

ADRIÁN OTERO GÓMEZ
CL. CUBA 15
O CARBALLIÑO
32500 OURENSE

MEDIDAS Y PROCEDIMIENTOS RGPD

El RGPD establece como uno de los principales requisitos la privacidad desde el diseño y por defecto. A fin de cumplir con este principio, en este documento se detallan las políticas de Protección de Datos que establecen las medidas y Procedimientos para garantizar la seguridad de los derechos y libertades de los interesados, así como el cumplimiento del Reglamento.

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de 11 de Junio) recoge las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en el Reglamento Europeo de Protección de Datos (RGPD).

El contenido principal de este Documento queda estructurado como sigue:

- I. Ámbito de aplicación del documento.
- II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.
- III. Procedimiento general de información al personal.
- IV. Funciones y obligaciones del personal.
- V. Procedimiento de notificación, gestión y respuestas ante las incidencias.
- VI. Procedimiento de revisión.
- VII. Consecuencias del incumplimiento del Documento de Seguridad.

- Anexo I. Registro de actividades de tratamiento.
- Anexo II. Autorizaciones para la salida o recuperación de datos.
- Anexo III. Registro de Incidencias.
- Anexo IV. Contratos o cláusulas de encargados de tratamiento.
- Anexo V. Cláusulas a clientes.
- a) Cláusula informativa a clientes.
- b) Cláusula albaranes o facturas.
- Anexo VI. Cláusulas para introducir en los correos electrónicos.
- Anexo VII. Medidas de seguridad.

Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

CAPÍTULO 1: ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de ADRIÁN OTERO GÓMEZ con DNI 76734046C, con domicilio en CL. CUBA, 15; 32500 O CARBALLIÑO (OURENSE).

Las medidas de seguridad se clasifican en tres niveles acumulativos que son básico, medio y alto, atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

Nivel básico: se aplicarán a los ficheros con datos de carácter personal.

Nivel medio: ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD.

Nivel alto: ficheros que contentan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales sin consentimiento.

CAPÍTULO II: MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

- Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales.

Existen en los equipos informáticos donde se gestionan los distintos ficheros existen controles de acceso personales.

Las contraseñas personales son memorizadas por su correspondiente usuario.

- Control de acceso.

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones y exclusivamente el personal autorizado podrá tener acceso al local donde se encuentren ubicados.

Exclusivamente el personal que se indica a continuación podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información y que a continuación se especifican.

Por parte del interesado responsable del fichero, la persona física, ADRIÁN OTERO GÓMEZ, así como sus representantes legales, si los hubiera.

Exclusivamente ADRIÁN OTERO GÓMEZ está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos utilizados.

Los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos se realizará únicamente y exclusivamente por los usuarios de los ficheros ante el responsable del Fichero que en este caso es ADRIÁN OTERO GÓMEZ.

El responsable de seguridad revisará periódicamente la información de control registrada y elaborará un informe según se detalla en el Capítulo VI de este documento.

- Gestión de soportes.

Los soportes que contengan datos de carácter personal son etiquetados para permitir su identificación, inventariados y almacenados en el local de ADRIÁN OTERO GÓMEZ y con el acceso restringido al que solo tendrán acceso las personas con autorización.

Los soportes informáticos existentes son copias de seguridad de los distintos ficheros que se almacenarán de acuerdo a las siguientes normas: se etiquetarán para poder relacionar el soporte con su fichero correspondiente y son inventariados por el propio sistema y aplicación

informática correspondiente.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el responsable del fichero o aquel en que se hubiera delegado.

Todas las salidas de ficheros serán registradas por los apartados específicos de las distintas aplicaciones informáticas relacionadas con los distintos ficheros.

- Acceso a datos a través de redes de comunicación.

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicación deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Régimen de trabajo fuera de los locales de la ubicación del fichero.

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- Ficheros temporales.

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

- Copias de seguridad.

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción al estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Las recuperaciones de datos de los ficheros correspondientes deberán ser autorizadas por escrito por el responsable del fichero, según el procedimiento indicado en el Capítulo V.

Las copias de respaldo y de los procedimientos de recuperación de los datos de los ficheros correspondientes se conservarán en un armario restringido y separado de donde se encuentran los sistemas informáticos, en el que se almacenará la copia mencionada.

- El responsable de seguridad.
El responsable del fichero designará a uno o varios responsables que con

carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad que con carácter general serán los anteriormente mencionados.

En ningún caso, la designación supone una delegación de la responsabilidad que corresponde a ADRIÁN OTERO GÓMEZ con NIF nº 76734046C.

Es responsable de seguridad desempeñará las funciones encomendadas durante el periodo en que continúe activa la actividad de ADRIÁN OTERO GÓMEZ. Una vez dada de baja la actividad de esta persona física podrá nombrar al mismo responsable de seguridad o a otro diferente.

- Pruebas con datos reales.

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

CAPÍTULO III. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas serán informadas de acuerdo con el siguiente procedimiento: se pondrá a disposición de todas las personas relacionadas con los distintos ficheros así como una copia de la legislación correspondiente y se incluirá en este documento de seguridad en su ANEXO VIII una certificación de recibo de la información.

CAPÍTULO IV: FUNCIONES Y OBLIGACIONES DEL PERSONAL

- Funciones y obligaciones de carácter general.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable del fichero o de seguridad en su caso las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo V.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

CAPÍTULO V. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como “incidencias de seguridad” entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de ADRIÁN OTERO GÓMEZ.

El procedimiento a seguir para la notificación de incidencias será la comunicación y gestión por medio de la persona que detectó la incidencia ante el encargado del fichero correspondiente.

El registro de incidencias se gestionará mediante un anexo que se adjuntará al presente documento y se actualizará e iniciarán a medida que vaya surgiendo distinto tipo de incidencias en dicho anexo se especificará el tipo de incidencia, persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma. Así mismo se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros, especificando detalladamente el procedimiento para registrar las recuperaciones de datos, que deberá incluir la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia.

Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

CAPÍTULO VI. PROCEDIMIENTO DE REVISIÓN

- Revisión del Documento de Seguridad.

Para la modificación del documento de seguridad y actualización a la normativa vigente se realizará a petición de cualquier responsable de los ficheros que observe su falta de actualización o algún tipo de carencia relativa a su fichero, redactándose y aprobándose conjuntamente con la totalidad de los encargados de los distintos ficheros.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

- Auditoría.

Se realizará una auditoría interna que verifique el cumplimiento del Reglamento de Seguridad según lo indicado en su artículo 17, y que debe realizarse al menos cada dos años. El informe analizará la adecuación al Reglamento de las medidas y controles, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias. Los informes de auditoría han de ser analizados por el responsable del fichero, y quedar a disposición de la Agencia Española de Protección de Datos.

CAPÍTULO VII. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas Enel presente documento por el personal afectado, se sancionará conforme a la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, el Reglamento Europeo de Protección de Datos y la legislación vigente aplicable.

ANEXO I. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Tratamiento: **Cientes**

Finalidad del tratamiento

Gestión de la relación con los clientes

Descripción de las categorías de clientes y de las categorías de datos personales:

Clientes:

Personas con las que se mantiene una relación comercial como clientes

Categorías de datos personales:

Facturar

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Administración tributaria

Bancos y entidades financieras

Gestoría

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

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

Tratamiento: **Empleados**

Finalidad del tratamiento

Gestión de la relación laboral con los empleados

Descripción de las categorías de empleados y de las categorías de datos personales:

Empleados:

Personas que trabajan para el responsable del tratamiento

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación comercial.

Gestionar la nómina

De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail

Datos profesionales

Datos bancarios, para la domiciliación del pago de las nóminas

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Gestoría laboral

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

Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades

Tratamiento: **Proveedores**

Finalidad del tratamiento

Gestión de la relación con los proveedores

Descripción de las categorías de proveedores y de las categorías de datos personales:

Proveedores:

Personas con las que se mantiene una relación comercial como proveedores de productos y/o servicios

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación laboral

De identificación: nombre, NIF, dirección postal, teléfonos, e-mail

Datos bancarios: para la domiciliación de pagos

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

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

ANEXO II. AUTORIZACIONES SALIDA O RECUPERACIÓN DE DATOS

Se adjuntará original o copia de las autorizaciones a los responsables del fichero firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos usando el impreso que se adjunta a continuación:

IMPRESO REGISTRO DE SALIDA DE SOPORTES

Fecha y hora de salida del soporte:

Número y tipo de soporte:

Información que contiene:

Destinatario:

Forma de envío:

Persona responsable de la entrega:

Nombre:

Firma:

Observaciones:

Firma del responsable de seguridad:

ANEXO III. REGISTRO DE INCIDENCIAS

Todas las incidencias se recogerán en este documento:

IMPRESO DE REGISTRO DE INCIDENCIAS

INCIDENCIA N°
Fecha y hora en que se ha producido:
Descripción de la incidencia:
Efectos producidos por la incidencia:
Persona que notifica la incidencia:

Si la incidencia afecta a ficheros de nivel medio o alto y se han tenido que realizar procedimientos de recuperación de datos:

Firma del responsable del fichero autorizando el procedimiento de recuperación de datos:
Procedimientos realizados para la recuperación de datos:
Persona que ejecutó el proceso:
Datos restaurados:
Datos que han tenido que grabarse manualmente en el proceso de recuperación:

FIRMA OBLIGATORIA EN TODA INCIDENCIA REGISTRADA:

Fecha de notificación y firma de la persona que la realiza:	Firma del responsable de seguridad:
Fecha:	

ANEXO IV. ENCARGADOS DE TRATAMIENTO

O Carballiño, 12 de marzo de 2026

Los aquí abajo firmantes son usuarios autorizados para acceder a ficheros que contienen datos personales, cuyo responsable es ADRIÁN OTERO GÓMEZ destinados al manejo y actualización de los distintos ficheros relacionados con ADRIÁN OTERO GÓMEZ y manifiestan que tienen pleno conocimiento del documento de seguridad y de las obligaciones que les conciernen en su condición de usuario del fichero.

ADRIÁN OTERO GÓMEZ

ANEXO V. a) CLÁUSULA INFORMATIVA A CLIENTES

TRATAMIENTO DE DATOS DE CLIENTES

El texto que se muestra a continuación estará incluido en todos aquellos formularios que se utilicen para recabar datos personales de clientes.

Responsable: ADRIÁN OTERO GÓMEZ - NIF: 76734046C

Dir. postal: CL. CUBA 15; 32500 O CARBALLIÑO (OURENSE)

Teléfono: 664807559

E-mail: adriloureiro97@gmail.com

“En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado, realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en ADRIÁN OTERO GÓMEZ estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.”

ANEXO V. b) CLÁUSULA ALBARANES O FACTURAS

“Nos tomamos muy en serio la protección de los datos de nuestros clientes y colaboradores. La información de carácter personal que sea recabada de Vd. incluida su factura, será incorporada a un fichero confidencial cuyo titular y responsable es ADRIÁN OTERO GÓMEZ (76734046C) siendo su finalidad gestionar nuestra relación comercial así como informarle sobre servicios o productos que pudiesen ser de su interés. Ponemos todo el cuidado y contamos con las medidas que la Ley exige para que la información personal que nos facilita y/o el resultado de su tratamiento no llegue a terceros, salvo imposición legal o previo consentimiento suyo. Tiene Vd. derecho a ejercitar los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición/revocación determinados por la Ley dirigiéndose por escrito a la siguiente dirección: Cl. Cuba 15 CP 32500 Carballiño (Ourense)”

ANEXO VI. CLÁUSULAS PARA INTRODUCIR EN LOS CORREOS ELECTRÓNICOS

“La información contenida en este mensaje y/o archivo(s) adjunto(s), enviada desde ADRIÁN OTERO GÓMEZ, es confidencial/privilegiada y está destinada a ser leída sólo por la(s) persona(s) a la(s) que va dirigida. Le recordamos que sus datos han sido incorporados en el sistema de tratamiento de ADRIÁN OTERO GÓMEZ y que siempre y cuando se cumplan los requisitos exigidos por la normativa, acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición/revocación, en los términos que establece la normativa vigente en materia de protección de datos, dirigiendo su petición a la dirección postal CL. CUBA 15; 32500, O CARBALLIÑO (OURENSE) o bien a través de correo electrónico adriloureiro97@gmail.com.

Si usted lee este mensaje y no es el destinatario señalado, el empleado o agente responsable de entregar el mensaje al destinatario, o ha recibido esta comunicación por error, le informamos que está totalmente prohibida, y puede ser ilegal, cualquier divulgación, distribución o reproducción de esta comunicación, y le rogamos que nos lo notifique inmediatamente y nos devuelva el mensaje original a la dirección arriba mencionada. Gracias”

ANEXO VII. MEDIDAS DE SEGURIDAD

INFORMACIÓN DE INTERÉS GENERAL

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos personales relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas mínimas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- **DEBER DE CONFIDENCIALIDAD Y SECRETO**
 - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
 - Los documentos en papel y soportes electrónicos se almacenarán en

lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

- No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- DERECHOS DE LOS TITULARES DE LOS DATOS

Se 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.) 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 y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL

- Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: <https://sedeagpd.gob.es>
- CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)
 - **UBICACIÓN DE LAS CÁMARAS:** Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
 - **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.
 - **CONSERVACIÓN DE IMÁGENES:** Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
 - **DEBER DE INFORMACIÓN:** Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.
 - **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 o a sus representantes 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 se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, 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 facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS:** Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la medida posible.
- **MALWARE:** En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **CORTAFUEGOS O FIREWALL:** Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un

firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- **CIFRADO DE DATOS:** Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD:** Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual.