GUÍA LEGAL

IMPLANTACIÓN Y ADECUACIÓN AL RGPD

LUCAS BARRIENTOS RUBIO

Documentación elaborada por:

INTRODUCCIÓN

Por medio de la presente Guía Legal, 2AConsulting **informa y documenta** acerca de todo lo necesario para **cumplir con el Reglamento (UE) 2016/679 General de Protección de Datos** (en adelante, <<**RGPD**>>).

La Guía consta de dos partes:

- I. EXPLICACIÓN TEXTOS LEGALES: en esta primera parte, se explica en qué consisten las cláusulas o textos legales que deben facilitarse a ***clientes y potenciales clientes***, ***proveedores, empleados y página web*** y, cómo implantarlos en la organización conforme a las recomendaciones de 2AConsulting y de la Agencia Española de Protección de Datos (en adelante, <<**AEPD**>>). Esta parte se divide en los siguientes apartados:

Contenido

{ TOC \o "1-3" \h \z \u }

- II. TEXTOS LEGALES: esta segunda parte contiene los textos legales explicados en la primera parte. Los textos legales aparecen en forma de ANEXO y están debidamente enumerados:

Si tras la lectura de la Guía Legal tuviera alguna duda, puede dirigirse al correo electrónico { HYPERLINK "mailto:comunicacionlegal@dobleaconsulting.es" } o llamar al número de teléfono 667 574 525.

I. EXPLICACIÓN TEXTOS LEGALES

1. CLIENTES Y POTENCIALES CLIENTES

Entre los deberes de la empresa como Responsable del Tratamiento, se encuentra el deber de información.

Por ello, cuando recabamos datos de nuestros clientes (personas con las que ya mantenemos una relación contractual o comercial) y potenciales clientes (personas con las que todavía no tenemos un relación contractual o comercial, pero se han puesto en contacto con nosotros para, por ejemplo, solicitarnos un presupuesto) como pueden ser datos de contacto de la persona con la que nos relacionamos como su nombre y apellidos, DNI, cargo desempeñado, correo electrónico o teléfono profesional, debemos informarle sobre qué haremos con sus datos y recabar en la medida de lo posible su consentimiento.

Conforme a las recomendaciones de la AEPD, esta información deberá proporcionarse a través de un sistema de "doble capa" que consiste en lo siguiente:

- 1º capa: información resumida sobre protección de datos, preferiblemente en formato "tabla".
- 2º capa: información más completa sobre protección de datos, de forma que el usuario pueda consultarla opcionalmente si no queda satisfecho con la información proporcionada en la 1º capa.

Teniendo presente lo anteriormente explicado, para informar debidamente a los clientes y potenciales clientes sobre el tratamiento de sus datos deberá seguir las siguientes instrucciones, diferenciando si sus datos se recaban presencialmente, por la página web (si la tuviera), por correo electrónico o a través de llamada telefónica.

- **Presencialmente**: por ejemplo, a través de un formulario físico donde puedan rellenar sus datos. En este caso, deberá facilitarse la 1º capa en el propio documento o formulario y, dar la posibilidad de consultar la 2º capa, añadiendo el texto en el reverso del formulario o documento, o incorporándolo en un cartel informativo que sea visible. La 1º capa la puede encontrar en el ANEXO 1. PRIMERA CAPA POLÍTICA DE PRIVACIDAD y la 2º capa en ANEXO 2. SEGUNDA CAPA POLÍTICA DE PRIVACIDAD.

- **A través de la página web**: por ejemplo, mediante un formulario de "contacto" o "registro" de la página web. En este caso, deberá facilitarse la 1º capa junto al formulario y, poner a disposición del interesado, la 2º capa a través de un link que enlace a este texto. La 1º capa la puede encontrar en el ANEXO 10. PRIMERA CAPA POLÍTICA DE PRIVACIDAD (WEB) y la segunda capa en el ANEXO 11. SEGUNDA CAPA POLÍTICA DE PRIVACIDAD (WEB). Sobre estos textos volveremos a hablar en el apartado *4. PÁGINA WEB*.

- **A través del correo electrónico**: es muy habitual que los datos de clientes y potenciales clientes se recaben a través del correo electrónico. Para informar sobre estos datos, los empleados deberán responder a estos correos incorporando una cláusula a modo de pie de firma. Es recomendable que esta cláusula aparezca de forma permanente. Esta cláusula contiene la misma información que la 1º capa pero está adaptada a este medio; por ello, hemos creado una específica para este supuesto. Puede encontrar esta cláusula en el ANEXO 9. CLÁUSULA DE CORREO ELECTRÓNICO. Sobre esta cuestión volveremos cuando tratemos el apartado *3. EMPLEADOS.*

- **Por llamada telefónica:** si le aportasen datos personales a través de una llamada telefónica, deberá a continuación enviar un correo de confirmación y en este correo cerciorarse que está incluida la anterior cláusula del ANEXO 9. CLÁUSULA DE CORREO ELECTRÓNICO. Otra solución es grabar una locución automática que pueda consultarse marcando una tecla al inicio de cada llamada, y que reproduzca el contenido de la cláusula ANEXO 1. PRIMERA CAPA POLÍTICA DE PRIVACIDAD. Por ejemplo: "si quiere consultar nuestra Política de Privacidad marque la tecla 0".

2. PROVEEDORES

A. *Proveedores con acceso a datos: Encargados de Tratamiento*

El RGPD considera como encargado de tratamiento a todos aquellos proveedores o prestadores de servicios que necesitan acceder y/o tratar los datos personales responsabilidad de LUCAS BARRIENTOS RUBIO para prestar dichos servicios.

A LUCAS BARRIENTOS RUBIO , como Responsable de Tratamiento, le es exigible un deber de diligencia en la elección y supervisión de sus encargados de tratamiento, debiendo elegir sólo a aquellos que ofrezca las garantías necesarias para aplicar las medidas técnicas y organizativas que correspondan al tratamiento, cumpliendo así con los requisitos del Reglamento General de Protección de Datos (RGPD) y garantizando la protección de datos personales de los interesados.

El modelo de contrato de Encargado de Tratamiento que se propone en el ANEXO 3. CONTRATO DE ENCARGADO DE TRATAMIENTO, contiene los requisitos del RGPD y deberá ser firmado con todos aquellos proveedores de LUCAS BARRIENTOS RUBIO que necesiten acceder a los datos de su responsabilidad para prestar sus servicios.

Por ejemplo y con carácter enunciativo pero no limitativo:

- Asesoría Laboral/Contable/Fiscal.
- Empresa de mantenimiento y soporte informático.
- Empresa de mantenimiento de software, hosting, cloud, tic…
- Videovigilancia con acceso a las imágenes.
- Autónomos que presten servicios.
- Agencias de Medios/Comunicación/Marketing/Explotación de datos.

B. *Proveedores sin acceso a datos*

Es muy común que existan proveedores que presten un servicio a LUCAS BARRIENTOS RUBIO para el que no necesiten acceder a datos personales.

El documento facilitado en el ANEXO 4. COMPROMISO DE CONFIDENCIALIDAD SIN ACCESO A DATOS es un contrato a suscribir por las personas que lleven a cabo una prestación de servicios sin acceso a datos, por ejemplo, por el personal de limpieza, mantenimiento o el servicio de mensajería.

3. EMPLEADOS

¿Debo informar a mis empleados del tratamiento de sus datos?

Para que las empresas puedan desarrollar su actividad, en la mayoría de ocasiones, es necesario que contraten a personas físicas y que éstas desempeñen sus funciones bajo las instrucciones de la propia organización. Estas personas conforman lo que se conoce como el personal laboral de la empresa. Para desarrollar la relación laboral, LUCAS BARRIENTOS RUBIO necesita tratar los datos personales de sus empleados. Por lo tanto, de acuerdo al RGPD deberá informar a dichos empleados del tratamiento de sus datos personales necesario para el mantenimiento de la relación laboral. Para cumplir este deber será necesario que todos los empleados de la empresa firmen el documento facilitado en el ANEXO 5. DOCUMENTO DE INFORMACIÓN Y COMPROMISO DE CONFIDENCIALIDAD. Este documento informa a los trabajadores del tratamiento de sus datos personales. Además les informa de su compromiso de confidencialidad respecto a los datos personales que pudieran conocer en el desempeño de sus funciones.

¿Deben ser informados de sus obligaciones en el tratamiento?

Por otro lado, en el desempeño de tales funciones, gran parte del personal accede y/o trata datos de carácter personal. Por ejemplo, los administrativos de las empresas suelen manejar multitud de datos de carácter personal como, por ejemplo, números de teléfono móvil o correos electrónicos, ya sea de clientes, proveedores, de otros trabajadores, etc. Para informar a los trabajadores de sus obligaciones en materia de protección de datos, deberán conocer y firmar los siguientes documentos:

- Funciones y obligaciones del personal con acceso a datos, dispuestas en el ANEXO 6. FUNCIONES Y OBLIGACIONES DEL PERSONAL. La firma de este documento prueba que el trabajador tiene el conocimiento suficiente para saber cómo tratar los datos de carácter personal de acuerdo a la normativa sobre protección de datos.

- Política de contraseñas para el personal que utilice soportes informáticos, facilitado en el ANEXO 7. POLÍTICA DE CONTRASEÑAS. La firma de este documento acredita que el trabajador sabe cómo elegir, cambiar y proteger adecuadamente las contraseñas que utiliza para acceder y/o tratar los datos de carácter personal.
- Protocolo de actuación en caso de violación de seguridad, dispuesto en el ANEXO 8. PROTOCOLO DE ACTUACIÓN EN CASO DE VIOLACIÓN DE SEGURIDAD. Una violación de seguridad es cualquier incidente que ocasione la destrucción, pérdida, alteración accidental o ilícita de los datos de carácter personal así como su comunicación o acceso no autorizado. El documento detalla el procedimiento que debe seguir la organización cuando se produce una violación de seguridad desde el momento inicial en que un trabajador la detecta. La firma de este documento acredita que el empleado está al tanto de dicho procedimiento.

Por último, los trabajadores deben incluir una información básica sobre protección de datos en todos los emails que envíen a través de su correo corporativo. Esta información, como ya se explicó anteriormente en el apartado *1. CLIENTES Y POTENCIALES CLIENTES*, la puede encontrar en el ANEXO 9. CLÁUSULA DE CORREO ELECTRÓNICO.

4. PAGINA WEB

Una página web es un canal de comunicación que utilizan las empresas principalmente para darse a conocer y promocionar sus productos y servicios pero también para cubrir otras necesidades como realizar ventas online, compartir fotos, organizar sus recursos, etc.

Desde el punto de vista de la normativa sobre protección de datos y de comercio electrónico y servicios de la sociedad de la información, las empresas deben incorporar en su página web distintos textos legales en función de las características concretas de cada una de ellas:

- Aviso Legal: Contiene la información mínima necesaria para que el usuario que visita la página web conozca quién es la organización titular del sitio web. Esta cláusula facilitada en forma de tabla deberá ser incorporada en la página web de las empresas siempre que faciliten, publiciten u ofrezcan un determinado producto o servicio.

  Únicamente quedarán excluidos de tal obligación blogs o páginas que no realicen ningún tipo de actividad comercial. Puede encontrar el modelo en el ANEXO 10. AVISO LEGAL.

  Además de facilitar la información básica identificativa de la empresa, se pueden añadir múltiples cláusulas no relacionadas estrictamente con la protección de datos o con la normativa sobre comercio electrónico y servicios de la sociedad de la información, sino con otras materias como propiedad intelectual, propiedad industrial, etc.

  Esta información deberá estar accesible desde una pestaña genérica que aparezca no sólo en la página principal de la página web sino también en las restantes subpáginas.

- 1º capa y 2º capa de Política de Privacidad: como explicamos en el apartado *1.CLIENTES Y POTENCIALES CLIENTES,* la 1º capa y 2º capa de la Política de Privacidad debe incorporarse en aquellas **páginas web que recaben datos de carácter personal** a través de mecanismos tales como formularios de contacto, formularios de registro, formulario a rellenar con los datos bancarios antes de realizar una compra online, newsletter, etc. La forma de incorporar estos textos es:

  - **1º capa,** deberá facilitarla de forma inicial al enviar los datos personales a través de la página web. Por ello, tiene que incorporarla junto al formulario de forma permanente o en forma de "pop-up" o desplegable, cuando se marque la casilla de "He leído y Acepto la Política de Privacidad". Al respecto, es importante habilitar herramientas que impidan al usuario enviar sus datos personales a no ser que haga clic en la casilla. Esta casilla en ningún caso podrá aparecer pre marcada. El texto de la 1º capa puede encontrarlo en el ANEXO 11. PRIMERA CAPA POLÍTICA DE PRIVACIDAD (WEB).

- **2º capa**, deberá estar accesible :
  - Pinchando en un enlace habilitado a tal efecto en la 1ª capa.
  - Desde una pestaña genérica que aparezca no sólo en la página principal de la página web sino también en las restantes subpáginas, como ocurre con el Aviso Legal.

  El texto de la 2º capa puede encontrarlo en el ANEXO 12. SEGUNDA CAPA POÍTICA DE PRIVACIDAD (WEB)

- **Aviso y Política de Cookies**: Han de aparecer siempre que se utilicen cookies que no estén exceptuadas de esta obligación (cookies técnicas). La forma de incorporar estos textos es:

  - **Aviso de Cookies (1ª capa o banner de cookies)**. Esta 1º capa contiene la información básica sobre las cookies Este Aviso debe incluir la siguiente información: (i) advertencia del uso de cookies propias, de terceros o ambas, (ii) finalidades de las cookies, (iii) advertencia de que si se realiza una determinada acción se entenderá que el usuario está dando su consentimiento y (iv) enlace a la Política de Cookies íntegra (2ª capa).

    El Aviso de Cookies se ofrecerá en la página de inicio, de forma que al entrar en la web sea fácilmente identificable y visible por parte del usuario, bien sea en la parte superior o en cualquier otro lugar.

    Puede encontrar el texto en el ANEXO 13. AVISO DE COOKIES

  - **Política de Cookies (2ª capa).** La segunda capa contiene información más detallada sobre las cookies. Este texto deberá concretar como mínimo: (i) definición y función de las cookies, (ii) información a través de un cuadro o listado sobre el tipo de cookies que utiliza la web y su finalidad, identificando también cuáles son propias y cuáles de terceros e (iii) información sobre la forma de desactivar o eliminar las cookies. La Política de Cookies deberá ser accesible:
    - Pinchando en el enlace que aparece en el Aviso de Cookies (1ª capa o banner de cookies).
    - Desde una pestaña genérica que se encuentre accesible desde todas las pestañas de la página web, como ocurre con el Aviso Legal y la Política de Privacidad.

    Puede encontrar el texto en el ANEXO 14. POLÍTICA DE COOKIES

II. TEXTOS LEGALES

ANEXO 1. PRIMERA CAPA POLÍTICA DE PRIVACIDAD.

Siguiendo los principios de licitud, lealtad y transparencia, ponemos a su disposición la presente tabla informándole del tratamiento de los datos personales que se dispone a proporcionarnos:

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS	
RESPONSABLE	LUCAS BARRIENTOS RUBIO margomrom@hotmail.com
FINALIDAD PRINCIPAL	Mantener relaciones profesionales y/o comerciales Gestionar la suscripción … (SEÑALAR LAS FINALIDADES QUE PROCEDAN)
LEGITIMACIÓN	Consentimiento del interesado
DESTINATARIOS	No se cederán datos a terceros, salvo autorización expresa u obligación legal (SI SE DECIERAN DATOS A OTRAS EMPRESAS QUE NO FUERAN ENCARGADOS DE TRATAMIENTO, SE DEBE ESPECIFICAR)
DERECHOS	Acceder, rectificar y suprimir los datos, portabilidad de los datos, limitación u oposición a su tratamiento, transparencia y derecho a no ser objeto de decisiones automatizadas.
INFORMACIÓN ADICIONAL	Puede consultar la información adicional y detallada sobre nuestra Política de Privacidad en { HYPERLINK } *(SE REDIRIGE A LA POLITICA DE PRIVACIDAD INTEGRA, SEGUNDA CAPA)*

☐ Declaro haber entendido la información facilitada y consiento el tratamiento que se efectuará de mis datos de carácter personal (ESTA CASILLA DEBE MARCARLA EL INTERESADO NECESARIAMENTE)

En caso de que desee recibir información marque la siguiente casilla:

☐ Autorizo al envío de comunicaciones informativas relativas a las actividades, productos o servicios por correo postal, fax, correo electrónico o cualquier otro medio electrónico equivalente (ESTA CASILLA ES OPCIONAL POR EL INTERESADO)

DIA/MES/AÑO

FIRMA

ANEXO 2. SEGUNDA CAPA POLÍTICA DE PRIVACIDAD.

POLÍTICA DE PRIVACIDAD

Siguiendo los principios de licitud, lealtad y transparencia, ponemos a su disposición la presente Política de Privacidad.

¿Quién es el Responsable del tratamiento de sus datos?

LUCAS BARRIENTOS RUBIO

CIF: 32667460P

DOMICILIO SOCIAL: AVDA. DE PARIS, Nº 31, 10005, CÁCERES (CÁCERES)

Email: { HYPERLINK "mailto:email@email.com" }

Teléfono: 647 908 541

¿Con qué finalidad tratamos sus datos personales?

En LUCAS BARRIENTOS RUBIO tratamos la información que nos facilita con la finalidad de gestionar la relación contractual que nos une, gestionar el envío de la información que nos solicita, facilitar a los interesados ofertas de nuestros servicios y/o productos de su interés y/o gestionar su candidatura.

¿Por cuánto tiempo conservaremos sus datos personales?

Sus datos, serán conservados el tiempo mínimo necesario para la correcta prestación del servicio ofrecido así como para atender las responsabilidades que se pudieran derivar del mismo y de cualquier otra exigencia legal.

¿Cuál es la legitimación para el tratamiento de sus datos?

La base legal para el tratamiento de sus datos personales puede ser la ejecución de una relación contractual potencial y/o suscrita, el interés legítimo, la habilitación legal y/o el consentimiento del propio interesado. Los datos que le solicitamos son adecuados, pertinentes y estrictamente necesarios y en ningún caso está obligado a facilitárnoslos, pero su no comunicación podrá afectar a la finalidad del servicio o la imposibilidad de prestarlo.

¿A qué destinatarios se comunicarán sus datos?

LUCAS BARRIENTOS RUBIO no comunicará sus datos a ningún tercero, salvo su consentimiento expreso u obligación legal.

¿Cuáles son sus derechos cuando nos facilita sus datos?

Los derechos de protección de datos de los que son titulares los interesados son:

- Derecho a solicitar el acceso a los datos personales relativos al interesado
- Derecho de rectificación o supresión
- Derecho de oposición

- Derecho a solicitar la limitación de su tratamiento
- Derecho a la portabilidad de los datos

Los titulares de los datos personales obtenidos, podrán ejercer sus derechos de protección de datos personales dirigiendo una comunicación por escrito al domicilio social de LUCAS BARRIENTOS RUBIO o al correo electrónico habilitado a tal efecto, { HYPERLINK "mailto:email@email.com" }, incluyendo en ambos casos fotocopia de su DNI u otro documento de identificación equivalente.

Modelos, formularios y más información disponible sobre sus derechos en la página web de la autoridad de control nacional, Agencia Española de Protección de Datos, en adelante, AEPD, { HYPERLINK "http://www.agpd.es" }

¿Puedo retirar el consentimiento?

Usted tiene la posibilidad y el derecho a retirar el consentimiento para cualquiera finalidad específica otorgada en su momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

¿Dónde puedo reclamar en caso de que considere que no se tratan mis datos correctamente?

Si algún interesado considera que sus datos no son tratados correctamente por LUCAS BARRIENTOS RUBIO puede dirigir sus reclamaciones al correo { HYPERLINK "mailto:email@email.com" } o a la autoridad de protección de datos que corresponda, siendo la AEPD la indicada en el territorio nacional, { HYPERLINK "http://www.agpd.es" }

Seguridad y actualización de sus datos personales

Con el objetivo de salvaguardar la seguridad de sus datos personales, le informamos que LUCAS BARRIENTOS RUBIO ha adoptado todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales suministrados. Todo ello para evitar su alteración, pérdida, y/o tratamientos o accesos no autorizados, tal como exige la normativa, si bien la seguridad absoluta no existe.

Es importante que, para que podamos mantener sus datos personales actualizados, nos informe siempre que se produzca una modificación de los mismos.

Confidencialidad

LUCAS BARRIENTOS RUBIO le informa que sus datos serán tratados con el máximo celo y confidencialidad por todo el personal que intervenga en cualquiera de las fases del tratamiento. No cederemos ni comunicaremos a ningún tercero sus datos, excepto en los casos legalmente previstos, o salvo que el interesado nos hubiera autorizado expresamente.

ANEXO 3. CONTRATO DE ENCARGADO DE TRATAMIENTO

En _____, a ___ de _____ de _____

En _____, a ___ de _____ de _____

De una parte, don/doña _____ provisto de DNI nº _____ actuando como legal representante de **LUCAS BARRIENTOS RUBIO** con domicilio en **AVDA. DE PARIS, Nº 31, 10005, CÁCERES (CÁCERES)** y CIF **32667460P** en adelante (en adelante, <<Responsable de Tratamiento>> o <<Encargado>>)..

De una parte, don/doña _____ provisto de DNI nº _____ actuando como legal representante de _____ con domicilio en _____ y CIF _____ en adelante (en adelante, <<Encargado de Tratamiento>> o <<Encargado>>).

Ambas partes, reconociéndose mutuamente capacidad legal suficiente para obligarse mediante este documento, y manifestando tener vigentes sus poderes y ser suficientes para obligar a sus representadas,

MANIFIESTAN

I.- Que, en cumplimiento de la normativa de protección de datos y, en especial, conforme al ***artículo 28 del Reglamento (UE) 2016/679 General de Protección de Datos,*** ambas partes de forma libre y espontánea voluntad acuerdan regular el acceso y tratamiento de los datos de carácter personal de conformidad con las siguientes

CLÁUSULAS

1. Objeto del encargo de tratamiento

Mediante las presentes cláusulas se habilita al Encargado de Tratamiento para tratar y/o acceder, por cuenta del Responsable, a los datos de carácter personal que sean necesarios para la prestación del servicio de _____ (indicar)

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el Responsable del Tratamiento, pondrá a disposición del Encargado del Tratamiento o le dará acceso, a la información que se describe a continuación:

2. a) Datos personales objeto de tratamiento (indicar)

	NIF		Tarjeta Sanitaria
	Nº Seguridad Social		Características Personales
	Nombre y apellidos		Circunstancias Sociales
	Dirección postal		Datos académicos/profesionales
	Dirección electrónica		Detalles del empleo
	Teléfono		Información Comercial

	Firma		Datos económicos y de seguros
	Dirección IP		Transacciones de bienes y servicios
	Imagen/voz		Datos de localización
	Marcas Físicas		Firma Electrónica
CATEGORÍAS ESPECIALES			
	Origen étnico o racial		Datos biométricos
	Opiniones/convicciones convicciones políticas, religiosas, filosóficas y/o afiliación sindical		Salud
	Datos genéticos		Vida u orientación sexual
OTROS:			

2.II Categoría de interesados cuyos datos personales son objeto de tratamiento (indicar)

	Empleados		Personas de contacto
	Clientes		Padres y/o tutores
	Proveedores		Representante legal
	Usuarios		Solicitantes
	Asociados o miembros		Beneficiarios
	Propietarios o arrendatarios		Cargos públicos
	Pacientes		Accionistas
	Estudiantes/alumnos		Menores de 13 años
	Datos de terceros		Otros:

2. Duración

La duración del presente acuerdo será la misma que la del acuerdo de prestación de servicios que lo origina.

3. Obligaciones del encargado del tratamiento

El Encargado del Tratamiento y todo su personal se obliga a:

a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo con las instrucciones del Responsable del Tratamiento. En el supuesto que el Encargado considerase que alguna de las instrucciones infringe cualquier normativa relativa a la protección de datos, informará inmediatamente al Responsable.

c) Llevar, por escrito, cuando proceda, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de Responsable , que contenga:

1. El nombre y los datos de contacto del Encargado y de cada responsable por cuenta del cual actúe el Encargado.
2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. Una descripción general de las medidas técnicas y organizativas de seguridad apropiadas que esté aplicando.

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

Únicamente subcontratar la custodia de las copias de seguridad de los datos a los que tenga acceso y/o trate y el mantenimiento de los servidores donde se mantiene la información, los cuales estarán sujetos a cumplir como mínimo las medidas de seguridad que se enuncian en un apartado siguiente.

Si fuera necesario realizar alguna otra subcontratación, este hecho se deberá comunicar previamente y por escrito al Responsable, con una antelación mínima de 15 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el Responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Encargado del Tratamiento y las instrucciones que dicte el Responsable.

Corresponde al Encargado inicial regular la nueva relación de forma que el nuevo Encargado quede sujeto a las mismas condiciones y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte de Subencargado, el Encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

e) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.

f) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

g) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

h) Garantizar que las personan autorizadas para tratar los datos personales, conocen sus funciones y obligaciones respecto al tratamiento de los mismos, según las exigencias del Reglamento o, en su caso, han realizado formación en específica en la materia.

i) Si las personas afectadas ejerciesen los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a obtener información transparente sobre el tratamiento de sus datos ante el Encargado, éste debe comunicarlo a la mayor brevedad posible mediante llamada telefónica o correo electrónico a la dirección que indique el Responsable y, en ningún caso, más allá del segundo día laborable siguiente al de la recepción de la solicitud.

j) El Encargado notificará al Responsable, sin dilación indebida, como máximo en un plazo de 24 horas siguientes desde que se tenga constancia de la misma y a través de la dirección de correo electrónico o número de teléfono que le indique el Responsable, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

Se facilitará, como mínimo, la siguiente información:

I. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

II. Datos de la persona de contacto para obtener más información.

III. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

IV. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

k) Dar apoyo al Responsable en la realización de las consultas previas a la autoridad de control, cuando proceda.

l) Poner a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

m) Implantar las medidas de seguridad necesarias, en función de la naturaleza, alcance, contexto y fines del tratamiento que permitan:

I. Garantizar la confidencialidad, integridad, disponibilidad y resilencia permanentes de los sitemas y servicios de tratamiento

II. Restaurar la disponibilidad y el acceso a los satos personales de forma rápida, un caso de incidente físico o técnico

III. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento

IV. Cuando lo exija el tratamiento, pseudonimizar y cifrar los datos personales

En todo caso, el Encargado de Tratamiento deberá garantizar como mínimo:

- Que existe un control físico a sus instalaciones donde realiza los tratamientos de datos del Responsable.
- Que el acceso a sus sistemas informáticos se realiza por medio de usuarios y contraseñas individuales.
- Que ha delimitado el acceso a los datos del Responsable únicamente a aquellos usuarios que lo precisen.
- Que dispone de copias de seguridad, en su caso, de los datos personales tratados del Responsable.
- En el supuesto de gestionar soportes o documentos con datos personales del Responsable, éstos están debidamente custodiados bajo llave o con dispositivos de cierre equivalentes.
- Que dispone de sistemas de protección perimetral y antivirus de protección de sus sistemas informáticos.
- Que dispone de un registro de incidencias de seguridad.
- Que ha establecido mecanismos y procedimiento de notificación de quiebras de seguridad

n) Una vez finalice el contrato de prestación de servicios, el Encargado del Tratamiento, según las instrucciones del Responsable del Tratamiento, deberá suprimir o devolverle todos los datos personales que obren en su poder, tanto en soporte informático como en soporte papel o, en su caso, facilitárselo a otro encargado que designe el Responsable del Tratamiento. Cualquiera de las dos opciones comportará que el Encargado no tenga en su poder datos personales titularidad del Responsable, salvo que, el encargado deba conservarlos, debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

4. Obligaciones del Responsable del Tratamiento

Corresponde al Responsable del Tratamiento:

a) Entregar al Encargado los datos necesarios para prestar el servicio

b) Dar las instrucciones que correspondan para llevar a cabo el tratamiento

c) Realizar análisis de riesgos y una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el Encargado, cuando proceda.

d) Realizar las consultas previas que correspondan.

e) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento de la normativa vigente en materia de protección de datos por parte del Encargado.

f) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

5. Información sobre protección de datos

El Responsable y el Encargado del Tratamiento (en adelante, << las Partes>>) autorizan la recogida y el tratamiento de los datos de los representantes legales firmantes del contrato principal de prestación de

servicios y, en su caso, de los empleados que actúen como personas de contacto (nombre y apellidos, DNI, correo electrónico, funciones desempeñadas, etc) con la finalidad de gestionar la relación contractual y favorecer la comunicación entre las partes.

Los datos serán conservados como mínimo hasta la finalización del contrato y, más allá de su extinción, si existiera un interés mutuo por las partes en mantener futuras relaciones profesionales y/o comerciales.

La base de legitimación para el tratamiento de los datos es el interés legítimo de las partes, el consentimiento que prestan al suscribir el presente contrato así como la ejecución del mismo.

Las Partes no está obligadas a proporcionarse los datos, pero la no facilitación puede conllevar la imposibilidad de entablar comunicaciones profesionales.

Las Partes se informan que no cederán los datos de los representantes legales ni de las personas de contacto a terceras partes, salvo que medie consentimiento expreso o en cumplimiento de una obligación legal.

En cualquier momento, las Partes podrán ejercitar sus derechos de acceso, rectificación, supresión, portabilidad de los datos, limitación u oposición a su tratamiento, así como a obtener información clara y transparente sobre el tratamiento de sus datos, enviando un escrito acompañado de una fotocopia del DNI o cualquier otro documento identificativo equivalente, a la dirección postal del encabezamiento o a un correo electrónico que se hayan facilitado de común acuerdo.

Si alguna de las Partes, considera que los datos no son tratados correctamente por la otra parte o que las solicitudes de ejercicio de derechos no han sido atendidas correctamente, tienen el derecho a presentar una reclamación a la autoridad de protección de datos que corresponda, siendo la Agencia Española de Protección de Datos la indicada en el territorio nacional, { HYPERLINK "http://www.agpd.es" }.

6. Responsabilidades

El Responsable del Tratamiento queda exonerado de cualquier responsabilidad derivada del incumplimiento por parte del Encargado del tratamiento de las estipulaciones contenidas en el presente contrato, que será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente ante las Autoridades de Protección de Datos, así como de las reclamaciones civiles y penales que los afectados por el incumplimiento puedan interponer ante la jurisdicción ordinaria, exonerando de toda responsabilidad al Responsable del Tratamiento.

ANEXO 4. COMPROMISO DE CONFIDENCIALIDAD SIN ACCESO A DATOS

Compromiso de confidencialidad sin acceso a datos

En __POBLACION__ a ___FECHA___

Estimado Sr./Sra. _____,

En relación a la normativa vigente en materia de protección de datos de carácter personal, queremos comunicarle que **LUCAS BARRIENTOS RUBIO** ha procedido a la implantación de las medidas de seguridad necesarias, con el fin de adaptar e implementar las medidas y requisitos necesarios para el cumplimiento de la normativa europea.

Igualmente se han adoptado las medidas adecuadas para limitar el acceso del personal a los datos personales, a los soportes que los contengan o a los recursos del sistema de información, para **la realización de trabajos que no impliquen el tratamiento de datos personales**.

El contrato de prestación de servicios que nos une, recoge expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal ajeno a **LUCAS BARRIENTOS RUBIO** pudiera conocer con motivo de la prestación del servicio.

Para el acceso incidental a los datos personales que tanto la empresa como sus trabajadores puedan realizar, le recordamos que en ningún caso podrá utilizar o tratar estos datos, ni los comunicará a otras personas o entidades, asumiendo el deber de secreto que se exige a todas las personas de su Organización. Este deber de confidencialidad será exigible durante la prestación de servicios y subsistirá una vez finalizada la misma.

Nombre y Firma

LUCAS BARRIENTOS RUBIO

Nombre y Firma

ANEXO 5. DOCUMENTO DE INFORMACIÓN Y COMPROMISO DE CONFIDENCIALIDAD

Documento de información y compromiso de confidencialidad

De conformidad con la normativa de protección de datos, y con motivo de la **formalización del contrato laboral** firmado con usted, le informamos que sus datos pasarán a formar parte de un tratamiento cuyo **responsable** es LUCAS BARRIENTOS RUBIO , con la **finalidad** de cumplir con todas aquellas obligaciones derivadas de la relación laboral, tales como la formalización de nóminas, cumplimiento de obligaciones sociales y tributarias, deberes en materia de prevención de riesgos laborales, etc.

Asimismo, le informamos que para el cumplimiento de las obligaciones legales y laborales sus datos pueden ser **comunicados a**:

- Entidades y Administraciones Públicas (Seguridad Social, Agencia Tributaria).
- Entidades de protección social, Mutuas de protección laboral y servicios de prevención de riesgos laborales o la preservación de la salud de los trabajadores.
- Entidades bancarias para pagos asociados a la relación laboral.
- Compañías aseguradoras para la tramitación de seguros.
- Administración pública para la solicitud de subvenciones.
- Aquella entidades o clientes que exijan o ante las cuales sea necesario identificar a los empleados: proyectos, formación, mensajería, *renting* y similares.

Sus datos serán **conservados** el tiempo necesario para satisfacer la finalidad para la que fueron recabados y, en todo caso, durante los plazos mínimos exigidos para atender las obligaciones laborales y tributarias.

Con la finalidad de mantener actualizados los datos proporcionados a la entidad, el empleado deberá comunicar en la mayor brevedad posible cualquier cambio que se produzca sobre los mismos.

Asimismo, el trabajador asume el compromiso de confidencialidad y de guardar secreto profesional y/o estatutario respecto de los datos que, con motivo de su actividad laboral, sean objeto de tratamiento por su parte. Dicha obligación subsistirá aun después de finalizar su relación laboral con LUCAS BARRIENTOS RUBIO .

(ELIMINAR PÁRRAFO SI NO HAY VIDEOVIGILANCIA, VERIFICAR FINALIDADES. COMUNICAR IGUALMENTE A LA REPRESENTACIÓN SINDICAL, SI ES QUE LA HUBIERA).

Igualmente queda informado expresamente que las instalaciones de la organización están videovigiladas con fines tanto de seguridad como de control laboral, lo cual se informa igualmente mediante los distintos carteles informativos distribuidos por las distintas ubicaciones de las instalaciones.

Puede **ejercer sus derechos** de acceso, rectificación, cancelación y oposición, así como aquellos reconocidos por el nuevo Reglamento Europeo de Protección de Datos cuando resulte de aplicación, dirigiéndose al responsable de recursos humanos. En caso de no recibir contestación alguna o considerar que su solicitud no ha sido atendida correctamente, el trabajador podrá solicitar la **tutela de sus derechos** ante la Agencia Española de Protección de Datos, { HYPERLINK "http://www.aepd.es" }.

Nombre y apellidos, fecha y firma del empleado

ANEXO 6. FUNCIONES Y OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS

Funciones y obligaciones del personal con acceso a datos de carácter personal

En __POBLACION__ a __FECHA__

Conforme a la normativa sobre protección de datos, todo el personal debe conocer las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir por su incumplimiento. De este modo, a continuación se recogen las principales obligaciones en materia de seguridad sobre los datos personales, así como la información sobre el uso y destino los mismos.

1. El personal solamente podrá **acceder** a los **tratamientos de datos de carácter personal** a los que esté **autorizado** por **LUCAS BARRIENTOS RUBIO** como Responsable del tratamiento y que sean necesarios para el desarrollo de sus funciones laborales, independientemente del dispositivo de tratamiento (informatizado o en soporte papel).

2. Está absolutamente **prohibida la comunicación** de datos personales a terceras partes ajenas a la empresa, excepto en los casos legalmente previstos, y en aquellos supuestos que sea necesario para el desarrollo de la actividad laboral, siempre y cuando estas comunicaciones sean legítimas.

3. El **uso del correo electrónico** es estrictamente profesional, no permitiéndose ningún uso personal de los recursos técnicos e informáticos facilitados por la entidad, excepto en aquellos casos en los que se cuente con el consentimiento expreso del empleador.

   El correo electrónico e internet pueden ser monitorizados, de manera que se informa que los correos electrónicos podrán ser consultados por el empleador con fines profesionales y al objeto de controlar el buen uso de los recursos proporcionados, así como el control técnico en el envío de correos electrónicos a través de la red de la entidad.

4. Todo el personal está obligado a **comunicar** al Responsable del Protección de Datos y/o, en su caso al Encargado departamental de protección de datos, cualquier **solicitud de ejercicio de derechos** de acceso, rectificación, oposición y cancelación y de aquellos derechos reconocidos por el nuevo Reglamento Europeo de Protección de Datos cuando resulte de aplicación, para que puedan atenderse debidamente.

5. El trabajador debe cumplir la **política de accesos a la información**, mediante la observancia de la política contraseñas indicada por la empresa:

   i. Cada usuario es responsable de la confidencialidad y salvaguarda de su propia contraseña, y no puede ser comunicada a terceros ajenos o no a la entidad.

   ii. En caso de elección libre de la contraseña por parte del usuario, queda absolutamente prohibido la utilización de contraseñas fácilmente identificables.

   Por otro lado, se informa que el empleador podrá tener conocimiento de los nombres de usuarios y contraseñas de los trabajadores para verificar el cumplimiento de sus obligaciones y deberes laborales.

6. Todos los usuarios autorizados para acceder a los datos de carácter personal, serán **responsables del puesto de trabajo** desde donde realizan el acceso, y garantizarán que ninguna otra persona no autorizada pueda ver la información sobre datos personales que muestran sus equipos informáticos.

7. Los **tratamientos de datos temporales o copias de documentos** creados exclusivamente para la realización de trabajos puntuales, temporales o auxiliares sólo se realizarán por autorización expresa del Responsable de protección de datos y Encargado departamental de protección de datos, en su caso, y deberán ser borrados o destruidos o incorporados a carpetas o archivos de la entidad cumplida la finalidad que motivo su creación.

8. El **acceso a Internet** mediante el uso de los equipos informáticos facilitados se limitará a temas directamente relacionados con las funciones desarrolladas por el trabajador en la entidad. En concreto el acceso a Internet queda prohibido, salvo autorización expresa de la entidad para:

    i. El acceso y participación en chats y debates a tiempo real, debido al alto riesgo de accesos no autorizados a través de la instalación de aplicaciones a tal efecto.

    ii. El acceso a fuentes de información que requieran el intercambio de datos (FTP, emule o sistemas P2P…..) o páginas Web, limitándose a aquellos que sean imprescindibles y directamente relacionados con la actividad desarrollada por el empleado en la empresa.

    iii. Introducir, descargar desde la red, reproducir, distribuir o poner a disposición de terceros programas informáticos sin licencia y no autorizados por la empresa o cualquier tipo de obra/material sujetos a derechos de propiedad intelectual e industrial en perjuicio de terceros, cuando no se disponga de la previa autorización.

9. Cuando se **abandone el puesto de trabajo**, ya sea temporalmente o por terminar su jornada laboral, el usuario como responsable del mismo, deberá dejar el puesto de manera que sea imposible la visualización de los datos protegidos. Esto podrá realizarse a través de la desconexión de los equipos informáticos o mediante un protector de pantalla. La reanudación del trabajo sólo será posible mediante la introducción de su contraseña correspondiente.

10. Todo el personal, cuando **utilice impresoras, fotocopiadoras y fax**, deberá procurar que en la bandeja de salida no quede ningún documento que contengan datos personales. La información contenida en las bandejas de salida que no pertenezcan a un trabajador, es confidencial, y destinadas únicamente a la persona a quien han sido enviados.

11. Los **terminales informáticos** desde donde se acceden a los datos de carácter personal, tendrán una **configuración fija** en sus aplicaciones y sistemas operativos que **sólo podrán ser cambiadas por el personal expresamente autorizado**. Está prohibido el uso de los sistemas informáticos para fines privados. Queda expresamente prohibido la realización de copias de ningún tipo salvo autorización expresa del Responsable de protección de datos o en su caso, del Encargado departamental de protección de datos, así como la utilización de cualquier tipo de soporte informático (tarjetas de memoria, disquetes, cds, cintas, pendrives, u otros) para grabar datos de carácter personal.

En el supuesto de que se **utilicen sistemas informáticos portátiles** propiedad de la empresa (ordenadores portátiles, teléfonos móviles, PDA´s, etc), el trabajador deberá respetar y reforzar las medidas de seguridad de custodia y protección de los dispositivos cuando se encuentre fuera de las instalaciones de la empresa.

12. El tratamiento de la **documentación en soporte papel** que contenga datos personales, debe ser utilizada con la debida diligencia y tomando las medidas de seguridad idóneas para impedir su visualización o acceso por parte de personas no autorizadas.

13. Toda la documentación, debe ser **custodiada y archivada** de manera que no sea accesible por personas no autorizadas. A tal efecto, se utilizarán los dispositivos de almacenamiento y custodia (armarios y cajones) facilitados por la empresa, no dejando fuera de los mismos los soportes objeto de protección, especialmente cuando el trabajador se encuentre ausente de su lugar de trabajo.

14. **No está permitido tirar documentos y papeles** que contengan datos personales, **sin adoptar las medidas necesarias** que impidan su posterior visualización. Asimismo queda prohibida su reutilización. En caso de destrucción, se utilizaran los mecanismos que la entidad ha habilitado para dicho fin, en caso contrario se realizará manualmente tomando las precauciones descritas.

15. Todo documento que contenga datos de carácter personal, deberá estar **debidamente identificado**, permitiendo la identificación del tipo de información que contiene y los datos de los afectados por el tratamiento de datos, de manera que posibilite al ejercicio de los derechos de acceso, rectificación, cancelación y oposición y de aquellos derechos reconocidos por el nuevo reglamento europeo cuando resulte de aplicación.

16. Queda totalmente **prohibida la extracción**, fuera de las instalaciones de la entidad, de documentos que contengan datos personales de los que es responsable la entidad sin la autorización del Responsable de protección de datos y/o, en su caso, del Encargado departamental de protección de datos, que en todo caso le indicará las medidas de seguridad a adoptar para su salida.
17. El **incumplimiento** de cualquiera de las obligaciones que afectan a los usuarios contenidas en la presente circular, comportará las **consecuencias jurídicas y laborales** que pudieran derivarse frente al trabajador, o cualquier tercero afectado como consecuencia del incumplimiento.

Nombre y apellidos, fecha y firma del trabajador.

ANEXO 7. POLÍTICA DE CONTRASEÑAS

Política de contraseñas

1. *Salvaguarda y protección de las contraseñas personales*

Cada usuario será responsable de la confidencialidad de su contraseña. En caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá avisar al Responsable del Protección de Datos o, en su caso, al Encargado departamental de protección de datos.

Las contraseñas se gestionarán mediante el mecanismo que se determina en el punto 3. Este mecanismo de asignación y distribución de contraseñas deberá garantizar la confidencialidad de las mismas. Recomendamos que cada tres (3) meses se realicen cambios en las contraseñas en aquellos equipos que tengan información sensible, pudiendo irse a seis meses (6) en los demás equipos. Como mínimo deberá hacerse un cambio anual de las mismas.

Mientras estén vigentes, las contraseñas se deberán guardar de forma ininteligible.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

2. *Alcance*

El estándar descrito en este documento es de aplicación para toda aquella generación de contraseñas utilizadas en las plataformas tecnológicas de LUCAS BARRIENTOS RUBIO y tiene como objetivo establecer los criterios para la generación de contraseñas fuertes y seguras, de tal forma que no puedan ser comprometidas fácilmente mediante ataques basados en diccionario u otro tipo de técnicas.

3. *Funcionamiento*

4.

5.

La generación de las contraseñas de los trabajadores será siempre diferente y aleatoria.

Las contraseñas generadas no deberán ser deducibles mediante ataques basados en diccionario o mediante técnicas de “fuerza bruta”. A continuación se enuncian las características que se deberían cumplir para la generación de contraseñas seguras y así prevenir este tipo de ataques:

Concepto	Valor
Contraseñas en blanco o nulas.	No permitido
Longitud mínima.	8
Longitud máxima.	16
Permitir caracteres alfabéticos.	Si
Número mínimo de mayúsculas.	2
Número mínimo de caracteres alfabéticos.	3
Permitir caracteres numéricos.	Sí
Número mínimo de caracteres numéricos.	1

Existirán mecanismos que permitan a un trabajador el cambio de contraseña cuando éste lo considere necesario. Los mecanismos de cambio de contraseña (a petición del trabajador o porque el sistema o aplicación le fuerce al cambio) cumplirán las siguientes funcionalidades:

- Las contraseñas no se visualizarán en pantalla durante la introducción de las mismas,
- Se pedirá la contraseña antigua antes de continuar con el mecanismo de cambio de contraseña,
- Se pedirá confirmación de la nueva contraseña antes de proceder al cambio (para evitar posibles errores de escritura),
- No se permitirá la reutilización de algunas de las dos (2) últimas contraseñas que el colaborador haya utilizado,
- Se verificará la correcta longitud y sintaxis de la nueva contraseña antes de proceder al cambio.

Se deberán observar los siguientes requerimientos de cambio forzoso y de unicidad:

Concepto	Valor
Número de días para que la contraseña expire(dependerá).	90 días naturales
Generación de contraseñas únicas cada vez que éstas sean renovadas.	Sí
Número mínimo de contraseñas almacenadas para comparación de unicidad.	3
La primera contraseña asignada a una cuenta de usuario debe ser aleatoria y el sistema debe solicitar su cambio inmediato en su primer ingreso.	Sí
Número de intentos fallidos antes que la cuenta sea bloqueada o suspendida.	4
Establecer en 30 minutos la duración del bloqueo o necesidad de avisar al administrador para el desbloqueo.	Sí

Se establecerán procedimientos de generación, almacenamiento, gestión y cambio de las contraseñas de las cuentas de administración y de las cuentas con acceso automático a los sistemas. Estos procedimientos deberán garantizar la confidencialidad, integridad y disponibilidad de estas contraseñas y deben dejar evidencias de su cumplimiento.

Entre las características que deben cumplir las contraseñas en su conformación para evitar el uso de palabras contenidas en diccionarios, también se encuentran los siguientes valores:

Concepto	Valor
Lista de exclusión	• La cuenta del empleado o parte del mismo. • La cuenta del empleado en orden inverso. • El nombre y apellidos. • DNI del empleado. • Fecha de nacimiento. • Número de nómina. • Nombre completo o parcial de la empresa. • Las dos contraseñas anteriores

4. *Ejemplos:*

✓ *Contraseñas válidas*

Se recomienda construir contraseñas que puedan ser recordadas con facilidad por el usuario pero difícil de adivinar por un tercero, cumpliendo a su vez con lo indicado en este estándar:

- Iniciales de una frase conocida combinada con números: no por mucho madrugar amanece más temprano: npmmamt9.
- En una palabra intercalar letras y números: contraseña = contr9sen3.
- Palabras ficticias que recuerdan a palabra reales combinadas con números: arena=orena86, playa=blaya41.

☒ *Contraseñas no válidas y/o no recomendadas*

- 1234567 ➔(solo números).
- silviagusm ➔(nombre completo o parcial, solo letras).
- 14041978 ➔ (fecha de nacimiento: 14-04-1978, solo números).
- 2AConsulting ➔(nombre de la empresa, solo letras).
- 2ACons ➔(nombre parcial de la empresa, sólo letras).
- datos ➔ (menos de 7 caracteres).

Nombre y apellidos, fecha y firma del trabajador.

ANEXO 8. PROTOCOLO DE ACTUACIÓN EN CASO DE VIOLACIÓN DE SEGURIDAD

Protocolo de actuación en caso de violación de seguridad

A la luz del nuevo Reglamento Europeo de Protección de Datos (en adelante, RGPD) los pasos a seguir en caso de violación de seguridad en los datos personales, son:

1. El **trabajador que detecte una violación de seguridad**, deberá **notificarlo** al Responsable del Protección de Datos o, en su caso, Encargado departamental de protección de datos tan pronto como tenga conocimiento de la misma.

   En el supuesto que la notificación se haya efectuado al encargado departamental de protección de datos, éste deberá comunicar la violación de seguridad al Responsable del Protección de Datos con la mayor brevedad posible.

2. El **medio o la forma de notificación** tanto al Responsable del Protección de Datos**,** cuando proceda, como al Encargado departamental de protección de datos se acordará de forma interna en la organización, pudiendo ser mediante llamada telefónica o correo electrónico habilitado a tal efecto.

3. Recibida la comunicación, el Responsable del Protección de Datos **deberá ponerse en contacto inmediatamente con** 2AConsulting proporcionándole los datos que sean necesarios (como mínimo, usuario que notificó la violación de seguridad, fecha y hora en que se detectó y descripción de los hechos) para que conjuntamente puedan efectuar un **análisis sobre el riesgo** que pueda entrañar la violación de seguridad. (Comunicarlo a { HYPERLINK "mailto:legal@dobleaconsulting.es" })

4. Si del análisis se concluye que la violación supone un **riesgo** para los derechos y libertades de las personas físicas titulares, dará pie a su **comunicación** en nombre de LUCAS BARRIENTOS RUBIO a la Autoridad de Control correspondiente, siendo en el caso español, la **AEPD.**

5. Desde el momento en que se tenga constancia del alcance de la violación de la seguridad, no podrá transcurrir más de **72 horas** sin que se notifique a la Agencia Española de Protección de Datos, siguiendo los requisitos formales dictados por el RGPD.

6. Procederá igualmente **notificar a los titulares afectados** cuando sea posible que la violación de seguridad entrañe un **alto riesgo** para sus derechos y libertades a menos de que LUCAS BARRIENTOS RUBIO hubiera adoptado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad (como, por ejemplo, cifrado de datos), haya tomado con posterioridad a la violación de seguridad medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice o cuando la notificación suponga un esfuerzo desproporcionado (en este caso, podrá sustituirse por medidas alternativas como puede ser una comunicación pública).

   Previa consulta a 2AConsulting, esta notificación será efectuada por LUCAS BARRIENTOS RUBIO pudiendo utilizar un modelo que, a tal efecto, 2AConsulting le facilitará.

7. **Toda violación de seguridad**, independientemente de que sea comunicada a la autoridad de control y,

en su caso, notificada a los interesados, **deberá registrarse especificando al menos la siguiente información:**

- ✓ Tipo y descripción detallada de la incidencia,
- ✓ Momento en que se ha producido y/o detectado,
- ✓ Persona que realiza la notificación, a quién se le comunica,
- ✓ Efectos que se derivan de la misma,
- ✓ Medidas correctoras aplicadas.

El documento de registro de la violación de seguridad lo generará 2AConsulting y lo pondrá a disposición de LUCAS BARRIENTOS RUBIO .

Esta información permitirá a la Autoridad de Control verificar el cumplimiento de lo dispuesto en el RGPD.

Nombre y apellidos, fecha y firma del trabajador.

ANEXO 9. CLÁUSULA DE CORREO ELECTRÓNICO

Cláusula de correo electrónico. Formato tabla recomendado por la AEPD

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS CONFORME EL NUEVO REGLAMENTO EUROPEO	
RESPONSABLE	LUCAS BARRIENTOS RUBIO { HYPERLINK "mailto:email@email.com" }
FINALIDAD PRINCIPAL	Mantener relaciones profesionales y/o comerciales Prestar el servicio contratado
LEGITIMACIÓN	Consentimiento del interesado Interés legítimo Ejecución de un contrato
DESTINATARIOS	No se cederán datos a terceros, salvo autorización expresa u obligación legal (SI SE DECIERAN DATOS A OTRAS EMPRESAS QUE NO FUERAN ENCARGADOS DE TRATAMIENTO, SE DEBE ESPECIFICAR)
DERECHOS DE LOS TITULARES	Acceder, rectificar y suprimir los datos, portabilidad de los datos, limitación u oposición a su tratamiento, derecho a no ser objeto de decisiones automatizadas, así como a obtener información clara y transparente sobre el tratamiento de sus datos
INFORMACIÓN ADICIONAL	Puede consultar la información adicional y detallada sobre nuestra Política de Privacidad en { HYPERLINK "https://www.grupoadaptalia.es/%20" }
CONFIDENCIALIDAD	Si Ud. no es el destinatario y recibe este mail/fax por error, rogamos se ponga en contacto con nosotros y destruya de inmediato el mail/fax por error recibido con todos sus documentos adjuntos sin leerlos ni hacer ningún uso de los datos que en ellos figuren, ateniéndose a las consecuencias que de un uso indebido de dichos datos puedan derivarse

ANEXO 10. AVISO LEGAL

Aviso Legal

TITULAR DEL SITIO WEB		
DENOMINACIÓN SOCIAL: LUCAS BARRIENTOS RUBIO		
CIF: 32667460P		
DOMICILIO SOCIAL: AVDA. DE PARIS, Nº 31, 10005, CÁCERES (CÁCERES)		
CONTACTO:	Teléfono: 647 908 541	
	Email:{ HYPERLINK "mailto:privacy@unusualwonder.com" }	
DATOS DE INSCRIPCIÓN EN EL REGISTRO MERCANTIL:	Tomo:	Libro:
	Folio:	Secc.:
	Hoja:	
CÓDIGOS DE CONDUCTA:		

ANEXO 11. PRIMERA CAPA POLÍTICA DE PRIVACIDAD (WEB)

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS	
RESPONSABLE	LUCAS BARRIENTOS RUBIO margomrom@hotmail.com
FINALIDAD PRINCIPAL	Facilitar la información solicitada Resolver la consulta planteada Mantener relaciones profesionales y/o comerciales Gestionar la suscripción Gestionar los procesos de selección de personal Gestionar el envío de newsletter … (SEÑALAR LAS FINALIDADES QUE PROCEDAN)
LEGITIMACIÓN	Consentimiento del interesado
DESTINATARIOS	No se cederán datos a terceros, salvo autorización expresa u obligación legal (SI SE DECIERAN DATOS A OTRAS EMPRESAS QUE NO FUERAN ENCARGADOS DE TRATAMIENTO, SE DEBE ESPECIFICAR)
DERECHOS	Acceder, rectificar y suprimir los datos, portabilidad de los datos, limitación u oposición a su tratamiento, transparencia y derecho a no ser objeto de decisiones automatizadas.
INFORMACIÓN ADICIONAL	Puede consultar la información adicional y detallada sobre nuestra Política de Privacidad en { HYPERLINK } *(SE REDIRIGE A LA POLITICA DE PRIVACIDAD INTEGRA, SEGUNDA CAPA)*

☐ He leído y acepto la Política de Privacidad (ESTA CASILLA DEBE MARCARLA NECESARIAMENTE EL INTERESADO ANTES DE ENVIAR SUS DATOS)

☐ Autorizo al envío de comunicaciones electrónicas informativas relativas a las actividades, productos o servicios por correo postal, fax, correo electrónico o cualquier otro medio electrónico equivalente (ESTA CASILLA ES OPCIONAL POR EL INTERESADO)

ANEXO 12. SEGUNDA CAPA POLÍTICA DE PRIVACIDAD (WEB)

Política de Privacidad

Siguiendo los principios de licitud, lealtad y transparencia, ponemos a su disposición la presente Política de Privacidad.

¿Quién es el Responsable del tratamiento de sus datos?

LUCAS BARRIENTOS RUBIO

CIF: 32667460P

DOMICILIO SOCIAL: AVDA. DE PARIS, Nº 31, 10005, CÁCERES (CÁCERES)

Email: { HYPERLINK "mailto:email@email.com" }

Teléfono: 647 908 541

¿Con qué finalidad tratamos sus datos personales?

En LUCAS BARRIENTOS RUBIO tratamos la información que nos facilita con la finalidad de gestionar la relación contractual que nos une, gestionar el envío de la información que nos solicita, facilitar a los interesados ofertas de nuestros servicios y/o productos de su interés y/o gestionar su candidatura.

¿Por cuánto tiempo conservaremos sus datos personales?

Sus datos, serán conservados el tiempo mínimo necesario para la correcta prestación del servicio ofrecido así como para atender las responsabilidades que se pudieran derivar del mismo y de cualquier otra exigencia legal.

¿Cuál es la legitimación para el tratamiento de sus datos?

La base legal para el tratamiento de sus datos personales puede ser la ejecución de una relación contractual potencial y/o suscrita, el interés legítimo, la habilitación legal y/o el consentimiento del propio interesado. Los datos que le solicitamos son adecuados, pertinentes y estrictamente necesarios y en ningún caso está obligado a facilitárnoslos, pero su no comunicación podrá afectar a la finalidad del servicio o la imposibilidad de prestarlo.

¿A qué destinatarios se comunicarán sus datos?

LUCAS BARRIENTOS RUBIO no comunicará sus datos a ningún tercero, salvo su consentimiento expreso u obligación legal.

¿Cuáles son sus derechos cuando nos facilita sus datos?

Los derechos de protección de datos de los que son titulares los interesados son:

- Derecho a solicitar el acceso a los datos personales relativos al interesado
- Derecho de rectificación o supresión
- Derecho de oposición
- Derecho a solicitar la limitación de su tratamiento
- Derecho a la portabilidad de los datos

Los titulares de los datos personales obtenidos, podrán ejercer sus derechos de protección de datos personales dirigiendo una comunicación por escrito al domicilio social de LUCAS BARRIENTOS RUBIO o al

correo electrónico habilitado a tal efecto, { HYPERLINK "mailto:email@email.com" }, incluyendo en ambos casos fotocopia de su DNI u otro documento de identificación equivalente.

Modelos, formularios y más información disponible sobre sus derechos en la página web de la autoridad de control nacional, Agencia Española de Protección de Datos, en adelante, AEPD, { HYPERLINK "http://www.agpd.es" }

¿Puedo retirar el consentimiento?

Usted tiene la posibilidad y el derecho a retirar el consentimiento para cualquiera finalidad específica otorgada en su momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.

¿Dónde puedo reclamar en caso de que considere que no se tratan mis datos correctamente?

Si algún interesado considera que sus datos no son tratados correctamente por LUCAS BARRIENTOS RUBIO puede dirigir sus reclamaciones al correo { HYPERLINK "mailto:email@email.com" } o a la autoridad de protección de datos que corresponda, siendo la AEPD la indicada en el territorio nacional, { HYPERLINK "http://www.agpd.es" }

Seguridad y actualización de sus datos personales

Con el objetivo de salvaguardar la seguridad de sus datos personales, le informamos que LUCAS BARRIENTOS RUBIO ha adoptado todas las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos personales suministrados. Todo ello para evitar su alteración, pérdida, y/o tratamientos o accesos no autorizados, tal como exige la normativa, si bien la seguridad absoluta no existe.

Es importante que, para que podamos mantener sus datos personales actualizados, nos informe siempre que se produzca una modificación de los mismos.

Confidencialidad

LUCAS BARRIENTOS RUBIO le informa que sus datos serán tratados con el máximo celo y confidencialidad por todo el personal que intervenga en cualquiera de las fases del tratamiento. No cederemos ni comunicaremos a ningún tercero sus datos, excepto en los casos legalmente previstos, o salvo que el interesado nos hubiera autorizado expresamente.

ANEXO 13. AVISO DE COOKIES

Aviso de Cookies (1ª capa o banner de cookies)

Esta web utiliza cookies propias y de terceros (si fuera el caso) para analizar su navegación y ofrecerle un servicio más personalizado y publicidad (si fuera el caso) acorde a sus intereses. Continuar navegando implica la aceptación de nuestra Política de Cookies (link enlazando con la 2ª capa).

ANEXO 14. POLÍTICA DE COOKIES

Política de Cookies

1. *¿Qué son las cookies?*

La Web de LUCAS BARRIENTOS RUBIO (en adelante la Web) utiliza Cookies. Las Cookies son ficheros enviados a un navegador por medio de un servidor web para registrar las actividades del Usuario en una web determinada. La primera finalidad de las Cookies es la de facilitar al usuario un acceso más rápido a los servicios seleccionados. Además, las Cookies personalizan los servicios que ofrece la Web, facilitando y ofreciendo a cada usuario información que es de su interés o que puede ser de su interés, en atención al uso que realiza de los Servicios.

La Web utiliza Cookies para personalizar y facilitar al máximo la navegación del usuario. Las Cookies se asocian únicamente a un usuario anónimo y su ordenador y no proporcionan referencias que permitan deducir datos personales del usuario. El usuario podrá configurar su navegador para que notifique y rechace la instalación las Cookies enviadas por la Web, sin que ello perjudique la posibilidad del usuario de acceder a los contenidos de dicha web. Sin embargo, le hacemos notar que, en todo caso, la calidad de funcionamiento de la página Web puede disminuir.

Los usuarios registrados, que se registren o que hayan iniciado sesión, podrán beneficiarse de unos servicios más personalizados y orientados a su perfil, gracias a la combinación de los datos almacenados en las cookies con los datos personales utilizados en el momento de su registro. Dichos usuarios autorizan expresamente el uso de esta información con la finalidad indicada, sin perjuicio de su derecho a rechazar o deshabilitar el uso de cookies.

Asimismo, la Web podrá saber todos los servicios solicitados por los usuarios, de forma que podrán facilitar u ofrecer información adecuada a los gustos y preferencias de cada usuario.

2. *¿Qué tipos de cookies existen?*

Las Cookies, en función de su Permanencia, pueden dividirse en:

- "Cookies de sesión": Las primeras expiran cuando el usuario cierra el navegador.

- "Cookies persistentes". Las segundas expiran en función de cuando se cumpla el objetivo para el que sirven (por ejemplo, para que el usuario se mantenga identificado en los Servicios) o bien cuando se borran manualmente.

Adicionalmente, en función de su Objetivo, las Cookies pueden clasificarse de la siguiente forma:

- *Cookies* de rendimiento: Este tipo de Cookie recuerda sus preferencias para las herramientas que se encuentran en los servicios, por lo que no tiene que volver a configurar el servicio cada vez que usted visita. A modo de ejemplo, en esta tipología se incluyen:

    - Ajustes de volumen de reproductores de vídeo o sonido.

    - Las velocidades de transmisión de vídeo que sean compatibles con su navegador.

- *Cookies* de geo-localización*:* Estas Cookies son utilizadas para averiguar en qué país se encuentra cuando se solicita un servicio. Esta Cookie es totalmente anónima, y sólo se utiliza para ayudar a orientar el contenido a su ubicación.

- *Cookies* de registro: Las Cookies de registro se generan una vez que el usuario se ha registrado o posteriormente ha abierto su sesión, y se utilizan para identificarle en los servicios con los siguientes objetivos:

    - Mantener al usuario identificado de forma que, si cierra un servicio, el navegador o el ordenador y en otro momento u otro día vuelve a entrar en dicho servicio, seguirá identificado, facilitando así su navegación sin tener que volver a identificarse. Esta funcionalidad se puede suprimir si el usuario pulsa la funcionalidad "cerrar sesión", de forma que esta Cookie se elimina y la próxima vez que entre en el servicio el usuario tendrá que iniciar sesión para estar identificado.

    - Comprobar si el usuario está autorizado para acceder a ciertos servicios, por ejemplo, para participar en un concurso.

- *Cookies* analíticas: Cada vez que un Usuario visita un servicio, una herramienta de un proveedor externo genera una Cookie analítica en el ordenador del usuario. Esta Cookie que sólo se genera en la visita, servirá en próximas visitas a los Servicios de la Web para identificar de forma anónima al visitante. Los objetivos principales que se persiguen son:

    - Permitir la identificación anónima de los usuarios navegantes a través de la "*Cookie*" (identifica navegadores y dispositivos, no personas) y por lo tanto la contabilización aproximada del número de visitantes y su tendencia en el tiempo.

    - Identificar de forma anónima los contenidos más visitados y por lo tanto más atractivos para los usuarios.

    - Saber si el usuario que está accediendo es nuevo o repite visita.

    - Importante: Salvo que el usuario decida registrarse en un servicio de la Web, la "*Cookie*" nunca irá asociada a ningún dato de carácter personal que pueda identificarle. Dichas Cookies sólo serán utilizadas con propósitos estadísticos que ayuden a la optimización de la experiencia de los Usuarios en el sitio.

- *Cookies* de publicidad comportamental: Este tipo de "*Cookies*" permite ampliar la información de los anuncios mostrados a cada usuario anónimo en los Servicios de la Web. Entre otros, se almacena la duración o frecuencia de visualización de posiciones publicitarias, la interacción con las mismas, o los patrones de navegación y/o compartimientos del usuario ya que ayudan a conformar un perfil de interés publicitario. De este modo, permiten ofrecer publicidad afín a los intereses del usuario.

- *Cookies* publicitarias de terceros: Además de la publicidad gestionada por la Web en sus Servicios, la Web ofrece a sus anunciantes la opción de servir anuncios a través de terceros ("AdServers"). De este modo, estos terceros pueden almacenar *Cookies* enviadas desde los Servicios de la Web procedentes de los navegadores de los Usuarios, así como acceder a los datos que en ellas se guardan.

    - Weborama: { HYPERLINK "http://www.weborama.com/e-privacy/our-commitment/" }

3. *¿Qué cookies utilizamos?*

⚠ El informático debe identificar qué tipos de cookies de entre las que aparecen en la pregunta 2. "¿Qué tipo de cookies existen?" emplea la página web distinguiendo a su vez si son propias o de terceros: (Eliminar el recuadro una vez identificadas las cookies que utilizan)

Las cookies que utilizamos en nuestra página web son:

- **Propias:** Son aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario.

  (Las más comunes son:
  - Cookies de sesión)

- **De terceros:** Son aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies.
-

  (Las más comunes son:

  - Google Analytics:
  { HYPERLINK "https://support.google.com/analytics/answer/6004245?hl=es" }

  - ComScore:

  { HYPERLINK "http://www.comscore.com/esl/Sobre-comScore/Politica-de-%20%20%20privacidad?cs_edgescape_cc=ES" }

  - Real Media:

  { HYPERLINK "http://www.realmedia.com/en%20us/pages/privacy_policy.html" })

4. *¿Cómo deshabilitar las Cookies?*

Normalmente es posible dejar de aceptar las Cookies del navegador, o dejar de aceptar las Cookies de un Servicio en particular.

Todos los navegadores modernos permiten cambiar la configuración de Cookies. Estos ajustes normalmente se encuentran en las ¨opciones¨ o ¨preferencias¨ del menú de su navegador. Asimismo, puede configurar su navegador o su gestor de correo electrónico, así como instalar complementos gratuitos para evitar que se descarguen los Web *Bugs* al abrir un email.

La Web ofrece orientación al Usuario sobre los pasos para acceder al menú de configuración de las *cookies* y, en su caso, de la navegación privada en cada uno de los navegadores principales:

- Internet Explorer: Herramientas - > Opciones de Internet - > Privacidad - > Configuración.
- Para más información, puede consultar el soporte de Microsoft o la Ayuda del navegador.

- Firefox: Herramientas - > Opciones - > Privacidad - > Historial - > Configuración personalizada.

- Chrome: Configuración - > Mostrar opciones avanzadas - > Privacidad - > Configuración de contenido.

- Safari: Preferencias - > Seguridad.
- Para más información, puede consultar el soporte de Apple o la Ayuda del navegador.

5. *¿Se pueden producir modificaciones de la Política de Cookies?*

La Web puede modificar esta Política de Cookies en función de las exigencias legislativas, reglamentarias, o con la finalidad de adaptar dicha política a las instrucciones dictadas por la Agencia Española de Protección de Datos, por ello se aconseja a los usuarios que la visiten periódicamente.

Cuando se produzcan cambios significativos en esta Política de *Cookies*, se comunicarán a los usuarios bien mediante la web o a través de correo electrónico a los usuarios registrados.

Nombre de archivo: Guia_Legal.docx
Carpeta: /Users/danielcastanera/Library/Containers/com.microsoft.Word/Data/Documents
Plantilla: /Users/danielcastanera/Library/Group Containers/UBF8T346G9.Office/User Content.localized/Templates.localized/Normal.dotm
Título:
Asunto:
Autor: Mireia
Palabras clave:
Comentarios:
Fecha de creación: 16/10/18 15:15:00
Cambio número: 2
Guardado el: 16/10/18 15:15:00
Guardado por: Usuario de Microsoft Office
Tiempo de edición: 1 minuto
Impreso el: 16/10/18 15:15:00
Ultima impresión completa
Número de páginas: 40
Número de palabras: 11.778 (aprox.)
Número de caracteres: 64.783 (aprox.)