1. DOCUMENTO DE INFORMACIÓN Y COMPROMISO DE CONFIDENCIALIDAD

Explicación:

Este documento deberá ser firmado por **todos los empleados** independientemente de que accedan y/o traten datos de carácter personal.

La **firma de este documento prueba** que:

- La empresa ha cumplido con el deber de informar al trabajador sobre la finalidad del tratamiento de sus datos, las personas o entidades a las que podrían cederse los mismos, etc.
- El trabajador conoce su deber de guardar la confidencialidad o el secreto de los datos de carácter personal que conozca con ocasión del desempeño de sus funciones.

En el supuesto que se efectúe un tratamiento de **datos biométricos** (huella dactilar, imagen facial, reconocimiento de iris, etc.) de los empleados, contacten directamente con el Departamento Legal de GRUPO ADAPTALIA a través del siguiente correo electrónico: **legal@grupoadaptalia.es**

Documento de información y compromiso de confidencialidad

En Madrid, el 13 de Noviembre de 2023

De conformidad con la normativa de protección de datos, le informamos que sus datos personales pasarán a formar parte de un tratamiento cuyo **responsable** es **Artigot Catering, S.L.**, con la **finalidad** de cumplir con todas aquellas obligaciones derivadas de la relación laboral, tales como la elaboración y gestión de nóminas, cumplimiento de obligaciones sociales y tributarias, deberes en materia de prevención de riesgos laborales, etc.

La **base de legitimación** para el tratamiento de sus datos es la ejecución del contrato laboral.

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.
- Entidades aseguradoras para la tramitación de seguros.
- Empresas auditoras y certificadoras que para, la aprobación de las cuentas anuales o la verificación del cumplimiento de alguna normativa, puedan acceder a datos de carácter personal.
- Administración pública para la solicitud de subvenciones.
- Entidades, clientes y proveedores 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 a la mayor brevedad posible cualquier cambio que se produzca sobre los mismos.

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 **Artigot Catering, S.L.**.

Igualmente queda informado expresamente que las instalaciones de la entidad están videovigiladas con la finalidad de salvaguardar la **seguridad** de las instalaciones, bienes y personas como de **control laboral**, lo cual se informa también mediante los distintos carteles informativos distribuidos por las distintas ubicaciones de las instalaciones.

Puede **ejercer sus derechos** de acceso, rectificación, supresión, oposición, limitación al tratamiento, portabilidad y a no ser objeto de decisiones individualizadas, cuando procedan, dirigiéndose al responsable de recursos humanos.

Si considera que sus datos no son tratados correctamente por **Artigot Catering, S.L.** o que las solicitudes de ejercicio de derechos no han sido atendidas de forma satisfactoria, tiene derecho a presentar una reclamación ante la Autoridad de Control, siendo la Agencia Española de Protección de Datos (AEPD), la indicada en el territorio nacional www.aepd.es.

Nombre y apellidos del empleado:	
Firma:	

2. FUNCIONES Y OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL

Explicación:

Este documento deberá ser firmado **sólo por los empleados que tengan acceso a datos de carácter 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, independientemente de que lo haga a través de medios automatizados (ordenadores, *pen drive*, teléfonos móviles de empresa, etc) o no automatizados (soporte papel).

En el documento se recoge también la **facultad del empresario** de acceder a los contenidos derivados del uso de medios digitales por lo empleados a los solos efectos de **controlar el cumplimiento de las obligaciones laborales o estatutarias** y de garantizar la integridad de dichos dispositivos, pudiendo de esta forma:

- Monitorizar el uso del correo electrónico y de Internet.
- Conocer las contraseñas de los empleados.

La facultad de "control laboral" del empresario está prevista en el artículo 20.3 del Estatuto de los Trabajadores y en el artículo 87 LOPDGDD. Podrá recurrirse a ella siempre y cuando las medidas sean proporcionadas y se haya informado previamente de las mismas al trabajador.

Este documento deberá consultarse con los representantes sindicales, caso que los hubiese.

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

En Madrid, el 13 de Noviembre de 2023

Conforme a la normativa sobre protección de datos, todo el personal debe conocer las normas de seguridad que afectan 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 de los mismos.

1. El personal solamente podrá **acceder** a los **tratamientos de datos de carácter personal** a los que esté **autorizado** por **Artigot Catering, S.L.** 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 de los soportes informáticos, aplicaciones, programas, correo electrónico corporativo, Internet y, en general, cualquier recurso técnico e informático facilitado por la entidad como herramienta de trabajo,** es estrictamente profesional no permitiéndose ningún uso personal excepto en aquellos casos en los que se cuente con el consentimiento expreso del empleador.

   Al respecto le informamos que el empleador podrá **acceder a los contenidos derivados del uso de los dispositivos digitale**s a los solos efectos de controlar **el cumplimiento de las obligaciones laborales y garantizar su integridad,** siempre con el debido respeto a la intimidad del trabajador.

   Asimismo, se informa al trabajador que, una vez terminada la relación laboral, el empleador podrá consultar la documentación e información contenida en el soporte informático proporcionado por la entidad empleadora, con el objetivo de poder continuar con los trabajos iniciados por dicho trabajador, complementar información requerida, así como, comprobar el buen uso de dicho soporte informático y de la información contenida en el mismo.

4. Todo el personal está obligado a **comunicar** al Data Security Protection Officer (o responsable interno de protección de datos, en lo sucesivo <<DSPO>>) y/o, en su caso, Data Security Protection Partner (o encargado departamental de protección de datos, en lo sucesivo <<DSPP>>) cualquier **solicitud de ejercicio de derechos** de acceso, rectificación, supresión, portabilidad de los datos, limitación u oposición a su tratamiento y derecho a no ser objeto de decisiones automatizadas.

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 deberán ser borrados o destruidos o incorporados a carpetas o archivos de la entidad, cumplida la finalidad que motivó 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, sistemas P2P,etc) 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/materiales 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 destinada 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.** Queda expresamente prohibido la realización de copias de ningún tipo salvo autorización expresa del DSPO o en su caso, del DSPP, 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, pudiendo ser a través de su cifrado.

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 organización, 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 utilizarán los mecanismos que la entidad ha habilitado para dicho fin (máquinas destructoras o papeleras específicas para su retirada por la empresa destructora). En caso contrario, se realizarán manualmente tomando las debidas precauciones.

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, supresión,

portabilidad de los datos, limitación u oposición a su tratamiento, y derecho a no ser objeto de decisiones automatizadas.

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 DSPO y/o, en su caso, del DSPP, 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 del empleado:	
Firma:	

3. POLÍTICA DE CONTRASEÑAS

Explicación:

La calidad de la contraseña es un factor importante a ser considerado, pues de ser adivinado o robado por una tercera persona ajena, podría causar problemas a la organización o sus recursos.

Por este motivo, a través de la siguiente Política de contraseñas, le ofrecemos unas **recomendaciones o líneas a seguir de cara a un mayor refuerzo en el establecimiento 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.

Política de contraseñas

En Madrid, el 13 de Noviembre de 2023

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 Data Security Protection Officer (o responsable interno de protección de datos, en lo sucesivo <<DSPO>>) o, en su caso, al Data Security Protection Partner (o encargado departamental de protección de datos, en lo sucesivo <<DSPP>>).

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 **Artigot Catering, S.L.** 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*

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 empleado 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.	**2**
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).
- Adaptalia → (nombre de la organización, solo letras).
- Grupoadapt → (nombre parcial de la organización, sólo letras).
- datos → (menos de 8 caracteres).

Nombre y apellidos del empleado:	
Firma:	

4. PROTOCOLO DE ACTUACIÓN EN CASO DE VIOLACIÓN DE SEGURIDAD

Explicación:

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.

Son **ejemplos típicos** de violación de seguridad la pérdida de un ordenador portátil, acceso no autorizado a la base de datos de una organización o el robo de información que contenga datos personales por un empleado que ha sido despedido.

En el supuesto de que la violación de seguridad entrañe un **riesgo para los derechos y libertades de los interesados**, la organización dispone de un **plazo de 72 horas** para **notificar** la violación de seguridad a la **AEPD**. Si supone un **alto riesgo para los derechos y libertades de los interesados**, deberá además **comunicarse a los interesados**.

El siguiente 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**.

Protocolo de actuación en caso de violación de seguridad

En Madrid, el 13 de Noviembre de 2023

De conformidad con la normativa sobre protección de datos, los pasos a seguir en caso de violación de seguridad en los datos personales son:

FASE 1: EMPLEADOS

1. El **trabajador que detecte una violación de seguridad**, deberá **notificarlo** al Data Security Protection Officer (o responsable interno de protección de datos, en adelante **<<DSPO>>**) o, en su caso, Data Security Protection Partner (o encargado departamental de protección de datos, en adelante **<<DSPP>>**) tan pronto como tenga conocimiento de la misma.

   En el supuesto de que la notificación se haya efectuado al DSPP, éste deberá comunicar la violación de seguridad al DSPO con la mayor brevedad posible.

2. **¿Qué se entiende por brecha de seguridad?**

   Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales. Esta puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente.

3. **¿Qué escenarios pueden considerarse brecha de seguridad?**

   Algunos ejemplos de brechas de seguridad en que el trabajador deberá comunicar inmediatamente al DSPO/DSPP son:

   - Pérdida/robo/hurto de dispositivos móviles.
   - Pérdida/robo/hurto de equipos informáticos.
   - Pérdida/robo/hurto de documentación en papel.
   - Pérdida de llaves de instalaciones o archivadores que almacenen datos.
   - Envío erróneo de correo electrónico a un tercero.
   - Envió de correos con copia visible a varios destinatarios sin relación entre sí.
   - Envío de un correo a un destinatario erróneo.
   - Infección de equipos con *ransomware* que cifre los archivos.
   - Recibir correos sospechosos con prácticas como *whaling* o *phishing*.
   - Conectarse en remoto sin haber activado la VPN.
   - Acceso no autorizado a instalaciones que almacenan datos.

- Acceso no autorizado a bases de datos.
- No cumplir con la política de mesas limpias o bloqueo de pantalla al abandonar el puesto de trabajo, provocando una visualización de una persona no autorizada.
- Revelación verbal a un tercero no autorizado.
- Publicación no intencionada de datos.
- Eliminación de documentos o soportes electrónicos sin garantizar su destrucción.
- Borrado o modificación accidental de datos.

Recordamos que la presente lista es ejemplificativa y no limitativa. Cualquier situación que el empleado detecte que podría afectar a la integridad, disponibilidad o confidencialidad de los datos, sería considerada una brecha de seguridad merecedora de ser reportada.

4. El **medio o la forma de notificación** tanto al **DSPP,** cuando proceda, como al **DSPO** se acordará de forma interna en **Artigot Catering, S.L.**, pudiendo ser mediante llamada telefónica o correo electrónico habilitado a tal efecto.

FASE 2: DSPO y/o DSPP

1. Recibida la comunicación, el **DSPO deberá ponerse en contacto inmediatamente con GRUPO ADAPTALIA** 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.

2. 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 **notificación** en nombre de **Artigot Catering, S.L.** a la Autoridad de Control correspondiente, siendo en el caso español, la **Agencia Española de Protección de Datos (en adelante, <<AEPD>>).**

3. 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 AEPD, siguiendo los requisitos formales dictados por el RGPD.

4. 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 que **Artigot Catering, S.L.** 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 GRUPO ADAPTALIA, esta notificación será efectuada por **Artigot Catering, S.L.** pudiendo utilizar un modelo que, a tal efecto, GRUPO ADAPTALIA le facilitará.

5. **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 **GRUPO ADAPTALIA** que lo pondrá a disposición de **Artigot Catering, S.L.** para su registro interno.

   Esta información permitirá a la Autoridad de Control verificar el cumplimiento de lo dispuesto en la normativa sobre protección de datos.

Nombre y apellidos del empleado:	
Firma:	

5. PROTOCOLO DE ACTUACIÓN EN CASO DE EJERCICIO DE DERECHOS:

La normativa sobre protección de datos reconoce derechos a los titulares de los datos de carácter personal: derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y a no ser objeto de decisiones individualizadas

El siguiente documento detalla el **procedimiento que debe seguir la organización cuando cualquier interesado ejerza alguno de estos derechos.**

La firma de este documento acredita que el **empleado está al tanto de dicho procedimiento**.

Protocolo de actuación en caso de ejercicio de derechos

En Madrid, el 13 de Noviembre de 2023

¿Qué derechos en materia de protección de Datos existen?

De acuerdo con la normativa de protección de datos, el espectro de derechos que cualquier persona puede ejercer ante las entidades que traten sus datos de carácter personal son:

- **Acceso**→ Derecho a obtener información sobre qué datos están tratando, para qué finalidad y si hay cesiones realizadas o previstas; así como a solicitar una copia de los datos que son objeto de tratamiento.
- **Rectificación**→ Derecho a pedir que se modifiquen aquellos datos que resulten ser inexactos o incompletos.
- **Supresión**→ Derecho a pedir que se eliminen o borren sus datos personales cuando ya no sean necesarios o se traten ilícitamente. Todo ello, siempre que no lo impida una obligación legal, o sea necesario para el ejercicio o defensa de reclamaciones
- **Oposición**→ Derecho a solicitar que no se lleve a cabo un determinado tratamiento de datos de carácter personal, siempre y cuando no prevalezcan motivos legítimos imperiosos o sea necesario para la formulación, el ejercicio o la defensa de reclamaciones.
- **Limitación del tratamiento**→ Derecho a solicitar que no se traten los datos mientras haya pedido la modificación de estos; el tratamiento sea ilícito pero en vez de solicitar que se supriman el interesado pide simplemente oponerse a su tratamiento; o cuando **Artigot Catering, S.L.** ya no necesita tratar sus datos pero son necesarios para el ejercicio o la defensa de reclamaciones.
- **Portabilidad de los datos**→ Derecho a pedir que se faciliten los datos a otra entidad, o a sí mismo, en un formato estructurado, de uso común y lectura mecánica. Dicha solicitud sólo se podrá realizar sobre datos cuyo tratamiento se efectúe por medios automatizados.
- **No ser objeto de decisiones automatizadas**→ Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente de forma similar.

Una vez que conocemos los derechos que puede ejercer cualquier interesado ante nuestra entidad, es necesario saber cuándo debe responderse:

- En el plazo máximo de 1 mes desde la recepción de la solicitud: si se actúa como Responsable de Tratamiento
- Sin dilación indebida y, en todo caso, según el plazo máximo establecido en el correspondiente contrato o acuerdo de tratamiento de datos: si se actúa en calidad de Encargado de Tratamiento.

Protocolo ejercicio de derechos

Para poder dar respuesta en tiempo y forma a cualquier ejercicio de derechos, es necesario señalar un procedimiento sencillo que permita conocer a cualquier empleado cómo actuar si llega a darse esta situación:

FASE 1: EMPLEADOS

Si cualquier empleado recibe un correo electrónico o una solicitud por cualquier otro medio que perciba como un ejercicio de derechos deberá remitirlo al Data Security Protection Officer (o responsable interno de protección de datos, en lo sucesivo <<DSPO>>) y/o, en su caso, Data Security Protection Partner (o encargado departamental de protección de datos, en lo sucesivo <<DSPP>>) para que éste se ponga en contacto con el DSPO.

FASE 2: DSPO y/o DSPP

1. En aquellos supuestos en que se reciba un ejercicio de derechos por **Artigot Catering, S.L.**, y la misma actúe en calidad de Encargado del Tratamiento, el DSPO deberá atender al procedimiento establecido en el correspondiente contrato o acuerdo de tratamiento de datos.
2. Para el resto de supuestos, aquellos en que **Artigot Catering, S.L.** actúe en calidad de Responsable del Tratamiento, el DSPO valorará las circunstancias y si cumple los requisitos de forma, en consecuencia, procederá a responder a tal solicitud dentro del plazo de 1 mes a contar desde la recepción de la solicitud.
3. Si no fuera posible acreditar la identidad del titular de los datos o existiesen dudas sobre la misma, se solicitará DNI o documento acreditativo equivalente para poder responder de forma adecuada.
4. En caso de duda, consultar con los expertos que ayudan en la materia o, en su caso, con el DPO para valorar las circunstancias concretas, y poder decidir si procedemos a contestar positivamente la solicitud o, en su caso, debemos darle una respuesta negativa al interesado.

De esta forma daremos respuesta de forma adecuada, evitando así sanciones por parte de las autoridades de control.

Nombre y apellidos del empleado:	
Firma:	

6. PROTOCOLO DE CONSERVACIÓN Y BORRADO DE DATOS DE CARÁCTER PERSONAL

Explicación:

Uno de los principios de la normativa sobre protección de datos es el de "**limitación del plazo de conservación**". Este principio implica que los datos deben ser mantenidos de forma que **se permita la identificación de los interesados durante no más tiempo del necesario para los fines para los cuales fueron recogidos**.

En consecuencia, el siguiente documento explica (i) **hasta cuánto tiempo deben conservarse los distintos tipos de datos personales** y, una vez llegado el plazo, (ii) **qué medidas de seguridad adoptar para proceder a su borrado y/o destrucción**.

La firma de este documento acreditaría que el **empleado está al tanto de dicho procedimiento.**

Al final del documento, encontrará **una tabla donde se recogen los periodos de conservación de la documentación que suele manejar una organización.** En el caso de que la organización no realice alguno de los tratamientos que aparecen en la tabla, **deberá eliminarlos**; igualmente, si la organización realiza otros tipos de tratamientos que no se encuentren en la tabla, **deberá añadirlos** junto con sus respectivos periodos de conservación.

Protocolo de conservación y borrado de datos personales

En Madrid, el 13 de Noviembre de 2023

1. Objeto

El presente protocolo tiene como finalidad la regulación del almacenamiento, conservación, bloqueo y destrucción de activos de información que contengan datos de carácter personal e información sensible, de los que **Artigot Catering, S.L.** sea Responsable o encargado del tratamiento.

Este se referirá a los activos de información, tanto automatizados como no automatizados, que sean generados o gestionados por **Artigot Catering, S.L.**.

El propósito de dicho protocolo no será otro que garantizar el conocimiento y disposición de toda la plantilla de **Artigot Catering, S.L.** de un procedimiento que asegure el correcto tratamiento y conservación de la documentación, no excediendo los periodos fijados en función tanto de las finalidades para las que se recogieron, como las obligaciones legales a las que pudiese estar sujeta la organización, así como la correcta supresión de estos.

2. Almacenamiento de información que contenga datos de carácter personal

Es necesario conservar la documentación en formato digital y físico durante el tiempo establecido. **Artigot Catering, S.L.** garantizará en todo momento que los datos de carácter personal almacenados dentro de los emplazamientos de la propia organización cumplen con los tres pilares fundamentales de la seguridad de la información: Integridad, disponibilidad y confidencialidad. Para aquellos tratamientos, operaciones o el simple almacenamiento datos de carácter personal que **Artigot Catering, S.L.** encomiende a un prestador de servicios, se garantizará mediante un contrato de encargo. Asimismo, el propio Responsable del tratamiento tiene la potestad de supervisar que dicho servicio cumple con todos los aspectos que establece la normativa de protección de datos, así como las medidas de seguridad adecuadas y la confidencialidad de estos

Artigot Catering, S.L. deberá identificar los activos de información relevantes para el ciclo de vida de la información y los datos y documentar su importancia. El ciclo de vida de la información debería incluir la creación, tratamiento, almacenamiento, transmisión, borrado y destrucción. Este inventario deberá ser preciso, estar actualizado, ser consistente y estar en consonancia con otros inventarios. Cada uno de estos activos deberán contar con un responsable (departamento, personal, dirección, etc), el cual designará las personas autorizadas para su utilización. Este responsable deberá:

- Asegurar que los activos son inventariados.
- Asegurar que los activos se clasifican y protejan debidamente.
- Definir y revisar periódicamente restricciones de acceso y clasificación de activos importantes.
- Asegurar el manejo adecuado para el borrado o destrucción del activo.

El personal de **Artigot Catering, S.L.** estará concienciado sobre los requisitos de seguridad que exige el uso aceptable de los activos de información. Asimismo, todos los empleados deberán devolver los activos de información de **Artigot Catering, S.L.** que estén en su poder al finalizar su empleo, contrato, acuerdo o tareas específicas.

La información deberá ser clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante la revelación o modificación no autorizadas. Respecto a la manipulación de la información, deberá contemplarse:

- Restricciones de acceso a los activos, con una política de contraseñas.
- Mantenimiento de un registro formal de receptores autorizados de los activos
- Protección de copias, sean temporales o permanentes.
- Almacenamiento de activos de TI conforme a las especificaciones de sus fabricantes.
- Marcado claro en todas las copias de soportes para la debida atención del receptor autorizado.

Con el objetivo de evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información y los datos personales se deberán tenerse en cuenta lo siguiente:

- Borrarse debidamente los contenidos de cualquier soporte que vaya a ser retirado.
- Solicitar autorización al Data Security Protection Officer (o responsable interno de protección de datos, en lo sucesivo <<DSPO>>), para extraer soportes de la organización.
- Los soportes deberán almacenarse en un entorno seguro y protegido, como armarios o cajoneras bajo llave.
- Se implementarán técnicas criptográficas para proteger los datos en soportes extraíbles, como el cifrado de las memorias USB o portátiles que contengan información personal.
- Los datos deberían transferirse a soportes de fabricación reciente antes de que se en conviertan ilegibles o se degrade el mismo soporte.
- Deberán almacenarse copias múltiples de datos valiosos en soportes separados.
- Se inventarían los soportes extraíbles.
- Solo se permitirá reproducir la información de soportes extraíbles cuando haya una razón de negocio para ello.
- La transferencia de información deberá ser monitorizada.

3. Conservación de datos de carácter personal y bloqueo

Es fundamental que la documentación que **Artigot Catering, S.L.** necesita manipular y tratar diariamente sea conservada adecuadamente. Por ello es necesario que todo documento que contenga datos personales no quede a la vista o resulte accesible por cualquier empleado cuyo puesto de trabajo no requiera el conocimiento de dichos datos, así como por terceros que pudiesen encontrarse en las oficinas de la organización. Los plazos de conservación de cada uno de los documentos o archivos

variarán en función del tratamiento al que se refieran. Todos aquellos datos personales que sean tratados en calidad de encargado de tratamiento por **Artigot Catering, S.L.** en tanto en cuanto, se tratan de la prestación de alguno de sus servicios, se borrarán, no quedando almacenados en ningún otro fichero, de conformidad por lo establecido en el contrato de Encargado de Tratamiento firmado con sus clientes, salvo que existiese una obligación legal o interés legítimo para dicha conservación.

Asimismo **Artigot Catering, S.L.** trata datos personales en calidad de Responsable de Tratamiento para la gestión de diferentes finalidades del tratamiento. Cada una de ellas tendrá un plazo de conservación que necesariamente habrá que respetar para garantizar los principios fundamentales de la normativa. En algunas ocasiones la normativa fija los plazos máximos de conservación, pero por norma general la normativa no establece dichos plazos, por lo que será una buena práctica de la empresa, el conservar los datos únicamente durante el plazo que resulten adecuados, pertinentes y no excesivos. En algunos casos, determinadas normas sí establecerán determinados **plazos mínimos de conservación**.

El **bloqueo de los datos** consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. En otras palabras, se trata de la obligación de mantener los datos cifrados cuya única función es desencriptarlos para poder usarlos para determinadas reclamaciones ante las administraciones competentes o los tribunales, cuyo acceso para ello, únicamente, será por parte del DSPO. Cuando la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar:

- La autenticidad de la evidencia.
- La fecha del bloqueo.
- La no manipulación de los datos.

Artigot Catering, S.L. estará obligada a bloquear los datos cuando proceda a su **rectificación** o **supresión**. Estas dos situaciones sucederán cuando:

- El interesado solicite al responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.
- El interesado solicite al responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando los datos no sean necesarios para cumplir con las finalidades por los que fueron recogidos; en los siguientes casos:
    - El interesado retire su consentimiento.

- El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
- Los datos son tratados ilícitamente.
- Los datos deben suprimirse debido a una obligación legal o los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

A través de la siguiente **tabla** se ejemplificará el **periodo de conservación de datos personales presentes en los activos de información** de **Artigot Catering, S.L.**. Esta tabla se encuentra dividida por las categorías de interesados y la finalidad por la que los datos fueron recabados. El periodo de conservación empezará a contar desde el momento en que **Artigot Catering, S.L.** recabó los datos, hasta su supresión. El periodo de bloqueo empezará a contar desde que proceda la rectificación o la supresión de los datos, a petición del interesado.

CATEGORÍAS DE INTERESADOS	FINALIDAD DEL TRATAMIENTO	PERIODO DE CONSERVACIÓN, INCLUYENDO SU BLOQUEO CUANDO PROCEDA	NORMATIVA DE REFERENCIA
Clientes	Ejecución de contrato	**Mientras el contrato esté en vigor. El bloqueo durará hasta 5 años después de la finalización del contrato.**	Artículo 1964.2 del Código Civil
	Facturación	**6 años desde la generación de la factura.**	Art. 30 del Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.
	Envío de publicidad	**Mientras se considere cliente.**	Artículo 21.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
	Prevención del blanqueo de capitales y de la financiación del terrorismo.	**10 años.**	Artículo 25 de la Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
Interesados sujetos a tratamientos de contabilidad	Documentación contable y comercial	**6 años, desde la generación de la documentación.**	Art. 30 del Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.
	Auditoría de cuentas	**5 años, desde la generación del informe.**	Artículo 30 de 22/2015, de 20 de julio, de Auditoría de Cuentas.
Potenciales clientes	Ejecución de medidas precontractuales	**Duración de las medidas. El bloqueo durará hasta 5 años después de la ejecución de las medidas.**	Artículo 1964.2 del Código Civil
	Envío de publicidad	**Hasta que el potencial cliente se oponga.**	Artículo 21.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio
Proveedores	Ejecución de contrato	**Mientras el contrato esté en vigor. El bloqueo durará hasta 5 años después de la finalización del contrato.**	Artículo 1964.2 del Código Civil

	Facturación	**6 años desde la generación de la factura.**	Art. 30 del Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.
Candidatos	Gestión de los datos del CV	**Se eliminarán inmediatamente tras finalizar el proceso de selección de personal. Ahora bien, en caso de que el interesado haya prestado su consentimiento, podrán almacenarse para futuros procesos de selección de personal durante el plazo de 1 año.**	Artículo 5.1.d del Reglamento General de Protección de Datos.
Empleados	Documentación laboral	**El bloqueo durará hasta 3 años después de la comisión de la posible infracción.** **En caso de infracción derivada del contrato de trabajo, el bloqueo durará hasta un año después de finalizado el contrato de trabajo.**	Artículo 4 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social. Artículo 59 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
	Videovigilancia (control laboral)	**30 días, salvo captación de ilícito.**	Artículo 22.3 de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
	Control de acceso	**30 días, salvo captación de ilícito que se procederá al bloqueo de las imágenes.**	Norma quinta de la Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
	Registro de jornada	**4 años.**	Artículo 34 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
	Nóminas y tributos	**El bloqueo durará hasta 4 años después de la finalización del contrato.**	Sección 3ª (La prescripción), Arts. 66 a 70 de la Ley 58/2003, de 17 de diciembre, General Tributaria.
	Seguridad social: Documentación que acredite el cumplimiento de obligaciones en materia de filiación, altas, bajas, documentos de cotización, recibos justificativos de gastos.	**4 años debe conservarse la documentación referente a altas, bajas, documentos de cotización y recibos justificativos de gastos.** **El bloqueo durará hasta 4 años después desde que le fuera exigible la obligación en materia de seguridad social.**	Artículo 21.1 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social. Artículo 24 del Real Decreto Legislativo 8/2015, de 30 de octubre, texto refundido Ley General de la Seguridad Social. Artículo 131 del Código Penal.

		El bloqueo durará hasta un máximo de 10 años, en caso de posible comisión de delito.	
	Denuncias internas	**3 meses.**	Artículo 24.4 de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
	Datos concernientes a la vigilancia de la salud	**Plazo de conservación de datos de salud en los términos reglamentariamente expuestos en función del riesgo al que se ha sometido al empleado. Ejemplo: Exposición a agentes cancerígenos: hasta 40 años desde la exposición.**	Artículo 22 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.
Usuarios web	Análisis de sus datos de navegación	**Durante la caducidad de las cookies.**	Artículo 45 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
	Gestión de los datos introducidos en formularios web	**Hasta que se cumpla la finalidad del formulario.**	Artículo 45 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
	Newsletter	**Hasta que el potencial cliente se oponga.**	Artículo 21.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio.
Terceros	Videovigilancia (seguridad)	**30 días, salvo captación de ilícito.**	Artículo 22.3 de Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
	Control de acceso	**30 días, salvo captación de ilícito.**	Norma quinta de la Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
Interesados de terceros	Gestión de los datos de interesados cuyos datos son responsabilidad de otro Responsable en el marco de un contrato de encargado de tratamiento.	**Mientras el contrato esté en vigor. El bloqueo durará hasta 5 años después de la finalización del contrato.**	Artículo 1964.2 del Código Civil
Interesados sujetos a obligaciones relacionadas con la protección de datos	Prueba de consentimiento, contestaciones de ejercicio de derechos, notificaciones de violaciones de seguridad, etc.	**Se bloquearán los datos durante un máximo de 3 años.**	Artículo 78 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Nombre y apellidos del empleado:	
Firma:	