GRUPOLAE

EMPRESAS

# RGPD/LOPD-GDD

## Medidas y Procedimientos

NOELIA BARON SANZ

Junio 2024

## ANEXO A. NOMBRAMIENTO DE ROLES

### A.1. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD

En Alcacer, a ..... de ..... de 20...

Yo, Noelia Baron Sanz, con NIF 49098762H, como representante legal de Noelia Baron Sanz, con CIF 49098762H de acuerdo con la normativa vigente de Protección de Datos, asumo las funciones del Responsable de Seguridad, haciéndome cargo de las tareas relacionadas a continuación:

- Actualizar el manual de Medidas y Procedimientos y adecuación del mismo a la normativa vigente.
- Implantar el plan de formación en materia de protección de datos para los empleados
- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias que pudieran incurrir en caso de incumplimiento
- Adoptar las medidas correctoras como consecuencia de las deficiencias detectadas en un proceso de auditoría y aprobadas por la entidad
- Mantener una relación del personal autorizado para conceder, anular o alterar los derechos de acceso, conforme con los criterios establecidos
- Mantener una relación del personal con acceso autorizado al lugar dónde se almacenan las copias de seguridad
- Mantener una relación del personal autorizado para acceder a los locales dónde se encuentren ubicados los sistemas de información
- Protocolos de comunicación con el Delegado de Protección de Datos por parte de los empleados
- Adoptar protocolos para el cumplimiento de las medidas de seguridad
- Realizar protocolos para el diseño de flujos de tratamiento de datos
- Informar de las consecuencias del incumplimiento del manual de Medidas y Procedimientos

Noelia Baron Sanz

**A.2. ASUNCIÓN DE RESPONSABILIDAD POR PARTE DE LAE CONSULTING**

En Alcacer, a ..... de ..... de 20...

Yo, Noelia Baron Sanz, con NIF 49098762H, como representante legal de Noelia Baron Sanz, con CIF 49098762H de acuerdo con la normativa vigente de Protección de Datos, delego en LAE CONSULTING, S.L., con CIF B75010686, las siguientes funciones atribuidas al Delegado de Protección de Datos:

- Asesorar e informar a Noelia Baron Sanz de las obligaciones que le incumben en observancia de la normativa vigente en materia de protección datos.
- Supervisar el cumplimiento normativo de Noelia Baron Sanz en el tratamiento de datos personales
- Supervisar la implementación y aplicación de las políticas de Noelia Baron Sanz en materia de protección de datos personales
- Supervisar el análisis de las operaciones de tratamiento de datos personales
- Supervisar el análisis de las categorías de datos que trata la Organización
- Supervisar el análisis de los riesgos que puedan derivarse de las operaciones de tratamiento llevadas a cabo por Noelia Baron Sanz
- Facilitar el asesoramiento al Responsable de Privacidad o Seguridad en materia de protección de datos
- Impartir plan formativo al personal de Noelia Baron Sanz que realice tratamiento de datos
- Asesorar a Noelia Baron Sanz ante inspecciones y procedimientos informativos de la Autoridad de Control.
- Realizar las notificaciones requeridas por la Autoridad de Control, concretamente las referidas a la Evaluación de Impacto de Protección de Datos y a las incidencias y brechas de seguridad
- Supervisar la realización de la Evaluación de Impacto de protección de datos personales
- Supervisar la realización de las auditorías correspondientes
- Mantener el secreto y confidencialidad en el desempeño de sus funciones

Noelia Baron Sanz

LAE CONSULTING NORMATIVAS, S.L.

**ANEXO B. COMUNICACIÓN CON EL DPO**

Todas las comunicaciones internas que se realicen al DPO por parte de los directivos, empleados o agentes de la empresa, quedarán registradas por orden numérico de entrada seguido del año en que se realice la comunicación. Dicho registro de entrada será la que se corresponderá con el número de comunicación.

Una vez recibida la comunicación por parte del DPO, el empleado quedará liberado totalmente de cualquier responsabilidad al respecto y será plena responsabilidad del DPO proceder a su inmediato análisis o comprobación para determinar la relación de los hechos u operaciones comunicadas.

Para el caso de que se trate de una comunicación de violación de seguridad de los datos personales se procederá de inmediato a restablecer las Medidas y Procedimientos establecidos en este documento dependiendo de los datos de que se trate.

Cualquiera que sea el criterio adoptado se informará al comunicante del curso dado a su comunicación.

| MODELO DE COMUNICACIÓN INTERNA CON EL DPO | | | |
|---|---|---|---|
| **REGISTRO** | **DÍA** | **MES** | **AÑO** |
| | | | |

Identificación del empleado que efectúa la comunicación:

- Nombre
- Apellidos
- DNI
- Cargo

**1. Descripción de Duda, Sugerencia, Comunicación:**

**2. Comunicación de Violación de Seguridad de dos Datos Personales**

2.1.-Descripción de la violación producida:

2.2.- Describir las consecuencias probables de la violación de seguridad de los datos personales (en caso de conocerse):

**3. Relación de documentación adjuntada**:

1.-……..

2.-……

**Firma del comunicante**

**ANEXO C. MODELOS DE COMUNICACIÓN O REGISTRO INTERNO ANTE LA VIOLACIÓN O BRECHA DE SEGURIDAD**

*La empresa cuenta con la obligación de registrar cualquier incidente o brecha de seguridad, independientemente de que deba ser notificada a la AEPD o no.

| **MODELO DE REGISTRO INTERNO DE INCIDENTE DE SEGURIDAD** | | | |
|---|---|---|---|
| **REGISTRO** | **DÍA** | **MES** | **AÑO** |
| | | | |
| | | | |
| **1. Descripción del incidente de seguridad:** | | | |
| **2. Medidas adoptadas para evitar que el incidente de seguridad vuelva a tener lugar:** | | | |
| **Firma del Responsable de Seguridad:** | | | |

| MODELO DE COMUNICACIÓN DE LA VIOLACIÓN DE SEGURIDAD ANTE LA AUTORIDAD DE CONTROL COMPETENTE | | | |
|---|---|---|---|
| **REGISTRO** | **DÍA** | **MES** | **AÑO** |
| | | | |
| Identificación del DPO o Responsable de Seguridad: | | | |
| **1.Naturaleza de la violación de la seguridad de los datos personales:** | | | |
| **2. Posibles consecuencias de la violación de seguridad de los datos personales:** | | | |
| **3. Medidas adoptadas para poner remedio a la violación de la seguridad de los datos personales:** | | | |
| **Firma del Responsable de Seguridad:** | | | |

**ANEXO D. PROCESOS DE GESTIÓN INTERNOS PARA ATENDER CUALQUIER PETICIÓN DE EJERCICIO DE DERECHOS.**

1. **Recepción de la solicitud:**

Cualquier petición de ejercicio de Derechos recepcionada en Noelia Baron Sanz a través de cualquier punto de atención al cliente de cualquier dependencia o recibida por cualquier otro medio como correo electrónico o postal, debe ser escaneada de manera inmediata a la persona designada por el Responsable del Tratamiento.

2. **Coordinación:**

El Responsable del Tratamiento, con el apoyo y asesoramiento del DPD valorará si el contenido del ejercicio de derechos se ajusta a las condiciones legales.

3. **Respuesta**

Cualquier proceso de los mencionados más adelante tiene como condición la necesidad de emitir respuesta al solicitante en el **plazo máximo de un mes desde su recepción**. La respuesta será siempre por escrito y comunicada mediante burofax con copia y acuse de recibo o correo certificado.

**FORMULARIO PARA EL EJERCICIO DEL DERECHO A ACCEDER, RECTIFICAR, SUPRIMIR, LIMITAR, PORTAR, OPONERSE.**

| | |
|---|---|
| D./D.ª: | DNI: |
| Domicilio: | CP: |
| Población: | Provincia: |
| Email: | |

**SOLICITA** *(marcar una de las opciones):*

☐ Ejercitar el derecho a obtener confirmación de si se están tratando mis datos personales y, en tal caso, a **acceder** a mis datos personales y a que se me remita dicha información por:

- ☐ correo postal a la dirección anteriormente indicada.
- ☐ email a la dirección anteriormente indicada.

☐ Ejercitar el derecho a **rectificar** mis datos de carácter personal, solicitando la modificación de los siguientes datos en el sentido que se indica a continuación:

_____
_____
_____

☐ Ejercitar el derecho a **suprimir** todos mis datos de carácter personal en los términos expuestos a continuación:

_____
_____
_____

☐ Ejercitar el derecho a **limitar** el tratamiento de mis datos de carácter personal en los términos expuestos a continuación:

_____
_____
_____

☐ Ejercitar el derecho a **portar** mis datos de carácter personal en los términos expuestos a continuación:

_____
_____
_____

☐ Ejercitar el derecho a **oponerme** al tratamiento de mis datos de carácter personal en los términos expuestos a continuación:

_____
_____
_____

Con el fin de verificar que efectivamente usted es el titular de los datos personales, es necesario que aporte una copia de su DNI o Pasaporte.

Para ejercer el derecho de rectificación de los datos personales, el interesado deberá acompañar, cuando sea necesario, la documentación justificativa de la inexactitud o del carácter incompleto de los datos personales tratados.

En cumplimiento de la Ley Orgánica de Protección y de Garantías de Derechos Digitales, se le facilita la siguiente Información Básica sobre el tratamiento de los datos personales: que proporcione en cualquier momento a Noelia Baron Sanz**:**

***Responsable del tratamiento:*** *Noelia Baron Sanz, con CIF 49098762H.* ***Finalidades del tratamiento****: Responder a su petición de ejercicio de derechos ARSULIPO.* ***Bases jurídicas del tratamiento****: El cumplimiento de las obligaciones legales.* ***Destinatarios de sus datos****: No se cederán datos a terceros salvo que exista una obligación legal.* ***Plazo de conservación de sus datos****: durante los plazos que imponga la ley o durante los cuales puedan derivarse responsabilidades para la Sociedad.* ***Derechos****: puede ejercer sus derechos legales, entre otros, acceder, rectificar, suprimir, limitar, portar, oponerse al tratamiento de sus datos de manera gratuita contactando con la Sociedad presencialmente o por correo ordinario en Avenida Colon 71, Planta 2 Puerta 3, 46290 Alcacer (Valencia) o sanzn73@gmail.com adjuntando en ambos casos copia legible de su DNI u otro documento que acredite oficialmente su identidad. También presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).*

Firma del cliente:

## ANEXO E. GESTIÓN DE USUARIOS

### Alta de usuarios/personal con acceso a datos

Únicamente el Responsable de Seguridad tiene competencias para dar de alta los identificadores de usuarios y asociarlos a los perfiles definidos por los diferentes niveles de acceso a las aplicaciones y a las categorías de datos.

Será la Dirección de la entidad quien tenga la última decisión sobre los derechos de acceso de los usuarios.

Para el primer acceso del usuario al sistema, el Responsable de Seguridad deberá comunicar de forma confidencial su identificador y su contraseña de acceso inicial, según las indicaciones en la norma sobre gestión de contraseñas.

Se tendrán en cuenta las siguientes normas en la asignación de identificadores:
- No se reutilizará nunca un identificador
- Utilizar al menos cuatro caracteres en la composición del identificador del usuario

### Baja de usuarios

Noelia Baron Sanz, se encargará de cancelar el usuario y sus derechos de acceso.

El Responsable de Privacidad o Seguridad almacenará información descriptiva sobre los perfiles de acceso de los usuarios que se den de baja, durante el tiempo requerido para el cumplimiento de las obligaciones legales.

### Modificación de los perfiles de acceso de los usuarios

La modificación de los derechos o permisos de acceso de un usuario requerirá de la misma autorización jerárquica, diferenciada para cada tipología de usuarios, ya descrita en el protocolo de alta. Por esto, el procedimiento anunciado en el apartado de alta será extensible a este punto de modificación de permisos.

### Reactivación de usuarios

La reactivación de usuarios exige un procedimiento diferenciado respecto al resto de protocolos enunciados anteriormente, dado que parte de la premisa de la existencia de un alta previa que no requiere de un cambio de permisos del usuario en el sistema.

En aquellos casos en los que el acceso del usuario al sistema se haya revocado por causas accidentales, como el olvido de la contraseña, un periodo prolongado de inactividad o un excesivo número de intentos fallidos, la reactivación del usuario exigirá su comunicación al Responsable de Seguridad, para resolver la situación.

**Registros**

Noelia Baron Sanz mantendrá actualizada la documentación en lo referente a:

- Perfiles de acceso e identificadores asociados por el usuario.
- Alta, baja, revocación y modificación de usuario por fechas.
- Datos sobre usuarios
- Nombre y apellidos completos
- Área, departamento y servicio, donde se especificará el departamento y/o unidad en qué trabaja el usuario

Cualquiera de estos datos se podrá utilizar para la reactivación de usuarios revocados, para su control, uso o modificación.

**Usuarios del sistema**

Con la intención de evitar efectuar modificaciones en el documento Medidas y Procedimientos y para mantener su actualización, se describirá el procedimiento a seguir para la obtención de la relación de los usuarios con acceso autorizado a los sistemas, así como los derechos que tienen concedidos.

Este procedimiento se basa en la asignación del identificador de usuario que se compone del nombre del mismo usuario. En el caso de encontrar otro usuario con el mismo identificador se establecerán otras combinaciones aleatorias.

Para la contraseña de cada usuario se establecerá otra de aleatoria que podrá ser cambiada por el usuario cuando crea conveniente. Se debe tener en cuenta que en ningún caso la contraseña podrá ser utilizada por un plazo superior a un año natural, pasado el cual se deberá cambiar obligatoriamente.

**Relación de usuarios**

Noelia Baron Sanz mantiene una relación actualizada de usuarios o personal con acceso autorizado al sistema de información e identificando las categorías de datos tratados:

| Nombre y apellidos | DNI | Datos a los que accede |
|---|---|---|
| Noelia Baron Sanz | 49098762H | Todos los archivos |
| | | |
| | | |
| | | |

**ANEXO F. RELACIÓN DE ENCARGADOS DEL TRATAMIENTO**

Noelia Baron Sanz dispone de una relación actualizada de todos aquellos prestadores de servicios, que por los servicios que vienen prestando en condición de Encargado de Tratamiento, disponen de un acceso a datos de carácter personal bajo la responsabilidad de Noelia Baron Sanz.

**PRESTADOR DE SERVICIO 1**

| | |
|---|---|
| Denominación Social | GALARZA&CO |
| CIF | |
| Dirección | C/ Guillem de Castro, Nº 44 Entresuelo, Ciutat Vella 46001 Valencia |
| Servicios que presta | Asesoría fiscal |
| Fichero a los que accede | Clientes |

## ANEXO G. PROCEDIMIENTOS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN

Noelia Baron Sanz ha establecido todos aquellos procedimientos necesarios a fin de:

- Disponer de una copia de respaldo como mínimo semanal, salvo que en dicho período no se hubiera producido ninguna actualización de los datos, así como de disponer de procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

- Disponer de un proceso de verificación cada seis meses para la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

## ANEXO H. INVENTARIO DE APLICACIONES INFORMÁTICAS

Noelia Baron Sanz recogerá en el presente anexo la relación de aplicaciones existentes para el tratamiento de datos de carácter personal en cada uno de los distintos equipos informáticos existentes.

| Nombre de aplicación | Finalidad |
|---|---|
| | |

## ANEXO I. OPERACIONES DE TRATAMIENTO NO AUTOMATIZADAS

### Criterio de archivo

El archivo de los soportes o documentos se realiza de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios garantizan la correcta conservación de los documentos, la localización y consulta de la información y posibilitan el ejercicio de los derechos de los interesados.

En aquellos casos en los que no exista norma aplicable, Noelia Baron Sanz deberá establecer los criterios y procedimientos de actuación que se seguirán para el archivo de la documentación en soporte papel. Así, los contratos, albaranes, presupuestos, facturas, currículum vitae o cualesquiera otros documentos que contengan datos de carácter personal se archivarán en compartimentos cerrados con llave a los que sólo tenga acceso personal autorizado y que permitan a su vez, su fácil y pronta recuperación para el caso en que se requiera

### Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el Responsable de Tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

### Custodia de soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el punto anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

### Destrucción documental

Las empresas deberán destruir los documentos de carácter confidencial mediante sistemas que aseguren su inutilidad. Generalmente se aceptarán los sistemas de destrucción del papel (destructora) así como servicios externos que certifiquen la destrucción del papel mediante medidas de cumplimiento normativo.

## ANEXO J. APLICACIÓN DE MEDIDAS CONCRETAS DE PROTECCIÓN DE DATOS POR DEFECTO

Siguiendo las directrices de la Guía de Protección de Datos por Defecto publicada por la Agencia Española de Protección de datos en el mes de octubre de 2020, y en cumplimiento del segundo apartado del artículo 25 del RGPD, corresponde al responsable del tratamiento la implantación de las medidas de protección de datos por defecto.

*"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".*

La normativa aplicable en materia de protección de datos se muestra flexible a la hora de seleccionar las medidas para garantizar el cumplimiento de la misma, pudiendo optar por diferentes alternativas. Aunque el riesgo del tratamiento para los derechos y libertades sea escaso, no se debe ignorar la elección de medidas concretas de seguridad que se han de implementar por parte del responsable del tratamiento.

El RGPD exige al responsable del tratamiento la configuración por defecto de tratamientos de datos personales que sean respetuosos con los principios de protección de datos personales, garantizando un tratamiento lo menos intrusivo posible. Mínima cantidad de datos personales, mínima extensión del tratamiento, mínimo plazo de conservación y mínima accesibilidad a datos personales.

A continuación, se establecen una serie de medidas que deberán adoptarse por defecto en la empresa.

- **Cantidad de datos personales recogidos:** Esta serie de medidas implican factores cualitativos y cuantitativos de los datos personales. Siguiendo las directrices de la AEPD, el responsable del tratamiento deberá considerar el volumen de datos personales tratados, el nivel de detalle, las diferentes categorías, la sensibilidad (categorías especiales de datos) y los tipos de datos personales requeridos y necesarios para llevar a cabo una operación de tratamiento. Las medidas aplicables son las siguientes:

    - Captación de datos estrictamente necesarios.
    - Graduación de la extensión de los datos recogidos en función de los casos de uso.
    - Utilizar mecanismos de recogida escalonada de información necesaria para el tratamiento. Es decir, retrasar la recogida de datos hasta la fase en la que sean estrictamente necesarios.
    - Alternativas y voluntariedad en la información de contacto reclamada al usuario: e-mail, postal, teléfono, etc.
    - Generalizar los datos: emplear por ejemplo rangos de edad en lugar de la edad concreta.

- **La extensión del tratamiento:** Los tratamientos de datos personales se limitarán a lo estrictamente necesario para cumplir con la finalidad oportuna. Las medidas a implementar son:
  - Posibilitar los ejercicios de derechos de oposición, limitación o supresión.
  - Minimizar la cantidad de copias temporales que se generen y reducir al máximo los tiempos de conservación, las transferencias y comunicaciones.
  - Seudonimización atendiendo a las operaciones de tratamiento que puedan existir.
  - Procesamientos de carácter local y aislado.
  - Configuración del tratamiento para perfilado o decisiones automáticas (para el caso en el que se empleen este tipo de cookies).
  - Posibilidad de configurar todas las operaciones optativas de tratamientos para finalidades no imprescindibles. Por ejemplo, tratamiento de datos para mejora del servicio, análisis de uso, personalización de anuncios, etc. (para el caso en el que se empleen cookies de análisis comportamental).

- **El periodo de conservación:** Si un dato personal no se necesita después de ejecutar una fase del tratamiento, deberá ser suprimido. Las medidas a aplicar son:
  - Configuración de borrado de datos de sesión tras su cierre (para el caso de las cookies de sesión).
  - Plazos de conservación limitados de perfiles de usuarios.
  - Configuración de la gestión de copias temporales.
  - Control del borrado de copias temporales.
  - Eliminación de los datos del titular al ejercer el derecho al olvido.
  - Establecer mecanismos de bloqueo de datos y borrado.
  - Configuración de plazos de conservación de datos de compra de productos.
  - Mecanismos de anonimización de los datos cuando sea oportuno.

- **La accesibilidad de los datos:** El responsable del tratamiento deberá establecer quién puede acceder a los datos personales. Deberá limitar la accesibilidad de los datos personales. Las medidas a aplicar son las siguientes.

  - Identificación sobre la información del interesado que se muestra a terceros. Por ejemplo, divulgación selectiva de elementos de CV, de la historia clínica, etc.
  - Política de gestión de accesos en la que se especifican los datos a los que puede acceder cada usuario con acceso a datos personales.
  - Definición y configuración de los perfiles de acceso y asignación granular de privilegios.
  - Bloqueos automáticos de sesión.
  - Asignación de perfiles de acceso a los datos de acuerdo con los roles de los usuarios.
  - Diseño de espacio de trabajo (zonas aisladas de entrevista, ficheros físicos no accesibles, carpetas no trasparentes, pantallas no expuestas a terceros cascos para los teléfonos, políticas de mesas limpias. etc.
  - En su caso, prohibición de impresión.
  - Control del borrado de salidas de impresión.

- Retención o eliminación de la información de sesión, en aplicaciones, sistemas compartidos, comunicaciones o sistemas proporcionados al empleado.
- Sistemas de anomización y/o seudonimización de textos a difundir cuando sea oportuno.
- Parámetros de gestión de elementos de conectividad de los dispositivos (Wifi, Bluetooth, etc.).
- Medidas técnicas para revisión y filtrado de información que se va a hacer pública.
- Controles de accesibilidad al contenido del usuario en redes sociales.
- Histórico sobre los últimos cambios llevados a cabo y el perfil que ha realizado el cambio.
- Histórico de perfiles y entidades que han accedido a la información.
- Opciones de elección respecto a dónde se almacenan los datos personales, ya sea en dispositivos locales o remotos, en este último caso, otros parámetros como encargados o países.
- Facilitar el derecho al olvido de los titulares.
- Configuración de la recepción de avisos cuando la información se está haciendo accesible a terceros.
- Configurar sistemas de alerta por acceso anómalos a los datos.
- Trazabilidad de la comunicación entre responsables, encargados y subencargados.

**ANEXO K. ANÁLISIS DE RIESGOS Y MEDIDAS DE SEGURIDAD**

Conforme a lo establecido por el RGPD, los responsables y encargados del tratamiento deberán llevar a cabo un análisis de riesgos, con el fin de que se puedan implantar las medidas de seguridad apropiadas para garantizar los derechos y libertades de las personas. Por tanto, este documento tiene como objeto estudiar los riesgos de las actividades de tratamiento con baja exposición al riesgo.

Identificación de riesgos con probabilidad baja de que se materialicen:

- Modificación o alteración no intencionada de los datos personales.
- Pérdida no intencionada de los datos personales.
- Acceso no autorizado a datos personales.
- Ausencia de procedimientos para el ejercicio de derechos.
- Tratamiento ilícito de datos personales.

A continuación, se incluyen algunas medidas técnicas para garantizar la salvaguarda de los datos:

- **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 media 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 por garantizar la existencia de un firewall activado y correctamente configurado 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.

**ANEXO L. RÉGIMEN GENERAL DE DESCONEXIÓN DIGITAL**

| | |
|---|---|
| Noelia Baron Sanz | 49098762H |
| Avenida Colon 71, Planta 2 Puerta 3, 46290 Alcacer (Valencia) | |
| sanzn73@gmail.com | |

El sistema de "registro de inicio y fin de jornada laboral" en Noelia Baron Sanz se realizará de la siguiente manera:

☐ *Papel*

☐ *Herramienta Web / App*

☐ *Control biométrico (huellas dactilares/reconocimiento facial/etc.)*

☐ *Otros*

En general, no se espera del trabajador ni se incentiva a que continúe revisando (una vez terminada la jornada laboral acordada) ni mucho menos contestando, posibles mensajes o llamadas relacionadas con su prestación laboral.

Las situaciones de prolongación de jornada por circunstancias especiales, se compensarán en metálico o en horas libres previa aprobación de la Dirección/Departamento de RRHH conforme a la normativa legal y convencional ordinariamente aplicables.

Excepcionalmente y cuando la función desempeñada por el trabajador, haga aconsejable o conveniente que chequee el teléfono corporativo/correo electrónico corporativo/aplicación corporativa de mensajería, una vez transcurrido el horario habitual de su jornada laboral ordinaria, se suscribirá un acuerdo por escrito en el que se fijará una hora concreta u horquilla horaria durante el que deberá revisar que no se ha producido ninguna urgencia. Se entenderá como situación de urgente necesidad, por ejemplo, aquella que habitualmente puede resolverse mediante una instrucción o directriz clara, que se puede transmitir mediante una llamada o mensaje corto, y que evita una previsible o probable implicación significativamente mayor de recursos corporativos a posteriori, en caso de no ser atajada o resuelta de forma temprana.

En ……..……., a … de …… de 20….

Firmado,

## ANEXO M. RECOMENDACIONES PARA PROTEGER LOS DATOS PERSONALES EN SITUACIONES DE MOVILIDAD Y TELETRABAJO

La organización, como responsable del tratamiento, puede tomar la decisión de que determinadas actividades de su empresa se ejecuten en situaciones de movilidad y teletrabajo. Dicha decisión puede formar parte de la estrategia de gestión, general o parcial para determinadas áreas o actividades (por ejemplo, personal que viaja con frecuencia) o puede ser motivada por situaciones excepcionales e incluso de fuerza mayor.

La organización y el personal que participa en las acciones de teletrabajo han de tener en cuenta las siguientes recomendaciones.

### RECOMENDACIONES DIRIGIDAS A RESPONSABLES DEL TRATAMIENTO

A continuación, se enumeran un conjunto de recomendaciones para el responsable del tratamiento que éste tendrá que adecuar a la situación concreta de su objeto de negocio:

**1. Definir una política de protección de la información para situaciones de movilidad**

• Basada en la política de protección de datos y seguridad de la información de la entidad, y formando parte de ella, es necesario definir una política específica para situaciones de movilidad que contemple las necesidades concretas y los riesgos particulares introducidos por el acceso a los recursos corporativos desde espacios que no están bajo el control de la organización.

• En dicha política hay que determinar qué formas de acceso remoto se permiten, qué tipo de dispositivos son válidos para cada forma de acceso y el nivel de acceso permitido en función de los perfiles de movilidad definidos. También deben definirse las responsabilidades y obligaciones que asumen las personas empleadas.

• Es necesario proporcionar guías funcionales adaptadas a formar a las personas empleadas, derivadas de dichas políticas, y que recojan al menos la información que se expone en el apartado “Recomendaciones dirigidas al personal que participa en las operaciones de tratamiento” de este mismo documento.

• El personal también ha de estar informado de las principales amenazas por las que pueden verse afectados al trabajar desde fuera de la organización y las posibles consecuencias que pueden materializarse si se quebrantan dichas directrices, tanto para los sujetos de los datos como para la persona trabajadora.

• En dichas guías se debe identificar un punto de contacto para comunicar cualquier incidente que afecte a datos de carácter personal, así como los canales y formatos adecuados para realizar dicha comunicación.

• El personal ha de firmar un acuerdo de teletrabajo que incluya los compromisos adquiridos al desempeñar sus tareas en situación de movilidad.

**2. Elegir soluciones y prestadores de servicio confiables y con garantías**

• Hay que evitar utilizar aplicaciones y soluciones de teletrabajo que no ofrezcan garantías y que puedan dar lugar a la exposición de los datos personales del personal, interesados y servicios corporativos de la organización, en particular, a través de los servicios de correo y mensajería.

• Hay que recurrir a proveedores y encargados que ofrezcan soluciones probadas y garantías suficientes que, en el mismo sentido, eviten la exposición de los datos personales del personal, interesados y servicios corporativos de la organización

• Si estos acceden a datos de carácter personal, tendrán la consideración de encargados de tratamiento y la relación se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable. Este contrato debe establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable, de acuerdo con los términos establecidos en el artículo 28.3 del RGPD.

**3. Restringir el acceso a la información**

• Los perfiles o niveles de acceso a los recursos y a la información tienen que configurarse en función de los roles de cada persona empleada, de una forma incluso más restrictiva respecto de los concedidos en los accesos desde la red interna.

• A su vez, hay que aplicar restricciones de acceso adicionales en función del tipo de dispositivo desde el que se acceda a la información (equipos portátiles corporativos securizados, equipos personales externos y dispositivos móviles como smartphones o tablets) y también dependiendo dela ubicación desde la que se accede.

**4. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad**

• Los servidores de acceso remoto han de ser revisados y hay que asegurar que están correctamente actualizados y configurados para garantizar el cumplimiento de la política de protección de la información para situaciones de movilidad establecida por la organización, así como el control de los perfiles de acceso definidos.

• Los equipos corporativos utilizados como clientes tienen que: o estar actualizados a nivel de aplicación y sistema operativo, o tener deshabilitados los servicios que no sean necesarios tener una configuración por defecto de mínimos privilegios fijada por los servicios TIC que no pueda ser desactivada ni modificada por el empleado o instalar únicamente las aplicaciones autorizadas por la organización, o contar con software antivirus actualizado, o disponer de un cortafuegos local activado, o tener activados solo las comunicaciones (wifi, bluetooth, NFC, …) y puertos (USB u otros) necesarios para llevar a cabo las tareas encomendadas o incorporar mecanismos de cifrado de la información.

• Si se permite el uso de dispositivos personales de las personas empleadas, al suponer un mayor riesgo por no incorporar los mismos controles de los equipos corporativos, además de exigir unos requisitos mínimos para poder utilizarlos en el establecimiento de conexiones

remotas (por ejemplo, contar con un sistema operativo y software original y actualizado), hay que valorar la posibilidad de restringir la conexión a una red segregada que únicamente proporcione un acceso limitado a aquellos recursos que se hayan identificado como menos críticos y sometidos a menor nivel de riesgo.

**5. Monitorizar los accesos realizados a la red corporativa desde el exterior**

• Hay que establecer sistemas de monitorización encaminados a identificar patrones anormales de comportamiento en el tráfico de red cursado en el marco de la solución de acceso remoto y movilidad con el objetivo de evitar la propagación de malware por la red corporativa y el acceso y uso no autorizado de recursos.

• Las brechas de seguridad que afecten a datos personales han de comunicarse a la Autoridad de Control y/o a los interesados, con el propósito de crear un entorno de teletrabajo resiliente.

• Se debe informar al personal, en la política de protección de la información para situaciones de movilidad, sobre la existencia y el alcance de estas actividades de control y supervisión.

• Si las actividades de monitorización se usaran además para verificar el cumplimiento de las obligaciones laborales del personal, el responsable del tratamiento deberá informar con carácter previo, y de forma clara, expresa y concisa a las personas empleadas y, en su caso a sus representantes, de la medida adoptada en el marco de las funciones de control previstas en el Estatuto de los Trabajadores que han de ejercerse dentro de su marco legal y con los límites inherentes al mismo.

• Los mecanismos de monitorización implementados en el contexto de acceso remoto a recursos corporativos en situaciones de movilidad y teletrabajo deben respetar los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales y el derecho a la desconexión digital2 en el ámbito laboral.

• La configuración definida para acceder a los recursos de forma remota debe ser revisada de forma periódica para garantizar que no ha sido alterada ni desactivada sin autorización además de permanecer actualizada y adaptada a un entorno externo de riesgo que evoluciona de manera continua

**6. Gestionar racionalmente la protección de datos y la seguridad**

• Las medidas y garantías establecidas en las políticas definidas tienen que establecerse a partir de un análisis de riesgos en el que se evalúe la proporcionalidad entre los beneficios a obtener de un acceso a distancia y el impacto potencial de ver comprometido el acceso a la información de carácter personal.

• En la política deben contemplarse los procedimientos internos para provisionar y auditar los dispositivos clientes de acceso remoto, los procedimientos de administración y monitorización de la infraestructura, los servicios proporcionados por encargados y la forma en que la política es revisada y actualizada a los riesgos existentes.

• Los recursos que pueden ser accedidos se han de limitar en función de la valoración del riesgo que represente una pérdida del dispositivo cliente y la exposición o acceso no autorizado a la información manejada.

• Hay que planificar y evaluar las aplicaciones y soluciones de acceso remoto teniendo en cuenta los principios de privacidad desde el diseño y por defecto a lo largo de todas las etapas de despliegue de la solución: desde la definición de los requisitos y necesidades hasta la retirada de la misma o de alguno de sus componentes.

**ANEXO N. INSTRUCCIONES Y RECOMENDACIONES SOBRE EL USO DEL CERTIFICADO ELECTRÓNICO**

De acuerdo con lo establecido en el artículo 14.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, están obligados a relacionarse y comunicarse mediante medios electrónicos, con las Administraciones públicas, para la realización de cualquier trámite de un procedimiento administrativo, los siguientes sujetos:

*a) Las personas jurídicas.*
*b) Las entidades sin personalidad jurídica.*
*c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.*
*d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.*
*e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.*

Debido a esta obligación, empresas y autónomos están obligados a utilizar el certificado digital, el cual contiene datos de carácter personal, ya que identifica a una persona física.

En consecuencia, deben implementarse medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con lo establecido en el artículo 32 del Reglamento General de Protección de Datos:

1. Adquirir certificados digitales de prestadores de servicios de confianza, quienes garantizan la idoneidad del certificado y la validez del mismo.
2. En cuanto al almacenamiento del certificado, se recomienda realizarlo en un ordenador principal y no guardarlo nunca en una memoria externa; y en cuanto a su uso, se recomienda que solamente puedan acceder a él, las personas autorizadas a ello que lo necesiten para sus funciones laborales, de manera que se minimicen los riesgos lo máximo posible.
3. En cuanto al archivo del certificado digital, se recomienda que disponga de clave de acceso, mediante una contraseña.
4. En caso de ceder el certificado a un tercero, como puede ser quien nos preste el servicio de asesoramiento fiscal y /o laboral, quien necesitará el certificado digital para la correcta prestación del servicio, se recomienda la firma de un contrato de prestación de servicios en el que consten instrucciones y limitaciones sobre el uso del certificado digital, así como las medidas de seguridad a implantar en este sentido.
5. Se recomienda el uso del servicio de firma centralizada en la nube, ya que, de esta manera, queda constancia de la cesión del certificado digital y cabe la posibilidad de limitar su uso.