**REGISTRO DE GARANTÍAS DE LOS DERECHOS DIGITALES**

**REGISTRO DE ACTIVIDADES DE TRATAMIENTO**

El presente documento es de aplicación tanto a las actividades de tratamiento como a los ﬁcheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del Responsable del Tratamiento, tanto cuando actúa como tal o como Encargado del Tratamiento; incluyendo los sistemas de información, comunicación, soportes, equipos y resto de recursos empleados, entre los cuales queda incluido el personal, para el tratamiento de datos de carácter personal.

**RESPONSABLE DEL TRATAMIENTO**

De conformidad con el Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, le informamos de que los datos de carácter personal facilitados en el presente serán incorporados en un fichero titularidad y responsabilidad de ${razon} con NIF: ${cif}, y domicilio: ${domicilio}

Datos de contacto:

* ${tel}
* ${correo}

**FINALIDAD DEL TRATAMIENTO**

La gestión de las relaciones laborales de los empleados del responsable del tratamiento.

Entre estas finalidades:

* Ejecutar el contrato laboral
* Registrar la jornada laboral
* Cumplimiento de los deberes del empresario en materia de prevención de riesgos laborales
* Atender y tramitar las solicitudes de los interesados en materia de ejercicio de derechos de conformidad con la normativa vigente en materia de protección de datos personales
* Evaluación de las competencias profesionales (productividad y capacidad del empleado).
* Ejercer funciones de control, de acuerdo con lo establecido en el artículo 20.3 del Estatuto de los Trabajadores

**CATEGORÍA DE INTERESADOS**

Empleados: personas que trabajan para el responsable del tratamiento.

**CATEGORÍA DE DATOS**

Los necesarios para el mantenimiento de la relación laboral

Se tratarán datos como: nombre, apellidos, número de Seguridad Social, dirección, teléfono de contacto, correo electrónico. Datos profesionales y académicos.

**CATEGORÍA DE DESTINATARIOS**

Agencia estatal de Administración Tributaria. Instituto Nacional de la Seguridad Social. Bancos y entidades financieras.

**TRANSFERENCIAS INTERNACIONALES**

No está previsto realizar transferencias internacionales de datos fuera del Espacio Económico Europeo.

La entidad realiza transferencias internacionales de datos a destinatarios establecidos fuera del Espacio Económico Europeo.

**PLAZO DE CONSERVACIÓN**

Se conservarán los datos durante el tiempo necesario para cumplir con la finalidad para la que se recabaron.

Una vez desaparezcan las finalidades para las que han sido recabados los datos inicialmente, estos se conservarán los términos previstos en la legislación fiscal y laboral para el cumplimiento necesario respecto a la prescripción de responsabilidades.

**MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES EN RELACIÓN CON EL DERECHO DE GARANTÍAS DIGITALES**

**MEDIDAS EN TELETRABAJO**

En el contexto del teletrabajo los sujetos de los datos cuyos derechos y libertades deben estar garantizados son tanto la propia plantilla de la organización como las personas físicas con las que esta se relaciona y de las que se tratan datos personales en el contexto de su actividad de negocio. En ese sentido, es necesario garantizar la conformidad con el RGPD en ambas dimensiones, atendiendo a las circunstancias particulares que determina cada uno de ellos.

En el caso del tratamiento de datos de las personas trabajadoras que realizan teletrabajo, cuando este suponga un tratamiento adicional de datos con respecto al que venía realizándose en el ámbito presencial, se ha de respetar el principio de licitud, por lo que, para los distintos tratamientos que se realicen con causa de esta modalidad de trabajo a distancia, habrá de considerarse:

* La voluntariedad del trabajo a distancia (artículo 5 de la Ley 10/2021, de 9 de julio, de trabajo a distancia).
* La no aplicabilidad del consentimiento como base jurídica recurriendo, según el tratamiento específico, a otras más adecuadas:
  + Tratamiento legitimado por la existencia de una relación contractual (artículo 6.1.b) con relación al art. 20.3 del Estatuto de los Trabajadores, que establece la facultad del empresario para ejercer el poder de dirección y control, siempre con observancia del principio de proporcionalidad.
  + Satisfacción del interés legítimo del empleador, siempre que frente a este no prevalezcan los intereses o los derechos y libertades fundamentales del trabajador (artículo 6.1.f), cuestión que ha de evaluarse a través de una “prueba de ponderación o contrapeso” que no debe confundirse con una EIPD.
  + El cumplimiento de obligaciones legales (artículo 6.1.c), como es el caso de la obligación del empleador de establecer un registro de jornada, establecida en el artículo 34.9 del Estatuto de los Trabajadores. Este se impone con una finalidad específica, favorable al trabajador, tal y como se reitera en diversos apartados del Preámbulo del RD-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. Debe valorarse si el registro va a usarse al único efecto de lo previsto en el artículo 34.9 del ET o si también se va a usar como medida de control por el empresario o empresaria, atendiendo a las circunstancias concretas en que vaya a desarrollarse el trabajo a distancia. En ese caso, será necesario informar al trabajador de la doble finalidad.
* El levantamiento de la prohibición del tratamiento de categorías especiales de datos. Por ejemplo, los datos biométricos dirigidos a la identificación unívoca del trabajador solo podría quedar amparado bajo el artículo 9.2.b del RGPD cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos
* específicos de la persona responsable del tratamiento o de la persona interesada en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho o un convenio colectivo con arreglo a Derecho que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses de la persona interesada.
* El respeto de los derechos relacionados con el uso de dispositivos en el ámbito laboral como son, entre otros, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral y el derecho a la desconexión digital.

En cuanto a los tratamientos ya en curso y que son el objeto de la actividad de negocio propia de la persona responsable, no se requiere la existencia de una base jurídica diferente de la que ya lo legitimaba cuando venía desarrollándose de manera presencial, no suponiendo los medios empleados una modificación de la legitimación de los mismos.

No obstante, no debe perderse de vista que la existencia de una base de legitimación no exime del cumplimiento del resto de principios de tratamiento recogidos en el artículo 5 del RGPD que se desarrollan a lo largo de todo el articulado de la norma, debiendo tenerse en cuenta que la modificación de los medios habilitados para el acceso y el tratamiento de los datos con causa de la situación de teletrabajo sí que puede generar la necesidad de introducir mayores garantías en la aplicación de dichos principios.

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
2. Elegir soluciones y prestadores de servicio confiables y con garantías
3. Restringir el acceso a la información
4. Configurar periódicamente los equipos y dispositivos utilizados en las situaciones de movilidad
5. Monitorizar los accesos realizados a la red corporativa desde el exterior
6. Gestionar racionalmente la protección de datos y la seguridad

Los recursos que se pretende proteger frente a infracciones en materia de protección de datos personales son:

* Los centros de tratamiento y locales donde se encuentren ubicados los ﬁcheros o se almacenen los soportes que los contengan.
* Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso a datos personales.
* Los servidores y el entorno del sistema operativo y de comunicaciones en el que se encuentran ubicados los ficheros que contienen datos personales.
* Los sistemas informáticos y/o aplicaciones establecidos para realizar el tratamiento de los datos personales.
* Cualquier otro recurso que, sin estar aquí individualizado, se utilice para tratar datos personales.

Se informa al trabajador/a que:

* sólo puede utilizar los datos personales objeto de tratamiento, o los que recojan para su inclusión, exclusivamente, para las finalidades que le haya indicado expresamente el Responsable del Tratamiento. En ningún caso podrá utilizar los
* datos para fines propios o de terceros ajenos a la entidad.
* siempre deberá tratar los datos personales de acuerdo con las instrucciones del Responsable del Tratamiento.
* no comunicará los datos a terceras personas, salvo que cuente con la autorización expresa del Responsable del Tratamiento, en los supuestos legalmente admisibles.
* debe mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del desarrollo de sus funciones o tareas laborales, incluso después de que finalice su objeto.
* si fuera conocedor de alguna incidencia, deberá notificarla inmediatamente al Responsable del Tratamiento, al Delegado de Protección de Datos (cuando estuviera designado) o bien a la persona que indique el Responsable del Tratamiento.
* debe garantizar y respetar la confidencialidad de los datos personales a los que tenga acceso, así como mantener el compromiso de cumplir con las medidas de seguridad correspondientes y que constan descritas en el presente documento, de las que ha sido informado convenientemente.
* **NORMAS Y PROCEDIMIENTOS DE SEGURIDAD**

El Responsable del Tratamiento ha establecido las siguientes normas y procedimientos de seguridad, de obligado cumplimiento, por parte de todo el personal:

**Uso adecuado de los recursos de la organización referentes a:**

Dispositivos tecnológicos que el Responsable del Tratamiento pone a disposición del personal.

Las Tablets, Ordenadores de Sobremesa, Portátiles, Móviles, Teléfonos Inteligentes como cualquier otro dispositivo que sirva para el tratamiento, transporte y/o almacenaje de información que el Responsable del Tratamiento ponga a disposición del personal para realizar su trabajo, deberán ser custodiados por la persona al cual se haya asignado, debiendo dicha persona cumplir con todas las medidas de seguridad que vengan impuestas por la empresa.

Dichos dispositivos no podrán emplearse con fines ajenos a la actividad laboral. Si el trabajador o la trabajadora necesitan utilizarlo con fines ajenos a la actividad laboral, deberán contar con la autorización previa y por escrito de la organización.

Cuando se utilicen los equipos fuera del centro de trabajo, queda prohibido conectarse a redes WiFi públicas o de acceso gratuito y dejar el equipo desprotegido, debiendo en todo momento estar pendiente del mismo.

Internet y redes WIFI.

Todo el personal debe procurar un uso seguro y legal, tanto de Internet como de las redes WiFi de la organización, por lo cual, bajo ningún pretexto podrán:

* Acceder a páginas web que supongan una actividad ilegal, o de contenido no relacionado con el trabajo, así como también el acceso a páginas de dudosa procedencia.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma, material ilegal, como, por ejemplo: pornografía (de cualquier tipo); material amenazante, fraudulento, discriminatorio, difamatorio, ofensivo, obsceno, insultante o contrario a la moral y las buenas costumbres.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma material de cualquier tipo que esté protegido por el secreto comercial o por patentes vigentes.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma cualquier archivo de tipo musical, de lectura o filmográfico, sin tener los derechos de propiedad intelectual correspondientes.
* Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
* Enviar mensajes no solicitados, cualquier tipo de virus, código malicioso o ataques internos o externos a la red.
* Dañar de cualquier forma equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red, tanto de la organización como de terceros.
* Interceptar, recopilar o almacenar datos sobre terceros que no estén relacionados con la actividad laboral y sin su conocimiento y consentimiento expreso.
* Obtener acceso no autorizado a equipos, sistemas o programas tanto dentro como fuera de la red.
* Conectarse a la red reservada para invitados.
* Conectarse a redes públicas.
* Realizar cualquier otro tipo de acción, tanto de forma directa como indirecta, que ponga en riesgo la disponibilidad, integridad y/o confidencialidad de la información, como la seguridad e integridad de los sistemas que utiliza la organización.

Terminales y líneas telefónicas.

Los terminales, tanto fijos como móviles, tarjetas SIM y líneas telefónicas contratadas, no pueden utilizarse para fines ajenos a los relacionados con la actividad laboral que el personal desempeña para el Responsable del Tratamiento.

Solamente podrán utilizarse para fines personales, los equipos señalados, en caso de emergencia familiar, aunque en ningún caso podrán almacenarse en los mismos datos personales que puedan individualizar a una persona.

Queda también prohibido la manipulación de los terminales para lograr privilegios superiores a los otorgados por la organización, grabar llamadas, duplicar tarjetas SIM y en general cualquier actividad contraria.

Correo electrónico.

Ud. es el principal responsable del correcto uso de la cuenta de correo electrónico profesional que se le asigna, por lo cual deberá cumplir con las siguientes obligaciones:

* Está prohibido el envío de correos electrónicos con en el que se adjunten bases de datos personales o bien se copie el contenido de las mismas dentro del cuerpo del correo electrónico. Si, por razones del trabajo que se desarrolla, debe enviarse este tipo de información, la misma deberá enviarse únicamente mediante un archivo adjunto y dicho archivo deberá estar cifrado, la clave, en ningún caso se transmitirá por correo electrónico.
* Está prohibido enviar o reenviar mensajes en cadena o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario.
* Está prohibido configurar la cuenta de correo electrónico profesional en cualquier dispositivo sin la autorización previa y por escrito de la dirección.
* Está prohibido permitir el acceso al contenido de su cuenta de correo electrónico profesional a cualquier persona, ya sea personal interno como externo de la organización; sólo podrán tener acceso a su contenido a quien la dirección indique y por razón fundada.
* No podrá utilizar su cuenta de correo personal, bajo ningún pretexto, para la realización de la actividad laboral.
* El correo electrónico corporativo solo podrá ser utilizado para los fines correspondientes a la actividad laboral y en ningún momento con fines propios o privados quedando totalmente prohibido el envío o la recepción de correos ajenos a las funciones laborales con contenido personal.
* Se advierte que para el envío de un correo electrónico a varias personas, se debe utilizar la casilla CCO (con copia oculta) ya que en caso contrario se podría entender que se vulnera el deber de secreto.

En todo caso, se informa a los empleados de que la entidad podrá acceder al correo en caso de considerarlo necesario.

**Política de escritorios limpios.**

Si no te encuentras en tu puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, que contengan información que puedan contener datos personales, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos y soportes deben ser archivados de forma segura.

Tu puesto de trabajo debe estar limpio y ordenado; podrás disponer únicamente de los activos que hemos puesto a tu disposición.

No podrás tener recipientes ni envases sobre tu mesa de trabajo, cuyo cierre no sea hermético y que contengan líquidos, con el fin de evitar su vertido encima de los equipos informáticos y/o cualquier otro tipo de soporte que pueda verse afectado por el vertido.

**Política de pantallas limpias.**

La ubicación de los puestos de trabajo y la colocación de las pantallas está organizada de tal forma que sólo la persona que utiliza la misma puede leer lo que se plasma en la pantalla, evitando miradas indiscretas.

Si la persona autorizada no se encuentra en su puesto de trabajo, debe quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla mediante el uso de la siguiente combinación de teclas:

*Botón Windows + L*

Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el ordenador.

**Política de contraseñas.**

El personal tiene prohibido divulgar, compartir y/o entregar, tanto a personal interno como externo de la organización, las contraseñas que tengan para acceder tanto a los sistemas informáticos, programas, como a las Bases de Datos que contengan datos de carácter personal.

Al momento de crear la contraseña, deberá tener en cuenta lo siguiente:

* La contraseña deberá tener, al menos, 15 caracteres. No obstante, el número de caracteres es optativo de cada organización, la razón de la extensión es que cuantos más dígitos tenga la contraseña, más difícil es romperla por un ataque de fuerza bruta si se consigue su hash.
* Deberán combinarse letras mayúsculas y minúsculas, números y símbolos.
* No podrá utilizar la misma contraseña en diferentes servicios.
* No podrá utilizar aquellas contraseñas que utilice en su vida privada, por ejemplo, la de acceso al banco, a su cuenta de red social, etc.
* No podrá reutilizar contraseñas que ya haya utilizado previamente.
* No podrá utilizar patrones de teclado, por ejemplo: “qwerty” o “uiop” o “1qaz” “2wsx” o “3edc” ni la combinación de estas.
* Las contraseñas tienen un período de vigencia de 3 meses. No obstante, el tiempo es optativo de cada organización, la razón de los 3 meses es que no todos los ataques van dirigidos a ser descubiertos ni a encriptar o destruir una base de datos en particular, existen ataques que tienen como fin recabar la mayor cantidad de información posible, por lo cual, si se cambia la clave cada 3 meses, la perdida de confidencialidad estará acotada a un tiempo menor.
* Una vez creada la contraseña, deberá asegurar su correcta gestión y almacenamiento, por lo cual, deberá seguir las siguientes directivas:
* No apuntar la contraseña en notas y pegarlas en el escritorio, pantalla u ordenador.
* No utilizar la opción de “recordar contraseña” que ofrecen los navegadores.
* No almacenar la contraseña, dentro de su ordenador, en archivos sin cifrar y que estén a la vista de cualquier usuario y que lleven nombres que permita su fácil identificación, por ejemplo: “listado de contraseñas”, “contraseñas”, “pass”, “password”, etc.

**Sobre la instalación por parte del personal laboral de programas por cuenta propia.**

El personal no puede instalar ningún tipo de software por cuenta propia sin la autorización previa y por escrito del Responsable del Tratamiento.

En el caso que el trabajador/a proceda sin autorización ni conocimiento por parte de la organización del Responsable del Tratamiento, el trabajador/a quedará vinculado y será́ responsable en caso de daños ocasionados al equipo informático y/o a la información en él contenida como consecuencia de dicha instalación.

Antes de instalar un programa, el personal autorizado deberá comprobar que se cuenta con la licencia y derechos de uso del programa; con la certificación del programa para su compatibilidad con el sistema operativo y los demás aplicativos; con la garantía del código para evitar posible presencia de virus, troyanos y otros programas espías.

En todos los casos, cualquier tipo de software que se instale, deberá mantenerse actualizado siguiendo las indicaciones del desarrollador del software en cuestión.

Pruebas con datos reales.

Las pruebas anteriores a la implantación y/o modiﬁcación de los sistemas de información que traten ﬁcheros con datos de carácter personal no se realizarán con datos reales.

En el caso de resultar necesario utilizar datos reales con el fin de poder realizar la prueba de forma positiva, deberá asegurarse el nivel de seguridad correspondiente al tipo de tratamiento y a los datos de carácter personal afectados para que los mismos no sean objetos de una brecha de seguridad.

**Control de accesos.**

El personal sólo puede acceder a los datos y dependencias que sean necesarios para el correcto desarrollo de sus funciones.

Entrada y salida de las instalaciones de la organización.

Existe implantado en la organización un sistema de control de accesos cuyo objetivo es la identiﬁcación de personal, con el fin de evitar el ingreso de personas ajenas a la organización y el registro de jornada horaria con el fin de controlar y monitorizar el flujo del personal de la entidad.

Despachos.

Aquellos despachos que disponen de una puerta con llave, son sus ocupantes los encargados de que permanezcan cerrados cuando finalice la jornada laboral o se ausenten de su puesto de trabajo.

Todos los despachos que dispongan de armarios y cajoneras con llaves, siendo aquellas personas que los utilizan, las encargadas de que permanezcan cerrados cuando finalice la jornada laboral o se ausente de su puesto de trabajo.

Es responsabilidad de quienes tengan asignadas llaves, la custodia de las mismas al igual que la comunicación de su extravío al Responsable del Tratamiento, Delegado de Protección de Datos (si estuviera designado) o a aquella persona que designe el Responsable del Tratamiento.

Queda prohibido realizar copias de las llaves al igual que distribuir las mismas sin autorización expresa del Responsable del Tratamiento. Tampoco se podrá ceder o prestar las mismas a terceras personas sin autorización expresa del Responsable del Tratamiento.

Cuarto del servidor.

Únicamente el Responsable de Seguridad, el Delegado de Protección de Datos (si estuviera designado) y/o el personal autorizado por el Responsable del Tratamiento, están autorizados para acceder a las dependencias en las que se encuentren los sistemas de información que corresponden al servidor y a las copias de respaldo.

Es responsabilidad de quienes tengan asignadas claves de acceso, la custodia de las mismas al igual que la comunicación de su filtración al Responsable del Tratamiento, Delegado de Protección de Datos (si estuviera designado) o a aquella persona que designe el Responsable del Tratamiento.

**Régimen de trabajo fuera de los locales de la organización:**

El tratamiento de datos de carácter personal, fuera de los locales de la organización, deberá ser autorizado expresamente por el Responsable del Tratamiento, teniéndose en consideración las funciones que realiza el personal en la organización.

En el caso de que se autorice el tratamiento de datos fuera de los locales de la organización, el personal que los trate, deberá cumplir con todas las medidas de seguridad indicadas en los puntos 5.1 y 5.3 del presente documento y con todas aquellas que establezca la organización para el caso concreto.

**Copias de respaldo y recuperación.**

La organización realiza copias de seguridad de forma habitual y sistemática, por lo cual es su responsabilidad acatar las indicaciones que vengan impartidas por el departamento informático de la empresa.

**Gestión de soportes.**

Utilización de soportes extraíbles.

Por regla general, el personal no podrá disponer fuera de la entidad de ningún soporte con datos de carácter personal en los que la entidad actúe como Responsable o Encargada del Tratamiento.

El personal laboral que lo desee deberá solicitar una autorización previa para el tratamiento de datos en relación con las salidas y/o entradas de soportes del centro de trabajo.

Únicamente el Responsable del Tratamiento o a quién este designe, podrán autorizar la salida de datos de carácter personal en soportes extraíbles de la organización.

Disposición final de soportes.

Reutilización:

Cuando un equipo deba ser reasignado a otro trabajador de la organización, por ejemplo, porque su usuario actual varía de función dentro de la empresa o bien deja de prestar servicios para la misma, el Responsable del Tratamiento, se encargará de solicitar la entrega y devolución cualquier dispositivo a través del cual puedan tratarse datos personales, incluso aquellos que otorguen el acceso físico a instalaciones y dependencias de la organización.

A tales fines, se procederá de la siguiente forma:

* Antes de reasignar el dispositivo o equipo en cuestión, se procederá a realizar copia de la información que contengan, en caso de ser necesario.
* Una vez realizada la copia de seguridad, se procederá a realizar un formato completo, de tal forma que no se mantengan usuarios ni claves.
* Realizado el formato completo y configurado el equipo para el nuevo usuario, se procederá a su entrega, previa firma el registro de entrega de dispositivo al trabajador.

**Disposición final:**

Se informa que la destrucción de la documentación, ya sea en soporte papel o digital, que se genera como consecuencia del desarrollo de las funciones inherentes al puesto de trabajo, sobre todo cuando se contenga datos personales, tiene una labor previa que si no se realiza correctamente puede derivar en un incumplimiento de la normativa de protección de datos.

Por lo expuesto, no pueden tirarse los documentos ni soportes, de ningún tipo, directamente a la basura, ni aunque se rompan en trozos; la disposición final de los mismos se realizará de la siguiente forma:

* Si se va a desechar el soporte, por ejemplo, un ordenador, portátil o móvil, discos duros, DVD’s, CD’s, memorias USB, cintas o cualquier otro tipo de dispositivo digital; por mal funcionamiento, antigüedad, inutilidad, etc., el empleado deberá ponerlos a disposición del Responsable del Tratamiento o de la persona designada por este a tal, para que dicha persona proceda a su desechado.
* Destruir los papeles que contengan información personal empleando las destructoras de papel debe ser en partículas habilitadas a tal fin, dentro de las instalaciones del responsable.

Procedimiento de notiﬁcación, gestión y respuesta ante las incidencias.

El procedimiento de notiﬁcación y gestión de incidencias consistente en violaciones de datos por parte de terceros, mediante acceso no consentido on-line o presencial, debe contener un registro en el que conste:

* El tipo de incidencia.
* El momento en que se ha producido.
* La persona que realiza la notificación.
* A quién se le comunica.
* Los efectos que se hubieran derivado de la misma.
* El sistema informático utilizado en caso de tratarse de gestión automatizada.
* **POLITICAS DE DESECHADO Y REUTILIZACIÓN DE SOPORTES Y EQUIPOS**

La organización con el fin de garantizar la privacidad, confidencialidad y seguridad de los datos de carácter personal durante el proceso de destrucción, desechado o reasignación de soportes, evitando el acceso a la información contenida en los mismos o su recuperación posterior, establece las siguientes políticas generales de actuación.

Asimismo, el objetivo es dar cumplimiento al principio de responsabilidad proactiva establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

La razón por la que se debe realizar una destrucción confidencial tanto de la información obsoleta como de los soportes que la almacenan es evitar posibles brechas de seguridad, definidas éstas en el RGPD como una violación de seguridad de los datos en aquellos casos en los se ocasione “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.”

Así pues, antes de eliminar o reutilizar un soporte que haya almacenado información personal o confidencial se deben aplicar los procedimientos establecidos en esta política para evitar la recuperación de la información una vez destruida.

La presente política resulta de aplicación a todos los puestos de trabajo, instalaciones y equipos ubicados dentro de las instalaciones de la Organización

Los usuarios de este documento es todo el personal de la Organización que traten datos de carácter personal o información confidencial.

Desechado

La destrucción de la documentación, ya sea en soporte papel o digital, que se genera en los distintos ámbitos de la empresa sobre todo cuando esta contenga datos personales, tiene una labor previa que si no se realiza correctamente puede derivar en un incumplimiento de la normativa de protección de datos vigente.

Por lo expuesto, no se tiran los documentos ni soportes de ningún tipo que contenga datos personales, directamente a la basura, ni aunque se rompan en trozos, debiendo proceder a la destrucción de los soporte de la siguiente forma:

* Los soportes, por ejemplo, un ordenador, portátil o móvil, discos duros, DVD’s, CD’s, memorias USB, cintas o cualquier otro tipo de dispositivo digital; antes de ser desechados por mal funcionamiento, antigüedad, inutilidad, se ponen a disposición del Responsable del Tratamiento o de la persona designada por este.
* La información contenida en papel, se desecha en las destructoras de papel habilitadas por la Organización dentro de las instalaciones del Responsable.

Reutilización

Cuando un equipo utilizado previamente por un empleado/socio/ voluntario se reasigna a otro miembro de la Organización, por ejemplo, como consecuencia de una movilidad funcional dentro de la empresa del primero o bien finalización del contrato laboral, despido o renuncia voluntaria de este, se establece el siguiente procedimiento de actuación.

* Antes de reasignar el dispositivo o equipo en cuestión a otro empleado, y siempre en caso de ser necesario, se realizan copias de la información contenida en el dispositivo reasignado.
* Una vez realizada la copia de seguridad, el dispositivo objeto de reasignación es formateado de forma completa empleando técnicas de formateo de nivel alto, de tal manera que no se mantengan usuarios ni claves asignadas con anterioridad.
* Realizado el formateo completo y configurado nuevamente el equipo para el nuevo empleado, se procederá a su entrega, previa firma el registro de entrega de dispositivo al personal.

La presente política debe ser conocida y estar accesible para todos los integrantes de la entidad, por lo cual se distribuirá la misma a través de los canales habilitados para ello dentro de la organización.

**POLÍTICA DE PANTALLA Y ESCRITORIOS LIMPIOS**

La organización establece la siguiente política de pantalla y escritorios limpios con la finalidad de evitar el acceso no autorizado a los documentos impresos y/o soportes que almacenen datos de carácter personal. Dando así cumplimientos al principio de responsabilidad proactiva establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

La presente política resulta de aplicación a todos los puestos de trabajo, instalaciones y equipos ubicados dentro de las instalaciones de la Organización.

Los usuarios de este documento son todos los integrantes de la Organización (personal laboral, altos cargos y directivos.)

Escritorio Limpio

En el caso de que el personal laboral se ausente del puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos que contengan datos personales, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

El puesto de trabajo debe estar limpio y ordenado.

El personal laboral solo podrá disponer únicamente de los activos que la empresa pone a su disposición.

Se prohíbe colocar sobre los escritores y mesas de trabajo, recipientes o envases cuyo cierre no sea hermético y que contengan líquidos, con el fin de evitar su vertido encima de los equipos informáticos y/o cualquier otro tipo de soporte que pueda verse afectado por el vertido.

Pantalla Limpia

La ubicación de los puestos de trabajo y la colocación de las pantallas dentro de la Entidad está organizada de tal forma que sólo la persona que utiliza la misma puede leer lo que se plasma en la pantalla, evitando miradas indiscretas.

En el caso de que el personal laboral se ausente del puesto de trabajo, deberá quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se deberá implementar finalizando la sesión en todos los sistemas o bloqueando la pantalla mediante el uso de la siguiente combinación de teclas:

*Botón Windows + L*

En el caso de una ausencia por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se deberá implementar finalizando la sesión en todos los sistemas y apagando el ordenador.

La presente política debe ser conocida y estar accesible para todos los integrantes de la organización, por lo cual se distribuirá la misma a través de los canales habilitados para ello dentro de la organización.

**POLÍTICA DE DESCONEXION DIGITAL**

La organización establece la política de desconexión digital con el fin de garantizar a los trabajadores, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, prevenir el estrés laboral y la fatiga informática, así como de su intimidad personal y familiar; de acuerdo con lo exigido por el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta Política es aplicable a todo el personal de la organización, independientemente del puesto función u horario que realice.

Horario Laboral

Dentro de la organización, el horario laboral será el previsto para cada trabajador en su contrato de trabajo, así como también debe componerse el mismo de acuerdo con el calendario laboral. Ambos documentos deberán ponerse a disposición del trabajador para que pueda consultarlo.

En relación a las horas extras realizadas por el personal, estas se regirán de acuerdo a los criterios establecidos en los convenios colectivos aplicables, o en su defecto, a lo establecido en el Estatuto de los Trabajadores.

Derechos y Obligaciones de la dirección aplicadas a la Desconexión Digital

La organización, a través de los miembros integrantes del equipo directivo o responsable o cualquier otro puesto que tenga a su cargo personal, como regla general, no contactará con las personas que tuviera a su cargo:

* Fuera del horario laboral.
* Durante los períodos de descanso (vacaciones, fines de semana).
* Durante el tiempo que dure la excedencia concedida.
* Durante las bajas (maternidad / paternidad, adopción accidentes, asistencia necesaria a familiares por enfermedad y/o accidentes)
* Durante las fiestas religiosas relacionadas con la religión que el trabajador profese.
* Durante los días que el calendario laboral indica como día no laborable.
* Durante los permisos solicitados para acudir a un evento familiar (acto escolar, entrega de premios, entrega de diplomas, etc.)
* Licencias por luto.

La presente obligación no será de aplicación cuando la comunicación con el trabajador se vea amparada por una situación de gravedad o de emergencia relacionada con su puesto de trabajo o con el mantenimiento adecuado de la actividad de la organización.

Dicha valoración se realizará, teniendo en cuenta y dándole prioridad, al derecho de desconexión digital que la ley le acuerda al trabajador.

El personal no está obligado atender o contestar llamadas telefónicas o correos electrónicos de los clientes, en los casos listados más arriba. Esto último, no resultará de aplicación durante el periodo de guardias establecidas en la entidad o cuando el puesto desempeñado implique atender consultas o incidencias urgentes de los clientes.

Por tanto, también se abstendrán de requerir respuesta en las comunicaciones enviadas a las personas trabajadoras fuera de horario de trabajo o próximo a su finalización, siempre que pudieran suponer para los destinatarios de las mismas la realización de un trabajo efectivo que previsiblemente pueda prolongarse e invadir su tiempo de descanso.

Los destinatarios de la comunicación tendrán derecho a no responder a la misiva hasta el inicio de la siguiente jornada laboral. En este sentido, en caso de enviar una comunicación que pueda suponer respuesta fuera del horario establecido al efecto, el remitente asumirá expresamente que la respuesta podrá esperar a la jornada laboral siguiente.

${razon} no podrá sancionar disciplinariamente a las personas trabajadoras con ocasión del ejercicio por parte de éstas de su derecho a desconexión digital en los términos establecidos en esta política. El ejercicio del derecho a desconexión digital no repercutirá negativamente en el desarrollo profesional de las personas trabajadoras.

Derechos y Obligaciones del personal aplicadas a la Desconexión Digital

Las personas trabajadoras de ${razon} tendrán derecho a no responder a ninguna comunicación, fuere cual fuere el medio utilizado (correo electrónico, WhatsApp, teléfono, etc.), una vez finalizada su jornada laboral, salvo que concurra alguna de las siguientes circunstancias:

* Que la comunicación se vea amparada por una situación de gravedad o de emergencia relacionada con su puesto de trabajo o con el mantenimiento adecuado de la actividad de la organización. Dicha valoración se realizará teniendo en cuenta y dándole prioridad al derecho de desconexión digital que la ley reconoce al trabajador.
* Durante el período de guardias establecidas en la entidad o cuando el puesto desempeñado implique atender consultas o incidencias urgentes de los clientes.

Como regla general, a efectos de garantizar el derecho a la desconexión digital en relación con la efectiva conciliación de la vida personal, familiar y laboral, y a salvo de las excepciones previstas, todos los integrantes de la organización ostentan las siguientes obligaciones:

* Las personas trabajadoras tendrán la obligación de dejar un mensaje de aviso en el correo electrónico con la mención de “ausente”, indicando los datos de contacto de quien hubiera sido designado por la empresa para su reemplazo, así como las fechas de duración de los períodos de ausencia en los supuestos de vacaciones, días de asuntos propios, libranzas, descanso diario y semanal, permisos, incapacidades o excedencias.
* La convocatoria reuniones de trabajo, tanto a nivel interno como las que se lleven a cabo con clientes, así como la formación obligatoria, se realizará teniendo en cuenta el tiempo aproximado de duración y, preferiblemente, no se extenderán hasta más tarde de la finalización de la jornada ordinaria de trabajo, a fin de que no se vea afectado el tiempo de descanso de las personas trabajadoras.
* Las personas trabajadoras deberán informar a la organización de aquellas nuevas situaciones que puedan verse afectadas al momento de aplicar la presente política de desconexión digital.
* Todos deberán respetar tanto el calendario como el horario laboral que informa la organización.
* Se establece la obligatoria asistencia a los cursos de formación y sensibilización sobre la desconexión digital.
* Debe cumplirse con lo expuesto en los puntos 2.5.1 y 2.5.2 de la presente política.

Situaciones excepcionales a la presente política

No serán de aplicación las medidas que garantizan el derecho a la desconexión digital en los casos en que concurran circunstancias de causa de fuerza mayor o que supongan un grave, inminente o evidente perjuicio empresarial o del negocio, cuya urgencia temporal necesita indubitadamente de una respuesta inmediata.

En dichos supuestos en los que ${razon} requiera una respuesta de la persona trabajadora una vez finalizada su jornada laboral, contactará con aquélla preferiblemente por teléfono para comunicarle la situación de urgencia que motiva dicha situación. El tiempo de trabajo así requerido podría calificarse como hora extraordinaria, de conformidad con lo establecido en cuanto a jornada y/o política de horas extraordinarias en el marco laboral de la entidad y/o el convenio colectivo.

Se excluye la aplicación del derecho a desconexión digital a aquellas personas trabajadoras que permanezcan a disposición de la Compañía y perciban, por ello, un complemento de “disponibilidad” u otro de similar naturaleza, en el entendimiento de que, durante el tiempo de atención continuada en régimen de localización, la persona trabajadora tendrá la obligación de atender las comunicaciones de ${razon} , de conformidad a las normas que regulen el correspondiente régimen de disponibilidad en cada una de las empresas

Medidas de Sensibilización

${razon} implementará las medidas de sensibilización sobre las que se ampara el derecho a la desconexión digital. Para lo cual se informará y/o formará a las personas trabajadoras sobre la necesaria protección de este derecho, teniendo en cuenta las circunstancias tanto laborales como personales de todos los trabajadores, y para ello pondrá a disposición de los mismos toda la información y/o formación que precisen para la comprensión y posterior aplicación de las mencionadas medidas protectoras del derecho a la desconexión digital. Corresponde a quienes tengan la responsabilidad sobre un equipo y/o superiores jerárquicos de las personas

trabajadoras, fomentar y educar mediante la práctica responsable de las tecnologías y con el propósito de dar cumplimiento al derecho a la desconexión digital.

La presente política debe ser conocida y estar accesible para todos los integrantes de la entidad, por lo cual se distribuirá la misma a través de los canales habilitados para ello dentro de la organización.

**MODO NO MOLESTAR**

Consiste en la posibilidad de programar nuestro móvil para silenciar notificaciones, llamadas, mensajes, alertas sin necesidad de apagarlo. Existen diferentes posibilidades al momento de programar el modo no molestar, por ejemplo, podemos elegir los días y las horas en las que deseamos que no se nos moleste

También podemos seleccionar las excepciones, por ejemplo, las llamadas entrantes de un número Determinado o bien si tenemos configurada alguna alarma

Podremos configurar nuestro dispositivo para:

* Silenciar totalmente el dispositivo, por lo cual no se reproducirán sonidos, notificaciones, llamadas y alarmas.
* Silenciar todo menos las alarmas, por lo cual, el único sonido que reproducirá nuestro dispositivo será el correspondiente a las alarmas configuradas.
* Personalizar que queremos silenciar y que no; por ejemplo, podremos configurar que nuestro dispositivo entre de forma automática en modo no molestar, de lunes a viernes entre las 12 de la noche y las 9 de la mañana; o bien configurar de que números de teléfono podremos escuchar la notificación correspondiente a llamadas y/o mensajes que nos entren cuando el “modo no molestar” esté operativo.

Configuración:

Android

Desde la pantalla de ajustes rápidos (deslizando el dedo de arriba hacia abajo por la pantalla) > Opción: “Sonidos y vibración” o “Sonidos” o “No molestar” (según el terminal y la versión) > Una vez allí, podremos configurar el modo no molestar de acuerdo a nuestras necesidades

Ios

Desde la pantalla de ajustes rápidos (deslizando el dedo de arriba hacia abajo por la pantalla) > Ajustes > No molestar > Activar en manual o bien programado. A través de esta última opción, podremos configurarlo de acuerdo a nuestras necesidades

**GEOLOCALIZACIÓN**

Geolocalizar a los trabajadores supone tratar sus datos personales ya que los datos de localización se refieren a una persona física identificada. En el caso de que la empresa se plantee instalar un GPS en los vehículos de empresa para conocer la ubicación de sus trabajadores durante la jornada laboral debe cumplir varios requisitos:

Información.

No es necesario que los trabajadores autoricen a instalar estos dispositivos. Pero sí es necesario informarles previamente de que se van a controlar sus desplazamientos. Indicando la finalidad del control y el sistema de geolocalización utilizado.

Necesidad.

El control por geolocalización debe ser necesario para una finalidad legítima. En consecuencia, sólo puede geolocalizarse a los trabajadores cuyas funciones hagan necesario este tipo de control. La ley no aclara los supuestos en los que se considera que existe una finalidad legítima pero algunos ejemplos serían:

Transporte.

Si se instala en el vehículo de los transportistas para saber la ubicación de los vehículos y coordinar las distintas entregas de mercancía.

Seguridad.

Si se instala en los vehículos de vigilantes de seguridad para conocer dónde se encuentran el vehículo y el trabajador, pues la empresa necesita saber en qué momento y lugar se están realizando las labores de vigilancia.

El uso de datos de geolocalización debe adecuarse al principio de proporcionalidad, esto es, ser proporcionado respecto a la finalidad perseguida. Además, se debe valorar previamente si se pueden usar otros medios menos intrusivos para la supervisión del personal y la localización de empleados.

En concreto, el artículo 90.1 de la Ley Orgánica de Protección de Datos (LOPDGDD) lo explica de esta manera:

*Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.*

Hay que tener en cuenta que el derecho del empleador a utilizar estos dispositivos debe respetar el derecho a la desconexión digital y a la limitación del tratamiento de datos de los empleados.

En este sentido, la geolocalización de empleados solo se podrá realizar en horas laborales y con la finalidad exclusiva de conocer la localización del trabajador. No se podrá usar fuera del horario de trabajo ya que se vulneraría el derecho a la desconexión digital del trabajador

**CONTROL DE LA ACTIVIDAD EMPRESARIAL**

El ET ha atribuido facultades específicas a la empresa que posibilitan el control del desarrollo de la prestación laboral. El ejercicio de estas facultades comporta en muchas ocasiones un tratamiento de datos personales.

El consentimiento de la persona trabajadora no es necesario, pues la base jurídica para la implantación de medidas de control de las personas trabajadoras y para el tratamiento de los datos personales que en tal contexto sean captados se encuentra en el artículo 20.3 del ET:

El control empresarial puede ser más o menos sofisticado, pero la implantación de nuevas tecnologías incrementa el riesgo de afectación a los derechos de las personas trabajadoras, por su gran potencial invasivo: controles biométricos como la huella dactilar, videovigilancia, geolocalización, etc.

Por ello, la implantación de medidas de control exige realizar un test de proporcionalidad en el que debe valorarse si la medida de control:

* Es susceptible de conseguir el objetivo propuesto (juicio de idoneidad).
* Es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad).
* Es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Superado el test, el empleador podrá adoptar la medida de control, pero habrá de respetar el derecho a la protección de datos si se produce un tratamiento de datos personales

El art. 88 del RGPD atribuye al convenio colectivo un papel relevante para establecer medidas más protectoras para la persona trabajadora en el tratamiento de datos que se produce al implantar «sistemas de supervisión en el lugar de trabajo».

La prevención debería tener mucho más peso que la detección, pues la prevención evita el riesgo de vulneración posterior de derechos fundamentales en la fase de control. Esa prevención se vincula con la subsidiariedad, que supone que la medida potencialmente invasiva de derechos fundamentales debe ceder ante medidas preventivas que hagan desaparecer el riesgo.

**ANEXOS**

**CONSENTIMIENTO DE DATOS DE GEOLOCALIZACIÓN**

Don/Doña \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, con DNI \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_mediante el presente documento MANIFIESTA que AUTORIZA a: ${razon} con domicilio en: ${domicilio} y NIF/CIF ${cif} , para recabar y tratar automatizadamente en un fichero del que es responsable los datos de geolocalización recogidos a través de (indicar el sistema de geolocalización) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , con previo consentimiento de quien firma el presente documento.

Así mismo, el firmante del presente documento, declara que ha sido previamente informado por el Responsable o Representante de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ en lo concerniente a lo siguiente:

1. Que, ${razon} dispone de un fichero de Recursos Humanos, cuya finalidad es proceder a la gestión adecuada de los trabajadores y de las funciones adquiridas en \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
2. Que los datos de carácter personal obtenidos van a ser incorporados en el fichero de Recursos Humanos.
3. Que, ${razon} dispone de todas las medidas de seguridad en materia de protección de datos de carácter personal recogidas en el Real Decreto 1720/2007 de 21 de diciembre.
4. Que, ${razon} podrá ceder a terceros los datos personales facilitados por el abajo firmante, únicamente con objeto de que se realicen determinados tratamientos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
5. Que puede ejercitar, en todo momento, los derechos ARCO (Acceso, rectificación, cancelación y oposición) reconocidos en la LOPD, en los términos y condiciones que las normativas aplicables establecen, ante \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, como Responsable del Fichero en la dirección postal facilitada al inicio de este documento.

Y en prueba de conformidad, el abajo firmante da su aceptación y consentimiento para que los datos referentes a su localización geográfica sean incluidos en el fichero de Recursos Humanos.

En \_\_\_\_\_\_\_\_\_\_\_ , a \_\_\_\_\_\_\_de \_\_\_\_\_\_\_ de 20\_\_\_\_

Firma trabajador/a: Firma Responsable empresa:

**CARTEL INFORMATIVO**

**INFORMACIÓN A EMPLEADOS DE LAS GARANTÍAS DE LOS DERECHOS DIGITALES RECOGIDAS EN LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE.**

${razon} con CIF ${cif}, domiciliada en ${domicilio} y contacto a través de: número de teléfono ${tel}y correo electrónico ${correo}

INFORMA,

* Usted, como empleado de ${razon}, tiene garantizadas todas las garantías digitales reconocidas en la legislación vigente.
* La desconexión Digital reconoce el derecho del trabajador a no estar disponible fuera del horario laboral.
* Se informa a los trabajadores de la existencia de control empresarial de los medios telemáticos de la empresa con el fin de verificar el efectivo cumplimiento de sus obligaciones legales y deberes laborales. La información recabada por estos medios podrá ser utilizada con fines disciplinarios y de verificación judicial.
* Al abandonar su puesto de trabajo o su terminal informático es su responsabilidad retirar de la vista o el alcance cualquier información confidencial. Política de pantalla y escritorio limpio.

Para solicitar información o ejercer cualquiera de los derechos recogido en el Reglamento General de Protección de Datos y La Ley 3/2018, deberá contactar con nosotros a través de la siguiente dirección ${domicilio} o mediante la dirección de correo electrónico ${correo}, pudiendo solicitársele copia de su DNI o pasaporte, a fin de acreditar su identidad.

**ANEXO AL CONTRATO – TELETRABAJO**

El presente protocolo está destinado a regular las condiciones para la realización de teletrabajo por parte de los empleados de ${razon} con NIF ${cif}, y domicilio en ${domicilio}, de acuerdo a las leyes vigentes en protección de datos (RGPD y LOPDGDD).

Las condiciones previstas en este documento serán de aplicación a todos los trabajadores de la Empresa con los que se haya acordado la realización total o parcial de las jornadas laborales a distancia, mediante el uso de dispositivos electrónicos, facilitados o no por parte de la Empresa.

SOPORTES Y SISTEMAS AFECTADOS

Los principales soportes y sistemas afectados por este protocolo son:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CONDICIONES PARA LA REALIZACIÓN DEL TELETRABAJO

La realización de las tareas a distancia por parte del trabajador estará supeditada a las siguientes condiciones:

* Autorización por parte de la Empresa, que habilite al trabajador a desarrollar sus tareas y funciones fuera de las instalaciones de la Empresa.
* La Empresa deberá haber detallado el período durante el cual se extiende el teletrabajo, además del horario laboral y tipo de jornada de cada trabajador.
* El traslado de soportes de las instalaciones de la empresa deberá estar autorizado por la empresa.

Asimismo, se vinculará cada soporte con un trabajador concreto.

* El uso soportes y sistemas, está supeditado al cumplimiento de las mismas medidas de seguridad que la empresa impone para el trabajo presencial.
* El trabajador gestionará sus claves personales de acceso a soportes y sistemas con la máxima diligencia, no comunicándolas a terceras personas y actualizando las consignas con la periodicidad indicada por la Empresa.
* El trabajador se compromete a comunicar cualquier robo, pérdida o acceso no autorizado a la información de la Empresa, en un plazo máximo de 24 horas. Para la notificación de la brecha de seguridad deberá dirigirse al correo electrónico ${correo}

USO DE DISPOSITIVOS PERSONALES

En caso de que el empleado desarrolle el teletrabajo con sus propios dispositivos personales, deberá seguir las siguientes pautas:

* Impedir el acceso de terceros a los dispositivos dotados con claves de acceso (claves, contraseñas, permisos, patrones de seguridad).
* Verificar que el software antivirus y el firewall está actualizado y que el equipo se encuentra protegido.
* Evitar el acceso a conexiones inalámbircas poco seguras, como las redes Wi-Fi abiertas.
* Eliminar de sus dispositivos todos los datos a los que hubiera tenido acceso de forma legítima. No será posible conservar una copia aunque hubiera descargado la información en su equipo u otro dispositivo.
* Comunicar robos, pérdidas de información u otras incidencias de la misma manera que si se tratase de dispositivos de la empresa, a través del correo electrónico ${correo}

DERECHO A LA DESCONEXIÓN DIGITAL

La Empresa implantará y coordinará el teletrabajo desde el respeto y reconocimiento del derecho a la desconexión digital de los trabajadores, de acuerdo al art. 88 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Este documento pretende garantizar la conciliación entre la vida laboral y familiar. Por tanto, se entiende que los trabajadores tienen derecho a ejercer la desconexión digital, fuera de la jornada laboral pactada con la empresa para el teletrabajo.

En \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, a \_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 20\_\_\_

Firma empleado/a Firma empresa

**NOTIFICACIÓN A EMPLEADOS DE REGISTRO DE GARANTÍAS DIGITALES**

Mediante la firma del presente documento declaro haber recibido y ser conocedor/a del Registro de Garantías Digitales implantado en ${razon}, en el cual se definen la serie de derechos que dispongo en materia de garantías digitales, así como de los derechos inherentes de la empresa para disponer de los materiales laborales e informáticos que pone a i disposición con el fin de ejercer su labor de control.

Nombre del trabajador/a:

DNI:

Fecha y lugar:

Firma: