajo, sector de actividad) Datos bancarios (nº cuenta, nº tarjeta de crédito/débito) Currículums Imágenes de perfil
e) Categorías de destinatarios	Administración Tributaria
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE CANDIDATOS

a) Responsable del tratamiento	Identidad: SmartRecruitech SL - Dirección postal: Plaza mayor, 4, 03630, Sax (Alicante) Correo electrónico: info@smartrecruitech.com Teléfono: 675274658
b) Finalidad del tratamiento	Gestión de la relación con los candidatos a un empleo en la empresa
c) Categorías de interesados	Candidatos: Personas que envían su CV o cumplimentan un formulario de solicitud de empleo para incorporarse a la organización del responsable del tratamiento
d) Categorías de datos	Los necesarios para gestionar la solicitud de empleo de posibles futuros trabajadores: Datos de identificación (nombre, apellidos, dirección postal, teléfono, email) Características personales (estado civil, fecha y lugar de nacimiento, edad, género, nacionalidad, otros excluyendo datos de raza, salud y afiliación sindical) Datos académicos (formación, nivel de estudios, títulos) Datos profesionales (experiencia previa)
e) Categorías de destinatarios	No se contempla el envío de datos de carácter personal a ningún destinatario
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
g) Plazo de supresión	1 año desde la presentación de la candidatura
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: SmartRecruitech SL Dirección postal: Plaza mayor, 4, 03630, Sax (Alicante) Correo electrónico: info@smartrecruitech.com Teléfono: 675274658
f) Transferencias internacionales	No está previsto realizar transferencias internacionales
h) Medidas de seguridad	Las reflejadas en el ANEXO MEDIDAS DE SEGURIDAD

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.

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.