INFORME EJECUTIVO DE **EVALUACIÓN DE IMPACTO** RELATIVA A LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL TRATAMIENTO RELATIVO AL SISTEMA DE **CONTROL HORARIO BIXPE**

ÍNDICE

Introducción

La gestión de riesgos en el ámbito de protección de datos está regulada en el artículo 35 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en adelante, RGPD.

La Evaluación de Impacto sobre Protección de Datos (EIPD) permite identificar riesgos y establecer una respuesta a éstos, adoptando las salvaguardas necesarias para reducir dichos riesgos hasta un nivel considerado aceptable. La EIPD pretende también dar respuesta al principio de responsabilidad proactiva ("accountability") de quienes tratan datos personales para determinar qué medidas son adecuadas para cumplir con el RGPD.

La EIPD es necesaria cuando exista una probabilidad de que un tipo de tratamiento, y de manera particular si se utilizan nuevas tecnologías, entrañe un **alto riesgo** para los derechos y libertades de las personas físicas teniendo en cuenta la naturaleza, alcance, contexto y fines de dicho tratamiento de datos.

El presente informe ejecutivo es un resumen de la Evaluación de Impacto realizada sobre la herramienta BIXPE CONTROL HORARIO para proporcionar a los Clientes de BIXPE (responsables del tratamiento) información sobre la adecuación de la herramienta a la normativa vigente en materia laboral y de protección de datos personales.

Identificación del tratamiento

- **Nombre del tratamiento:** BIXPE control horario.
- **Responsable y datos de contacto**: la herramienta está desarrollada y comercializada por ABBANZA RESEARCH INT, S.L., C/ Severo Ochoa, n.11 2ª Plt. Ofic. 5, 28521 Rivas Vaciamadrid (Madrid), CIF: B84596113, e-mail: info@abbanza.com, tel. 34 916 088 881, url: www.bixpe.com
- **Descripción del tratamiento:** Desarrollo de una app de fichaje y control horario para su comercialización. El personal de la empresa cliente podrá fichar las horas trabajadas a través de teléfono móvil, ordenador o tableta. En versiones posteriores, se podrá realizar el fichaje a través de huella dactilar y/o firma digital. La empresa Cliente podrá acceder a la información de fichaje a través de la app (Android, IOS) o de la página web. El fichaje puede ser geolocalizado y también tiene la posibilidad de subir fotos del usuario en el momento del fichaje.

  El sistema permitirá crear calendarios laborales y asignar horas de trabajo a cada trabajador y por cliente, lo que permite contabilizar horas extraordinarias y gestionar horas de proyectos. También genera informes para ver las horas trabajadas, horas en pausa y horas extra. Permite la edición de fichajes, eliminar jornadas y añadir jornadas, para corregir posibles errores, por parte de empleados y de gerentes.

Análisis de necesidad de la Evaluación.

Como fase previa a la realización de la EIPD, se hace necesario realizar un estudio sobre la necesidad de ésta. Para ello, se han evaluado los siguientes aspectos:

- Datos personales que se van a tratar
- Proveniencia de los datos
- Operaciones de tratamiento a realizar
  - ✓ Mecanismo de recogida de datos
  - ✓ Sistema de almacenamiento y tratamiento
  - ✓ Uso principal que se le va a dar al dato
  - ✓ Destrucción del dato
- Personas o grupos de personas afectadas.

Adicionalmente, través del siguiente cuestionario[1] se han evaluado otros aspectos que permiten identificar la necesidad de realización de una EIPD:

Pregunta / cuestión	SI/NO	COMENTARIOS
¿La autoridad de supervisión competente ha publicado una lista de tratamientos para los que se exige llevar a cabo la evaluación? ¿El tratamiento objeto de evaluación se puede considerar que está incluido en esa lista?	**SI**	La AEPD ha publicado una lista de tratamientos que SI requieren EIPD. Entre ellos se citan: *"Tratamientos que impliquen la observación, monitorización, supervisión, **geolocalización o control del interesado** de forma sistemática y exhaustiva (…)"* *"Tratamientos que impliquen el uso de **datos biométricos con el propósito de identificar** de manera única a una persona física"*
¿Las operaciones de tratamiento implican llevar a cabo una evaluación sistemática y amplia de aspectos personales relativos a personas físicas?	**SI**	Se puede considerar evaluación sistemática el estudio y la generación de informes por trabajador.

[1] Cuestionario elaborado por la Autoritat Catalana de Protecciò de Dades – Guía práctica. Evaluación de Impacto relativa a la Protección de Datos.

Pregunta / cuestión	SI/NO	COMENTARIOS
¿Con las operaciones de tratamiento se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc., de personas identificadas o identificables?	**SI**	Se pueden determinar comportamientos de personas identificadas.
¿Con carácter general, podemos considerar que una de las finalidades del tratamiento es predecir comportamientos?	**NO**	
¿En base al tratamiento se van a tomar decisiones con efectos jurídicos para las personas afectadas?	**SI**	No es la finalidad del tratamiento, pero la información elaborada a través del tratamiento si puede permitir la toma de decisiones con efectos jurídicos (amonestaciones, despidos…)
¿En base al tratamiento de los datos se van a tomar decisiones que podrían afectar significativamente o perjudicar de alguna manera a las personas afectadas?	**SI**	No es la finalidad del tratamiento, pero la información elaborada a través del tratamiento si puede permitir la toma de decisiones con efectos jurídicos (amonestaciones, despidos…)
¿Va a ser objeto de tratamiento a gran escala alguna categoría/s especial/es de datos?	**NO**	
¿Se va a llevar un control sistemático, o monitorización, a gran escala de áreas de acceso público?	**NO**	
¿La iniciativa o proyecto supone la recopilación de nuevos datos de carácter personal que hasta ahora no se recogían?	**SI**	En aquellos clientes que anteriormente no realizaban control horario o, si lo realizaban, no era a través de geolocalización o con captación de fotografía.
El tratamiento se va a llevar a cabo con información disociada o anonimizada.	**SI**	Las operaciones de tratamiento se realizan con un identificador que asigna la herramienta. Solo cuando se muestra la información al usuario se asocia al nombre del trabajador.
El tratamiento implica cruzar información con otras fuentes u orígenes externos para ser ampliada.	**NO**	
El tratamiento implica revelar información a terceros.	**NO**	A los clientes que han contratado la herramienta. No es una revelación

Pregunta / cuestión	SI/NO	COMENTARIOS
		como tal sino un acceso a la información que genera el sistema.
El tratamiento implica el uso de los datos para finalidades distintas a las previstas inicialmente.	**NO**	Las funcionalidades de la herramienta están dirigidas exclusivamente a control horario.
Se van a utilizar tecnologías que podrían ser especialmente intrusivas para la privacidad.	**SI**	Geolocalización, captación de fotografía en el momento del fichaje y, en un futuro, huella digital y firma.
¿Existen riegos específicos para la seguridad de la información, en particular, un riesgo relevante de acceso por parte de terceros no autorizados?	**NO**	Existen los riesgos de cualquier sistema de información, pero no se detectan riesgos específicos relativos a accesos no autorizados.
Se van a realizar transferencias internacionales de datos.	**SI**	Hay prestadores de servicio ubicados en USA, pero adheridos al escudo de privacidad.
Se van a tratar datos de menores de edad.	**NO**	La finalidad de la herramienta no implica recoger esta información.
El tratamiento implica la evaluación o puntuación (scoring) de personas.	**NO**	
El tratamiento en sí mismo impide a las personas afectadas ejercer un derecho o las limita de alguna manera.	**NO**	Los derechos de las personas están garantizados salvo las excepciones a dichos ejercicios que marque la normativa laboral.
¿El tratamiento supone algún tipo de vigilancia u observación sistemática de personas?	**SI**	Se realiza observación sistemática de la jornada laboral.
¿El tratamiento implica combinar diferentes fuentes de información o datos relacionados con tratamientos diversos?	**NO**	El tratamiento como tal no, pero genera información que se puede combinar con otras fuentes o tratamientos (gestión de RR.HH. principalmente)
¿Se tratan datos relativos a personas en situación de desequilibrio en relación con el responsable del tratamiento?	**NO**	
¿Las operaciones de tratamiento suponen utilizar o aplicar soluciones tecnológicas u organizativas de forma innovadora?	**NO**	El uso de Apps y tecnologías web y móviles está consolidado.
Los datos recogidos ¿se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni	N/A	El uso que se dé a la información que recoge la herramienta dependerá del Cliente.

Pregunta / cuestión	SI/NO	COMENTARIOS
incompatible con la legitimidad de su uso (principio de limitación de la finalidad)?		
La finalidad que se pretende cubrir ¿requiere de todos los datos a recabar y para todas las personas/interesados afectados (principio de minimización de datos)?	**SI**	Los campos obligatorios son los mínimos necesarios para la funcionalidad de la herramienta y, también para dar cumplimiento a la normativa laboral sobre control horario (Real Decreto Ley 8/2019 que modifica el artículo 34 del Estatuto de los Trabajadores). La geolocalización y fotografía se activan por el Cliente en función de sus necesidades.
Las tecnologías empleadas para el tratamiento son ¿adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad?	**SI**	El uso de Apps y tecnologías web y móviles está consolidado.

Por todo lo anteriormente expuesto, se concluye que **PROCEDE** realizar una Evaluación de Impacto sobre el tratamiento de datos a través de BIXPE CONTROL HORARIO.

Evaluación de impacto.

Descripción del método de evaluación.

La EIPD objeto del presente informe se ha realizado siguiendo la metodología propuesta por la Agencia Española de Protección de Datos en su "Guía práctica para las Evaluaciones de Impacto en la Protección de Datos sujetas al RGPD" (ver. Junio 2018).

El proceso de evaluación se ha dividido en 3 grandes bloques:

1. *Identificación del contexto en el que se tratan los datos:*
   - 1.1. Estudio del **ciclo de vida** de los datos objeto de tratamiento: origen éstos, clasificación y almacenamiento, uso y tratamiento, accesos por parte de terceros y procesos de destrucción.
   - 1.2. Análisis de la **necesidad y proporcionalidad** del tratamiento: identificar finalidades y medios del tratamiento; identificar los datos objeto de tratamiento y evaluar su necesidad para la finalidad con la que se pretenden recoger teniendo en cuenta también el origen de éstos.
   - 1.3. **Licitud** del tratamiento: evaluación de la base legitimadora del tratamiento, conforme al artículo 6 del RGPD.
2. *Gestión de los riesgos:*
   - 2.1. Identificación de **amenazas y riesgos:** identificación de potenciales escenarios de riesgo que afecten negativamente a los derechos y libertades de los afectados.
   - 2.2. **Evaluación y valoración** de riesgos detectados: estimar la probabilidad y el impacto de que los riesgos detectados se materialicen.
   - 2.3. **Tratamiento** de los riesgos: definir las medidas necesarias para tratar los riesgos detectados y reducir el nivel de exposición.
3. *Conclusiones:*

   Elaboración de un **informe final de conclusiones** basado en el nivel de riesgo residual, valorando si se considera elevado o aceptable y, por tanto, si la EIPD es favorable o no.

Identificación del contexto.

- **Estudio del ciclo de vida de los datos.**

En la siguiente tabla se expone detalladamente el ciclo de vida y el flujo de datos personales que se produce a través de este, así como todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin.

		ETAPAS DEL CICLO DE VIDA DEL DATO				
		Captura (C)	**Clasificación Almacenamiento (C/A)**	**Uso Tratamiento (U/T)**	**Acceso por terceros (cesión o tratamiento) (AT)**	**Destrucción (D)**
ELEMENTOS	**Actividades del proceso**	Recogida y registro: - Alta de usuarios por parte del administrador. - Generación de datos por parte del usuario cada vez que ficha. - Captura automática de posición GPS (si la opción está habilitada) - Captura automática de la fotografía del usuario (si la opción está habilitada) - Captura automática de datos estadísticos a través de cookies.	Estructuración: - Almacenamiento de la información en sistemas cloud de Azure	Consulta y utilización: - Consulta por Cliente - Generación de informes - Exportación de datos - Realización de estudios estadísticos	Almacenamiento: - Microsoft Azure West Europe (Holanda) Consulta: - Abbanza Research, Int, S.L. - Zoho Corporation, B.V. - Stripe Inc - Mailjet, SAS.	Borrado: - Todos los registros se conservan un máximo de 4 años. Bloqueo otros 4 años. - Los datos generados por las cookies se conservan el tiempo necesario para elaborar las estadísticas.
	Datos tratados	Nombre completo e-mail Número de afiliación Rol Posición GPS Fotografía Huella dactilar Firma digital Número de tarjeta Horarios de fichaje Datos generados por cookies	Nombre completo e-mail Número de afiliación Rol Posición GPS Fotografía Huella dactilar Firma digital Número de tarjeta Horarios de fichaje Datos generados por cookies	Nombre completo e-mail Número de afiliación Rol Posición GPS Fotografía Huella dactilar Firma digital Número de tarjeta Horarios de fichaje Datos generados por cookies	Nombre completo e-mail Número de afiliación Rol Posición GPS Fotografía Huella dactilar Firma digital Número de tarjeta Horarios de fichaje Datos generados por cookies	Nombre completo e-mail Número de afiliación Rol Posición GPS Fotografía Huella dactilar Firma digital Número de tarjeta Horarios de fichaje Datos generados por cookies
	Intervinientes	Usuario: generador de datos Administrador: inclusión de datos	Proceso automático	Usuario: generador de datos y consulta. Administrador: consulta	Procesos automáticos Accesos puntuales para mantenimiento de sistemas por parte de Abbanza	Abbanza Usuario Administrador
	Tecnologías	PC Tablet Smartphones App	Servidores cloud	PC Tablet Smartphones App	Servidores cloud App	Borrado de campos en servidores cloud
	Transferencias Internacionales de datos	N/A	Procesamiento de pagos (devoluciones)	Procesamiento de pagos (devoluciones)	Stripe Inc en USA, compañía adherida a Escudo de Privacidad	N/A

- **Análisis de terceros intervinientes.**

A continuación, se identifica la participación de intervinientes para analizar si éstos pueden suponer una amenaza sobre los datos de carácter personal:

IDENTIFICACIÓN	CATEGORIA Y SERVICIO	EVALUACIÓN
Microsoft Azure	Alojamiento cloud. Encargado de tratamiento	Los servidores contratados para el alojamiento se encuentran en West Europe, concretamente en Holanda. La compañía dispone de directrices en materia de seguridad y de cumplimiento del RGPD: https://www.microsoft.com/en-us/security https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview Adicionalmente, aunque se utilizan servidores ubicados en EEU, la compañía Microsoft se encuentra adherida al Escudo de Privacidad de Departamento de Comercio del Gobierno de Estados Unidos. **NO SUPONE UNA AMENAZA SOBRE LOS DATOS OBJETO DE TRATAMIENTO.**
Abbanza Research, Int, S.L.	Desarrollador y mantenimiento de la herramienta. Encargado de tratamiento.	Los clientes que contratan la herramienta formalizan contrato de tratamiento a de datos por cuenta de terceros, bien como documento individual, bien como cláusula de las condiciones generales de contratación. El acceso a la información se realiza exclusivamente para tareas de mantenimiento o en caso de incidencias. **NO SUPONE UNA AMENAZA SOBRE LOS DATOS OBJETO DE TRATAMIENTO.**
Zoho Corporation B.V.	Software de soporte y ayuda a usuarios, facturación. Encargado de tratamiento.	La compañía se encuentra en Amsterdam, Países Bajos. La compañía dispone de directrices en materia de seguridad y de cumplimiento del RGPD: https://www.zoho.eu/es-xl/privacy.html https://www.zoho.eu/gdpr.html Adicionalmente, aunque se utilizan servidores ubicados en EEU, la compañía Zoho se encuentra adherida al Escudo de Privacidad de Departamento de Comercio del Gobierno de Estados Unidos. **NO SUPONE UNA AMENAZA SOBRE LOS DATOS OBJETO DE TRATAMIENTO.**
Stripe Inc	Plataforma de procesamiento de pagos. Encargado de tratamiento.	La plataforma está gestionada por Zoho Corporation aunque ABBANZA puede acceder cuando el Cliente solicita el reembolso. La compañía Stripe se encuentra adherida al Escudo de Privacidad de Departamento de Comercio del Gobierno de Estados Unidos. **NO SUPONE UNA AMENAZA SOBRE LOS DATOS OBJETO DE TRATAMIENTO.**
Mailjet, SAS.	Plataforma de e-mailing. Encargado de tratamiento.	La compañía se encuentra en Francia. La compañía dispone de políticas anti-spam: https://es.mailjet.com/sending-policy/ **NO SUPONE UNA AMENAZA SOBRE LOS DATOS OBJETO DE TRATAMIENTO.**

Análisis de legitimación y licitud, necesidad y proporcionalidad de las operaciones de tratamiento respecto a la finalidad.

- **Legitimación y licitud**

La **legitimación** para el tratamiento de los datos se encuentra en:

- ✓ Artículo 6.1.a): Consentimiento del interesado. Los usuarios deben aceptar las condiciones de privacidad de la herramienta cuando acceden por primera vez a ésta.
- ✓ Artículo 6.1.b): Tratamiento necesario para la ejecución de un contrato. El control de las horas trabajadas es necesario para la relación laboral entre empresa y trabajador.
- ✓ Artículo 6.1.c): Tratamiento necesario para el cumplimiento de una obligación legal. La empresa deber cumplir con la normativa laboral sobre control horario (Real Decreto Ley 8/2019 que modifica el artículo 34 del Estatuto de los Trabajadores).
- ✓ Artículo 6.1.f): Tratamiento necesario para satisfacer intereses legítimos. Realización de estadísticas y estudio de datos para mejora de la herramienta.

La **licitud** del tratamiento de los datos se analiza en los siguientes apartados:

- ✓ **Procedimiento para cumplir con el deber de información:** el usuario debe aceptar las condiciones de tratamiento de datos la primera vez que accede a la herramienta. En dichas condiciones se advierte que ABBANZA es encargada de tratamiento y que el Responsable del tratamiento es la empresa cliente. También se informa sobre el tratamiento que ABBANZA puede realizar de los datos recabados a través de cookies. Adicionalmente, ABBANZA facilita a sus clientes un modelo informativo sobre el tratamiento de datos a través de BIXPE para que éstos lo faciliten a sus trabajadores.
- ✓ **Procedimiento para recabar el consentimiento:** No procede recabar consentimiento ya que la legitimación principal para el tratamiento de datos se basa en el cumplimiento de obligación legal, en la necesidad de dicho tratamiento para la ejecución del contrato laboral y el interés legítimo en mejorar la herramienta. No obstante, como comentado anteriormente, el usuario debe aceptar las condiciones de tratamiento de datos la primera vez que accede a la herramienta.
- ✓ **Procedimiento previsto para ejercicio de derechos:** los usuarios disponen de un apartado en la herramienta de contacto y sugerencias para el desarrollador. En caso

de recibir algún ejercicio de derechos por parte de los interesados, ABBANZA trasladará ésta al Cliente en calidad de Responsable del tratamiento.

- **Necesidad y proporcionalidad:**

	Análisis	Observaciones
Principio de limitación de la finalidad ¿Los datos se usan exclusivamente para la finalidad declarada e informada?	Cumple	La herramienta, por si misma, no proporciona utilidades que permitan usos distintos a los informados.
Principio de minimización de datos ¿La finalidad requiere todos los datos a recabar y de todos los interesados?	La finalidad de control horario puede no requerir necesariamente la geolocalización ni la captación de imágenes.	Tanto la geolocalización como la captación de imágenes son utilidades que se deben activar por parte del administrador (Cliente) quien deberá analizar si, para su organización, los datos resultan necesarios.
	La combinación de fichaje a través de huella digital y captación de imágenes puede resultar excesiva para la finalidad de verificación del usuario que ficha.	Cuando se active la función de fichaje a través de huella digital la opción de captar imagen se desactivará.
Principio de minimización de datos ¿Las tecnologías respetan los principios fundamentales de privacidad?	Cumple	La única tecnología que pudiera considerarse invasiva es la geolocalización y se trata de una utilidad opcional, informada y legitimada por el desarrollo de la relación laboral.
Principio de limitación de conservación ¿Los datos se mantienen el tiempo estrictamente necesario para las finalidades del tratamiento?	Cumple	Los registros se conservan un máximo de 4 años para dar cumplimiento a la legislación laboral. Posteriormente se conservan durante 4 años más, debidamente bloqueados.
Conclusiones	La herramienta respeta los principios de limitación de finalidad y limitación de conservación. El principio de minimización del dato se cumple, pero en mayor o menor medida dependiendo de las necesidades del Cliente.	

Análisis de Riesgos del tratamiento: identificación, evaluación y respuesta

- **Identificación detallada de riesgos (exposición a amenazas)**

GRUPO	COD.	AMENAZA	FASE DEL TRATAMIENTO (*)
GENERALES	G1	Pérdidas económicas y daños reputacionales por incumplimiento de legislación de protección de datos.	U/T
	G2	Pérdidas económicas y daños reputacionales por incumplimiento de legislación sectorial que pueda incidir en la protección de datos.	U/T, D
	G3	Pérdidas económicas, de clientes y daños reputacionales derivados de la falta o ineficacia de medidas de seguridad.	C, C/A, UT, AT, D
	G4	Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por la deficiente gestión de la privacidad.	UT
	G5	Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	UT
	G6	Incorporación tardía de expertos en protección de datos o definición deficiente de sus funciones y competencias.	N/A
LEGITIMACIÓN Y CESIÓN DE DATOS	L1	Tratar o ceder los datos cuando no es necesario para la finalidad perseguida.	UT
	L2	No disponer de legitimación clara y suficiente para el tratamiento o la cesión de datos.	C, UT
	L3	Consentimiento dudoso, viciado o inválido para el tratamiento o la cesión.	C
	L4	Dificultar la revocación del consentimiento o la oposición a un tratamiento o cesión.	UT, D
	L5	Dificultad para garantizar la legitimidad de la recogida o cesión.	C
	L6	Tratar categorías especiales de datos sin necesidad o sin adoptar salvaguardas.	N/A
	L7	Enriquecer los datos, cuando no esté previsto en la finalidad inicial y sin informar, mediante interconexión con otros sistemas (propios o de terceros). Revertir un proceso de disociación.	UT
	L8	No permitir la utilización anónima de un producto o servicio cuando la identificación no es indispensable.	N/A
TRANSFERENCIAS INTERNACIONALES	TI1	Carencia de mecanismos de control de cumplimiento de garantías adecuadas.	C/A, U/T
	TI2	Impedimentos por parte del importador para el ejercicio de procedimientos de supervisión y control.	C/A, U/T
	TI3	Incapacidad de ayudar a los interesados en el ejercicio de sus derechos ante el importador.	U/T
	TI4	No obtención de las autorizaciones legales	N/A

GRUPO	COD.	AMENAZA	FASE DEL TRATAMIENTO (*)
REGISTRO DE ACTIVIDADES DE TRATAMIENTO	AT1	No disponer de mecanismos y procedimientos para poder mantener actualizado el registro de actividades de tratamiento.	U/T
	AT2	No disponer de mecanismos y procedimientos para detectar cuando deber realizarse EIPD.	C, UT
TRANSPARENCIA DE LOS TRATAMIENTOS	T1	No proporcionar información en la recogida de datos o recabarlos de manera fraudulenta o no autorizada.	C, C/A
	T2	Entorno web: ubicar la información en lugares de difícil localización o diseminada que dificulte su acceso.	U/T, AT
	T3	No redactar la información con lenguaje claro que impida que los interesados se hagan una idea clara de los elementos esenciales sobre el tratamiento.	C
CALIDAD DE LOS DATOS	C1	Solicitar datos innecesarios para las finalidades del nuevo sistema, producto o servicio.	C
	C2	Existencia de errores que propicien la falta de integridad de la información, permitiendo registros duplicados con informaciones diferentes.	C/A, U/T
	C3	Garantías insuficientes para el uso de datos con fines históricos, científicos o estadísticos.	U/T
	C4	Utilizar los datos para finalidades no especificadas o incompatibles con las declaradas: datos transaccionales, de navegación o geolocalización para monitorizar el comportamiento, realizar perfiles o toma de decisiones.	U/T
	C5	Utilizar los datos para finalidades no especificadas o incompatibles con las declaradas: toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.	U/T
	C6	Utilizar metadados para finalidades no especificadas o incompatibles con las declaradas.	UT, AT
	C7	Realizar inferencias o deducciones erróneas mediante el uso de técnicas de inteligencia artificial, reconocimiento facial o análisis biométricos.	C/A, UT
	C8	No disponer de procedimientos y herramientas para garantizar la cancelación de oficio de los datos una vez que han dejado de ser necesarios.	AT, D
CATEGORÍAS ESPECIALES DE DATOS	CE1	Fallos o errores para recabar el consentimiento expreso cuando sea ésta la legitimación a su tratamiento o cesión.	N/A
	CE2	Considerar erróneamente la habilitación legal como legitimación al tratamiento o cesión.	N/A
	CE3	Disociación deficiente o reversible en procesos de investigación que solo prevén usar datos anónimos.	N/A

GRUPO	COD.	AMENAZA	FASE DEL TRATAMIENTO (*)
DEBER DE SECRETO	S1	Acceso no autorizado a datos.	C/A, U/T, AT, D
	S2	Violaciones de confidencialidad por agentes intervinientes.	C/A, U/T, AT, D
TRATAMIENTOS POR ENCARGO	ET1	Inexistencia de contrato o contrato erróneo.	U/T, AT, D
	ET2	Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento.	U/T, AT, D
	ET3	Gestión y control deficiente de los encargados y subcontratistas. Dificultades para comprobar que éstos cumplen con las instrucciones.	U/T, AT, D
	ET4	No disponer de un procedimiento (o que sea deficiente) para comunicar el ejercicio de derechos al responsable.	U/T
	ET5	Dificultad para conseguir la portabilidad de datos a otros entornos una vez finalizado el contrato.	U/T, D
DERECHOS DE LOS INTERESADOS	D1	Dificultar o imposibilitar el ejercicio de derechos.	U/T
	D2	Carencia de procedimientos para la gestión de los derechos.	U/T
	D3	Carencia de procedimientos para comunicar rectificaciones, cancelaciones u oposiciones a los cesionarios.	N/A
SEGURIDAD	S1	Inexistencia de comité o responsable de seguridad o deficiente definición de sus funciones y competencias.	C, C/A, U/T, AT, D
	S2	Inexistencia de política de seguridad.	C, C/A, U/T, AT, D
	S3	Deficiencias técnicas y organizativas en la gestión del control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	C, U/T, AT
	S4	Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo e un sistema de información.	C, U/T, AT
	S5	Uso de identificadores que revelan información del afectado.	C, U/T, AT
	S6	Deficiencias en la protección de la confidencialidad de la información.	C, U/T, C/A, AT
	S7	Falta de formación de los agentes intervinientes sobre las medidas de seguridad y consecuencias de no adoptarlas.	C, U/T, AT
	S8	Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral...) para terceros no autorizados.	U/T, AT, D

***(*) C**: Captura, **C/A**: clasificación/almacenamiento, **U/T**: uso/tratamiento, **AT**: acceso por terceros, **D**: destrucción*

- **Impacto y probabilidad de cada riesgo identificado (riesgo inherente) y Gestión de los riesgos: decisión adoptada para cada riesgo, objetivos de control, controles y medidas propuestas (riesgo residual)**

El riesgo inherente y el riesgo residual se han valorado conforme a la siguiente **MATRIZ DE RIESGOS[2]:**

Probabilidad					
	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4
		IMPACTO			

Bajo
Medio
Alto
Muy Alto

[2] Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD – Agencia Española de Protección de Datos.

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
G1	Pérdidas económicas y daños reputacionales por incumplimiento de legislación de protección de datos.	Riesgo de sanción por incumplimiento. Riesgo de difusión de sanción.	2	Disponer de un Sistema de Gestión de Protección de datos que contempla revisiones y controles periódicos de cumplimiento.	1
G2	Pérdidas económicas y daños reputacionales por incumplimiento de legislación sectorial que pueda incidir en la protección de datos.	Riesgo de sanción por incumplimiento. Riesgo de difusión de sanción.	6	Disponer de un Sistema de Gestión de Protección de datos que contempla revisiones y controles periódicos de cumplimiento.	1
G3	Pérdidas económicas, de clientes y daños reputacionales derivados de la falta o ineficacia de medidas de seguridad.	Riesgo de difusión de ineficacia de medias de seguridad.	1	Disponer de un Sistema de Gestión de Protección de datos que contempla revisiones y controles periódicos de cumplimiento.	1
G4	Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por la deficiente gestión de la privacidad.	Riesgo de dejar de utilizar la herramienta por parte del Cliente.	6	Revisiones periódicas de la herramienta y actualizaciones.	4
G5	Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados.	Riesgo de no atender ejercicios de derechos y reclamaciones de los interesados.	6	Acciones de formación y concienciación de personal técnico.	2
L1	Tratar o ceder los datos cuando no es necesario para la finalidad perseguida.	Riesgo de incumplimiento del principio de limitación de la finalidad. Riesgo de cesiones de datos no legítimas.	6	Acciones de formación y concienciación de personal técnico.	1
L2	No disponer de legitimación clara y suficiente para el tratamiento o la cesión de datos.	Riesgo de incumplimiento del principio de legitimación. Riesgo de cesiones de datos no legítimas.	6	Habilitación de casillas de consentimiento al tratamiento de datos.	2
L3	Consentimiento dudoso, viciado o inválido para el tratamiento o la cesión.	Riesgo de incumplimiento del principio de legitimación.	6	Habilitación de casillas de consentimiento al tratamiento de datos.	1

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
L4	Dificultar la revocación del consentimiento o la oposición a un tratamiento o cesión.	Riesgo de reclamación de los interesados.	4	Habilitación de canales de comunicación con el interesado.	1
L5	Dificultad para garantizar la legitimidad de la recogida o cesión.	Riesgo de incumplimiento del principio de legitimación.	4	Habilitación de casillas de consentimiento al tratamiento de datos. Habilitación de textos informativos.	1
L7	Enriquecer los datos, cuando no esté previsto en la finalidad inicial y sin informar, mediante interconexión con otros sistemas (propios o de terceros). Revertir un proceso de disociación.	Riesgos de incumplimiento del principio de limitación de la finalidad. Riesgo de incumplimiento del deber de información.	6	No existe medida de control por parte de ABBANZA.	6
AT1	No disponer de mecanismos y procedimientos para poder mantener actualizado el registro de actividades de tratamiento.	Riesgo de incumplimiento del deber de mantener actualizado el RAT	1	No existe medida de control por parte de ABBANZA.	1
AT2	No disponer de mecanismos y procedimientos para detectar cuando deber realizarse EIPD.	Riesgo de incumplimiento de deber de realización de EIPD	1	Realización de la presente EIPD y revisión periódica de ésta cuando se produzcan cambios en la herramienta	1
T1	No proporcionar información en la recogida de datos o recabarlos de manera fraudulenta o no autorizada.	Riesgo de incumplimiento del deber de información.	6	Habilitación de casillas de consentimiento al tratamiento de datos. Habilitación de textos informativos.	1
T2	Entorno web: ubicar la información en lugares de difícil localización o diseminada que dificulte su acceso.	Riesgo de incumplimiento del deber de información.	3	Incluir textos informativos en zonas visibles y de fácil acceso al usuario	1
T3	No redactar la información con lenguaje claro que impida que los interesados se hagan una idea clara de los elementos esenciales sobre el tratamiento.	Riesgo de incumplimiento del deber de información.	3	Redacción de texto informativo a interesados de forma clara.	1
C1	Solicitar datos innecesarios para las finalidades del nuevo sistema, producto o servicio.	Riesgos de incumplimiento del principio de limitación de la finalidad.	6	Antes de incluir campos nuevos, revisar la presente EIPD.	2

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
C2	Existencia de errores que propicien la falta de integridad de la información, permitiendo registros duplicados con informaciones diferentes.	Riesgo de no mantener los datos actualizados.	1	Revisiones periódicas de las bases de datos	1
C3	Garantías insuficientes para el uso de datos con fines históricos, científicos o estadísticos.	Riesgo de utilizar datos no actualizados en fases estadísticas	1	No existe medida de control por parte de ABBANZA.	1
C4	Utilizar los datos para finalidades no especificadas o incompatibles con las declaradas: datos transaccionales, de navegación o geolocalización para monitorizar el comportamiento, realizar perfiles o toma de decisiones.	Riesgos de incumplimiento del principio de limitación de la finalidad. Riesgo de incumplimiento del deber de información.	6	No existe medida de control por parte de ABBANZA.	6
C5	Utilizar los datos para finalidades no especificadas o incompatibles con las declaradas: toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.	Riesgos de incumplimiento del principio de limitación de la finalidad. Riesgo de incumplimiento del deber de información.	6	No existe medida de control por parte de ABBANZA.	6
C6	Utilizar metadados para finalidades no especificadas o incompatibles con las declaradas.	Riesgos de incumplimiento del principio de limitación de la finalidad. Riesgo de incumplimiento del deber de información.	1	Api de integración con otras herramientas de los Clientes.	1
C7	Realizar inferencias o deducciones erróneas mediante el uso de técnicas de inteligencia artificial, reconocimiento facial o análisis biométricos.	Riesgo de valoraciones erróneas.	1	No existe medida de control por parte de ABBANZA.	1
C8	No disponer de procedimientos y herramientas para garantizar la cancelación de oficio de los	Riesgo de incumplimiento del principio de minimización del dato.	2	Procedimientos automáticos de borrado de datos pasados 4 años.	1

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
	datos una vez que han dejado de ser necesarios.	Posibilidad de acceso a datos personales una vez finalizada su utilidad.			
S1	Acceso no autorizado a datos.	Riesgo de tratamiento de datos por personal no autorizado.	6	Procedimientos robustos de validación y verificación periódica de accesos: contraseña de, mínimo 6 caracteres, 1 mayúscula y 1 número. Cambio recomendado (con aviso de la herramienta) 1 vez al año. Fichaje en modo PIN (6 cifras) generado por gerente o aleatoriamente con envío por mail al usuario. Almacenamiento cifrado de contraseñas. Recuperación exclusivamente por el usuario (generar nueva contraseña)	3
S2	Violaciones de confidencialidad por agentes intervinientes.	Riesgo de tratamiento de datos por personal no autorizado.	6	Idem a anterior	3
ET1	Inexistencia de contrato o contrato erróneo.	Riesgo de tratamiento de datos por parte de terceros sin las garantías adecuadas.	3	Firma de contratos de tratamiento con todos los clientes y/o aceptación de las condiciones de contratación.	1
ET2	Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento.	Riesgo de tratamiento de datos por parte de terceros sin las garantías adecuadas.	3	Firma de contratos de tratamiento con todos los clientes y/o aceptación de las condiciones de contratación.	1
ET3	Gestión y control deficiente de los encargados y subcontratistas. Dificultades para comprobar que éstos cumplen con las instrucciones.	Riesgo de tratamiento de datos por parte de terceros sin las garantías adecuadas.	3	Firma de contratos de tratamiento con todos los subcontratistas y/o aceptación de las condiciones de contratación.	1
ET4	No disponer de un procedimiento (o que sea deficiente) para comunicar el ejercicio de derechos al responsable.	Riesgo de no atender en tiempo y forma las solicitudes de ejercicio de derechos por parte de los interesados.	3	Canal de comunicación con clientes	1
ET5	Dificultad para conseguir la portabilidad de datos a otros entornos una vez finalizado el contrato.	Riesgo de no atender de manera eficiente el derecho a la portabilidad	4	ABBANZA puede facilitar la portabilidad, pero bajo solicitud del Cliente, responsable de los datos.	4

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
D1	Dificultar o imposibilitar el ejercicio de derechos.	Riesgo de no atender en tiempo y forma las solicitudes de ejercicio de derechos por parte de los interesados.	3	Procedimiento interno de traslado de los ejercicios de derechos que lleguen a ABBANZA al cliente.	2
D2	Carencia de procedimientos para la gestión de los derechos.	Riesgo de no atender en tiempo y forma las solicitudes de ejercicio de derechos por parte de los interesados.	3	Procedimiento interno de traslado de los ejercicios de derechos que lleguen a ABBANZA al cliente.	2
S1	Inexistencia de comité o responsable de seguridad o deficiente definición de sus funciones y competencias.	Riesgo de aplicación errónea o falta de aplicación de los preceptos del RGPD y LOPDGDD.	3	Designación de un coordinador de protección de datos.	1
S2	Inexistencia de política de seguridad.	Riesgo de aplicación errónea o falta de aplicación de los preceptos del RGPD y LOPDGDD.	3	Disponer de un Sistema de Gestión de Protección de Datos y de una Política de Protección de Datos.	2
S3	Deficiencias técnicas y organizativas en la gestión del control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.	Riesgo de acceso a datos por personal no autorizado.	6	Procedimientos robustos de validación y verificación periódica de accesos.	2
S4	Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información.	Riesgo de no poder atribuir acciones al usuario que las ha realizado.	6	Procedimientos robustos de validación y verificación periódica de accesos.	2
S5	Uso de identificadores que revelan información del afectado.	Riesgo de divulgación de información personal.	1	Requisitos de usuarios y contraseñas que impidan identificadores sencillos	1
S6	Deficiencias en la protección de la confidencialidad de la información.	Riesgo de divulgación de información personal.	3	Mecanismos de protección de la confidencialidad del sistema cloud de Azure	2
S7	Falta de formación de los agentes intervinientes sobre las medidas de seguridad y consecuencias de no adoptarlas.	Riesgo de accesos no autorizados, usos con finalidades incompatibles, pérdida de información.	6	Acciones de formación y concienciación en protección de datos.	2

COD.	AMENAZA	RIESGO	RIESGO INHERENTE	MEDIDA DE CONTROL	RIESGO RESIDUAL
S8	Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral...) para terceros no autorizados.	Riesgo de accesos no autorizados, usos con finalidades incompatibles.	1	Acciones de formación y concienciación en protección de datos.	1

Conclusiones

Una vez evaluados los potenciales riesgos a los que se enfrentan los datos personales manejados a través de la herramienta, identificados los riesgos y analizadas las salvaguardas puestas en marcha para reducir dichos riesgos hasta un nivel considerado aceptable, se concluye que **la herramienta BIXPE CONTROL HORARIO no supone una amenaza para los derechos y libertades de los interesados.**

De igual modo, teniendo en cuenta el ciclo de vida del dato, los intervinientes en cada fase de tratamiento, la legitimación y licitud de éste, la necesidad y proporcionalidad de los datos y los riegos a los que éstos se exponen, BIXPE CONTROL HORARIO se considera una herramienta adecuada para dar cumplimiento a la normativa laboral sobre control horario (Real Decreto Ley 8/2019 que modifica el artículo 34 del Estatuto de los Trabajadores).

Por último, teniendo en cuenta el riesgo residual detectado, aunque éste se considera **asumible**, es posible su reducción implantado medidas de control adicionales que se **sugieren** a continuación:

COD.	RIESGO RESIDUAL	MEDIDA DE CONTROL PROPUESTA	RESPONSABLE DE IMPLANTACIÓN
G4	4	Reevaluar periódicamente la EIPD, especialmente cuando se vayan a incluir nuevas utilidades.	Abbanza Research Int, S.L.
L7	6	Informar a los interesados si se va a realizar interconexión con otros sistemas para enriquecer los datos generados por BIXPE.	Empresas Cliente.
C4	6	Informar a los interesados si se van a utilizar los datos con otras finalidades distintas a las previamente informadas. Recabar el consentimiento previo en caso de que sea necesario.	Abbanza Research Int, S.L. Empresas Cliente.
C5	6	Informar a los interesados si se van a utilizar los datos con otras finalidades distintas a las previamente informadas en lo relativo a toma de decisiones automatizadas.	Empresas Cliente.
S1	3	Controles periódicos de verificación de accesos autorizados. Revisar periódicamente los usuarios y dar de baja aquéllos inactivos.	Empresas Cliente.
S2	3	Controles periódicos de verificación de accesos autorizados. Revisar periódicamente los usuarios y dar de baja aquéllos inactivos.	Empresas Cliente.
ET5	4	Realizar desarrollos que permitan la portabilidad a otros entornos cuando el Cliente lo solicite.	Abbanza Research Int, S.L.

Informe realizado por **HELAS CONSULTORES, S.L.**

En Madrid, a 19 de julio de 2019

07214398B JOSE HELGUERO (R: B83017780)

Firmado digitalmente por 07214398B JOSE HELGUERO (R: B83017780)
Fecha: 2019.07.22 14:29:50 +02'00'