FUNDACION ACOBE
D/Dª HUGO BUSTILLOS GARCIA
C/ VIRGEN DEL SAGRARIO, 19 BAJO DCHA
28026 MADRID MADRID
Tlf.: 913145671

Fecha: 07-02-2024

Asunto: Informe de Verificación del cumplimiento de la Normativa de Protección de Datos de Carácter Personal

Estimado Cliente:

Nos complace remitirle el Informe de Verificación del cumplimiento de la Normativa de Protección de Datos de Carácter Personal de su Organización, confeccionado tras la Verificación de cumplimiento.

Este documento es una evidencia más de la responsabilidad proactiva que acredita su Entidad con respecto a la Normativa de Protección de Datos personales. El referido Informe se estructura de la siguiente manera:

- Objetivo y alcance del Informe
- Plan de trabajo y metodología en la elaboración del Informe
- Resumen ejecutivo, indicando fortalezas y debilidades detectadas, resumiendo las áreas de acción más significativas
- Auditoría de aspectos jurídicos y organizativos del cumplimiento de la Normativa, indicando recomendaciones/valoraciones por cada punto auditado
- Auditoría de aspectos técnicos del sistema de tratamiento de datos, indicando recomendaciones/valoraciones por cada punto auditado

Tenga en cuenta la necesaria revisión del Informe de Verificación por su parte, a fin de darle el curso oportuno de modo que se implementen de manera efectiva las medidas correctoras que en su caso resulten adecuadas.

Aprovechamos para informarle que, añadido al seguimiento previsto a su proyecto de cumplimiento normativo que realizará su Técnico asignado, éste podrá recabar nuevamente su colaboración en caso de haberse detectado la necesidad de actualizar su documentación de Protección de Datos.

Reciba un cordial saludo.

Atentamente,

CARMONA GARCÍA, TERESA

INFORME DE VERIFICACIÓN DEL CUMPLIMIENTO DE LA NORMATIVA DE **PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

FUNDACION ACOBE

Realizado por: **TERESA CARMONA GARCÍA**
Técnico Experto en Protección de Datos
ADEPLUS CONSULTORES S.L.U.
Fecha informe: 19-01-2024

ÍNDICE

OBJETIVO Y ALCANCE

Esta Verificación de cumplimiento del Reglamento General de Protección de Datos de Carácter Personal (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) tiene como objetivo, de una parte, desarrollar el Principio de "Responsabilidad Proactiva" con el que se encuentra comprometido FUNDACION ACOBE , y de otra cumplir con el requisito del artículo 32.1.d) del citado RGPD en relación al establecimiento de: *Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

El alcance de la Verificación son los tratamientos de datos realizados en FUNDACION ACOBE , que se relacionan a continuación:

Tratamiento	Tipo tratamiento	Nivel de Riesgo	Tipo de Riesgo
APOYO ESCOLAR	SEMIAUTOMATIZADO	MEDIO	- Usurpación de identidad o fraude - Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
ASESORAMIENTO LEGAL	SEMIAUTOMATIZADO	MEDIO	- Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no

			incidental p accesorios a categorías especiales de datos - Usurpación de identidad o fraude - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
ORIENTACION LABORAL	SEMIAUTOMATIZADO	MEDIO	- Usurpación de identidad o fraude - Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
CURSOS DE CAPTACION Y APOYO A LA INSERCION SOCIO-LABORAL	SEMIAUTOMATIZADO	MEDIO	- Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Usurpación de identidad o fraude

			- Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
ATENCION SOCIAL	SEMIAUTOMATIZADO	MEDIO	- Usurpación de identidad o fraude - Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
RETORNO VOLUNTARIO	SEMIAUTOMATIZADO	MEDIO	- Usurpación de identidad o fraude - Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad

ACTIVIDADES CULTURALES Y DE TIEMPO LIBRE	SEMIAUTOMATIZADO	MEDIO	- Usurpación de identidad o fraude - Discriminación - Daño Reputacional - Prejuicio económico moral o social significativo para los afectados - Riesgos derivados del tratamiento no incidental p accesorios a categorías especiales de datos - Tratamiento de datos de grupos afectados en situación de especial vulnerabilidad y/o menores de edad
DONACIONES	SEMIAUTOMATIZADO	------	------
PAGINA WEB Y REDES SOCIALES	AUTOMATIZADO	------	------
TRABAJADORES	SEMIAUTOMATIZADO	------	------
VOLUNTARIADO	SEMIAUTOMATIZADO	------	------

Esta Verificación se planifica con carácter anual sin perjuicio de aquéllas que tengan que realizarse con carácter extraordinario por modificaciones sustanciales en el sistema de información de FUNDACION ACOBE .

Como resultado de la Verificación anual, el Informe de auditoría dictamina sobre el grado de cumplimiento de la Normativa, en su caso identifica sus deficiencias y sugiere las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. Asimismo, incluye los aspectos auditados y la metodología, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basan las conclusiones formuladas.

En relación a las primeras actuaciones a llevar a cabo por FUNDACION ACOBE , el Informe se presenta al interlocutor designado con ADEPLUS CONSULTORES S.L.U. que en su caso, deberá

elevarlo a la Dirección de la empresa para que adopte las medidas correctoras adecuadas. Este curso del informe se debe realizar sin perjuicio de la participación de los distintos departamentos con acceso a datos en la parte que les afecte:

- TRABAJADOR SOCIAL
- ABOGACIA
- VOLUNTARIADO
- AREA DE PROYECTOS
- AREA DE ACOGIDA
- PSICOLOGIA
- MONITORES
- TECNICOS ORIENTACION LABORAL
- RESPONSABLE DE FORMACION
- PROFESORA CASTELLANO
- AREA DE COMUNICACION

PLAN DE TRABAJO

Esta Verificación obligada por el Reglamento General de Protección de Datos (RGPD) se ha realizado durante el día 19-01-2024 por parte del Técnico Experto en Protección de Datos: TERESA

CARMONA GARCÍA. Para su realización se han recabado, en su caso, las evidencias oportunas que soportan las consideraciones del Técnico, y se ha entrevistado a las siguientes personas de FUNDACION ACOBE con conocimiento sobre los diferentes tratamientos de datos realizados en la Organización:

INTERLOCUTOR DE FUNDACION ACOBE	PUESTO DE TRABAJO
Ramiro	Gerente

Para la correcta ejecución de la Verificación se han revisado los siguientes aspectos:

A) **Documentación**

- Política de Protección de Datos
- Análisis de Riesgo
- Registro de Actividades de tratamiento
- Normas, procedimientos y registros relativos al cumplimiento del RGPD
- Contrato de Consultoría y Auditoría de la Normativa de Protección de Datos suscrito entre FUNDACION ACOBE y ADEPLUS CONSULTORES S.L.U.
- La página web: www.acobe.org

B) **Normativa Sectorial de aplicación a los tratamientos de datos en FUNDACION ACOBE**

Por su parte, en relación a la legislación sectorial o específica de aplicación a los tratamientos de datos, considerando su impacto en las obligaciones de conservación de datos, la legitimación para el tratamiento de datos y, en general, a los efectos de determinar cómo afecta al sistema de información:

- Normativa aplicable
- Legislación Tributaria
- Legislación Laboral

RESUMEN EJECUTIVO

Identificamos a continuación las fortalezas y las debilidades detectadas en los tratamientos de datos llevados a cabo por FUNDACION ACOBE , resumiendo las áreas de actuación más significativas.

Referencia	FORTALEZAS	DEBILIDADES
Contrato con ADEPLUS CONSULTORES S.L.U.	Asesoría Jurídica en Protección de datos concertada con ADEPLUS CONSULTORES S.L.U. Evaluación de Impacto en Privacidad	
Política de Protección de Datos	Adopción de una Política de Protección de Datos en la Organización Aplicación de los Principios jurídicos relativos al tratamiento de datos	
Registro de Actividades del Tratamiento	Conocimiento por parte de los responsables de la Organización de las medidas técnicas y organizativas de implantación El Registro de Actividades del Tratamiento está actualizado e incorpora los registros preceptivos	
Designación DPD o interlocutor con ADEPLUS CONSULTORES S.L.U.	Establecimiento y asignación de los roles de control para el cumplimiento de la Normativa de Protección de Datos	
Gestión del Personal y Criterios Organizativos	Identificación y caracterización de los distintos departamentos con acceso a datos Conocimiento y claridad en la atribución de obligaciones y responsabilidades al personal en el tratamiento de datos	

	Criterios organizativos de la documentación acordes con las mejores prácticas de confidencialidad y ejercicio de derechos de los interesados	
Auditoría e Indicadores Críticos	Los indicadores críticos del cumplimiento de la Normativa de Protección de datos son adecuadamente gestionados: Violaciones de seguridad y ejercicio de derechos ARSLOP Cumplimiento del principio de responsabilidad proactiva en cuanto a la mejora continua de los sistemas de tratamientos de datos	
Protección de las Instalaciones	Protección de equipos de trabajo destinados al tratamiento de datos	Ausencia de aplicación de medidas de seguridad físicas sobre las instalaciones
Adquisición de Productos		La gestión de los proveedores TIC no contribuye a la seguridad del sistema de información
Integridad y Actualización del sistema	Implantación de medidas que aportan garantías en el sistema de tratamiento de datos El grado de protección de las telecomunicaciones alcanza un nivel robusto	
Protección de la Información	El proceso de copias de seguridad, dota de una mayor resiliencia al sistema de tratamiento de datos Los mecanismos de identificación y autenticación contribuyen al mantenimiento de la confidencialidad en el acceso a datos al sistema de tratamiento	

	Cumplimiento de los principios de conservación y supresión de datos de carácter personal	

A partir de este Resumen Ejecutivo, para una comprensión ampliada del análisis realizado revise cada uno de los aspectos jurídicos, organizativos y técnicos detallados a continuación en el Informe, tomando como referencia la indicada en el cuadro superior.

ASPECTOS JURÍDICOS Y ORGANIZATIVOS

Los aspectos jurídicos y organizativos del Cumplimiento de la Normativa de Protección de Datos de Carácter Personal parten del principio de "Responsabilidad proactiva" consagrado en el artículo 5.2 RGPD. Concretan en particular lo establecido en los artículos señalados a continuación:

1. Política de Protección de Datos: Artículos 5-11, y 24 RGPD.
2. Registro de Actividades del Tratamiento: Artículo 30 RGPD.
3. Designación del DPD o interlocutor con ADEPLUS CONSULTORES S.L.U.: Artículo 37 RGPD.
4. Gestión de personal y criterios organizativos: Artículos de 15-22, 28, y 39 RGPD.
5. Auditoría e indicadores críticos: Artículos 15-22, 32, y 33 RGPD.

Si bien podrá apreciarse que la verificación del Técnico en este apartado resulta muy pormenorizada, del propio principio de "Responsabilidad proactiva" se infiere que no debe entenderse estos aspectos como un *checklist* desligado de los procesos de mejora continua de la Organización, del compromiso de la Dirección y de una auténtica preocupación de FUNDACION ACOBE por un cumplimiento real de la Normativa alineado con sus objetivos de negocio, al tiempo que respetuoso con los derechos y libertades de los interesados.

La Verificación se fundamenta en los hallazgos realizados en el transcurso de la Auditoría, que una vez analizados permiten realizar una valoración por parte del Auditor, que se acompaña finalizando cada apartado.

1. POLÍTICA DE PROTECCIÓN DE DATOS

La Normativa de Protección de Datos establece los Principios que deben regir los tratamientos de datos que se dan en la Organización. Este cumplimiento, alineado con el principio de "Responsabilidad Proactiva", determina la necesidad de implementar una Política de protección de datos a fin de poder demostrar la conformidad con la Norma: "se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos".

Se Verifica a continuación tanto la adopción íntegra de la Política por parte de FUNDACION ACOBE , que a su vez está relacionado con otros elementos objeto de verificación.

- **Comprobación del contenido y alcance de la Política de Protección de Datos**

CONTROL	VERIFICACIÓN	HALLAZGO
Dispone de una Política de Protección de Datos escrita	Satisfactorio	La Política de Protección de datos está impresa o guardada en un formato electrónico en su versión 1.0.
Dicha Política de Protección de datos ha sido aprobada al máximo nivel de la Organización	Satisfactorio	La Política de Protección de datos ha sido aprobada y firmada por la Dirección.
La Política de Protección de datos establece los Principios, Ámbito de aplicación y roles de atribución de responsabilidades	Satisfactorio	La Política de Protección de datos ha sido revisada e incluye el rol de control establecido en la Organización.
La Política de Protección de datos está accesible para los grupos de interés de la Organización	Satisfactorio	La Política de Protección de datos ha sido publicada y está accesible para los grupos de interés de la Organización.
Consta de manera documentada la adhesión de los empleados a la Política de Protección de datos	Satisfactorio	Los trabajadores se han adherido a la Política de Protección de datos de la Organización, y este hecho consta de manera documentada.

- **Implementación de Principios en los tratamientos de datos**

CONTROL	VERIFICACIÓN	HALLAZGO
En la Organización se dan tratamientos de datos basados en el consentimiento, por lo que se	No Aplica	Este requisito no aplica en la Organización

cuenta con una declaración o una clara acción afirmativa del interesado para el tratamiento de sus datos personales		
Los tratamientos de categorías especiales de datos realizados en su Organización basados en el consentimiento cuentan con la obtención del consentimiento explícito del interesado	No Aplica	Este requisito no aplica en la Organización
En el tratamiento de datos de los menores de 14 años, se cuenta con el consentimiento de sus padres o representantes	Satisfactorio	El tratamiento de datos de menores es lícito al recabar autorización o el propio consentimiento del representante legal del menor.
Los tratamientos de datos de la Organización basados en una obligación legal están amparados por una norma con rango de Ley	Satisfactorio	Los tratamientos de datos basados en una obligación legal están convenientemente trazados con una Ley.
Los tratamientos de datos con fines de mercadotecnia directa cuentan con una legitimación adecuada	Satisfactorio	La Organización aplica correctamente la legitimación para el tratamiento de datos con fines de mercadotecnia directa.
En su Organización se dan tratamientos de datos basados en un Interés Público, derivados exclusivamente de su condición de Administración Pública	No Aplica	Este requisito no aplica en la Organización
Su Organización es responsable de datos que no provienen directamente del interesado. Sobre estos tratamientos informa a los afectados en la primera comunicación, o en cualquier caso antes de un mes desde la incorporación de datos al sistema	No Aplica	Este requisito no aplica en la Organización
La Organización ha implantado mecanismos de información en todos los medios de captura de datos	Satisfactorio	Se han incluido las cláusulas y mecanismos de información al interesado sobre tratamientos de datos en los distintos canales de entrada de datos, con el contenido establecido en Normativa.

Se han revisado los distintos medios de captura de datos para cumplir con el principio de minimización de datos	Satisfactorio	En cumplimiento del principio de "minimización de datos" no se están recabando datos para los que no exista una finalidad legítima.
Los tratamientos con fines de Videovigilancia que se dan en su Organización, son en todo caso informados mediante la colocación del cartel de señalización de zona videovigilada en un lugar visible	No Aplica	Este requisito no aplica en la Organización
La página web dispone de un Aviso Legal, y de cookies en su caso	Satisfactorio	La página web cuenta con el aviso legal establecido en la Normativa sobre Servicios de la Sociedad de la Información.

2. REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

El Registro de Actividades del Tratamiento (RAT) concreta otra obligación derivada de la aplicación del Principio de "Responsabilidad Proactiva" establecido en la Normativa: "Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información (...)".

En el transcurso de la verificación de este hito, el Auditor parte de la comprobación tanto de la existencia de este documento en su Área Privada de Cliente, así como la posibilidad de acceso al documento por parte de FUNDACION ACOBE .

El objetivo de la revisión del Registro de Actividades del Tratamiento (RAT) tiene un doble enfoque, que abarca por un lado la verificación del contenido completo y actualizado del documento, como la confirmación de su efectividad en cuanto a su difusión a los departamentos que se ven afectados por él.

- **Comprobación del contenido y alcance del Registro de Actividades del Tratamiento**

CONTROL	VERIFICACIÓN	HALLAZGO
El Responsable cuenta con un Registro de Actividades del	Satisfactorio	El Responsable cuenta y ha accedido a su Registro de actividades de tratamiento en

tratamiento con el contenido establecido en el artículo 30.1 del Reglamento General de Protección de Datos		una versión con el contenido establecido en la Normativa.
El Registro de Actividades del Tratamiento está actualizado a fecha de esta Verificación	Satisfactorio	El Registro de Actividades del Tratamiento está actualizado y es acorde a los tratamientos de datos verificados a fecha de esta Auditoría.
Se incluyen en el Registro de Actividades del Tratamiento los contratos de Encargado del tratamiento firmados con todos los proveedores de servicio con acceso a datos	Satisfactorio	Se encuentran adjuntos al Registro de Actividades del tratamiento, o como parte de él, los Contratos de Encargado del tratamiento con los proveedores de servicio con acceso a datos.
En su caso, se incluyen en el Registro de Actividades del Tratamiento los contratos de Encargado del tratamiento firmados con aquellos terceros por cuya cuenta se traten datos	Satisfactorio	Se encuentran adjuntos al Registro de Actividades del tratamiento, o como parte de él, los Contratos de Encargado del tratamiento con los Clientes (Empresa) por cuya cuenta se tratan datos.

❖ **Revisión de las Normas relacionadas con el Registro de Actividades del Tratamiento**

CONTROL	VERIFICACIÓN	HALLAZGO
Existe, como parte del Registro de Actividades del Tratamiento o aparte de éste, un Análisis de Riesgo actualizado	Satisfactorio	Se ha realizado un Análisis documentado completo, sobre los riesgos derivados del tratamiento de datos en la Organización que incluye una valoración de la necesidad de realizar una Evaluación de Impacto, en su caso. Y se encuentra actualizado.
Las medidas organizativas y técnicas necesarias para el cumplimiento de la Normativa son conocidas por quienes deben asignar las responsabilidades	Satisfactorio	Consta la comunicación de las medidas de necesaria implantación para mitigar los riesgos derivados de los tratamientos de datos entre quienes tienen que coordinar y/o ejecutar su implantación.
El personal en contacto con el sistema de información de la Organización tiene acceso a los formatos de comunicación de "Violaciones de datos"	Satisfactorio	Se han tomado medidas para que las posibles "Violaciones de seguridad" sean notificadas en un formato estandarizado que permita el registro de todos los elementos necesarios para la valoración preceptiva sobre su gravedad y

		consecuencias.
Se verifica que el personal destinado a ello tenga acceso a los formatos de ejercicio de Derechos ARSLOP	Satisfactorio	Se ha tomado una medida fundamental para que los posibles ejercicios de Derechos sean notificados en un formato estandarizado que permita la adecuada atención a la solicitud del interesado o su representante.
Sobre los tratamientos con "riesgo alto" para la seguridad y/o los derechos y libertades de los interesados se ha realizado la Evaluación de Impacto en Privacidad preceptiva	No Aplica	Este requisito no aplica en la Organización

3. DESIGNACIÓN DE DELEGADO DE PROTECCIÓN DE DATOS O INTERLOCUTOR CON ADEPLUS

La Normativa de Protección de Datos establece la obligación de contar con un Delegado de Protección de datos en determinados supuestos, asociados a un mayor nivel de riesgo en los tratamientos de datos. Este rol de control conjuga el principio de “Responsabilidad proactiva” con el de “Enfoque de Riesgo”.

La designación de esta figura, con las funciones atribuidas en el art. 39 del RGPD, también puede realizarse de manera voluntaria siempre que medie la preceptiva comunicación a la Agencia Española de Protección de Datos y se den el resto de requisitos.

En la Verificación se analiza la posición de esta figura en FUNDACION ACOBE , así como en su defecto la adecuada interlocución con ADEPLUS CONSULTORES S.L.U., como Consultora especializada, del Responsable designado:

CONTROL	VERIFICACIÓN	HALLAZGO
Se ha analizado la necesidad de contar con un Delegado de Protección de Datos, y se ha actuado en consecuencia	Satisfactorio	La Organización está al tanto de las exigencias de nombramiento de Delegado de Protección de Datos en determinados supuestos y ha actuado conforme el criterio de "Responsabilidad proactiva".
El Coordinador designado en la Organización es proactivo en la	Satisfactorio	Se han notificado a la consultora encargada las modificaciones en los

comunicación a Adeplus Consultores de las novedades o cambios sustanciales en los tratamientos de datos		tratamientos de datos que deben ser registradas. Sin perjuicio de otras comunicaciones relevantes.

4. GESTIÓN DE PERSONAL Y CRITERIOS ORGANIZATIVOS

La Responsabilidad Proactiva de la Organización pasa por la involucración de todo el personal que participa en los tratamientos de datos en la Política de Protección de datos de la Entidad, y en la concreción de ésta en normas conocidas y asumidas en el conjunto de FUNDACION ACOBE .

La verificación de este objetivo debe basarse en registros documentados de formación en materia de Protección de datos al personal sobre los elementos mencionados.

Abundando en el Principio de "Responsabilidad proactiva", resulta crítica la creación de una cultura de Protección de datos en la Organización que genere inercias alineadas con la obligación general del Responsable de establecer una *Protección de Datos desde el diseño y por defecto*, y que promueva la contribución individual del trabajador al cumplimiento global de la Organización, y en sentido contrario una responsabilidad disciplinaria por los incumplimientos.

- **Departamentos de FUNDACION ACOBE involucrados en las distintas etapas de los tratamientos de datos**

CONTROL	VERIFICACIÓN	HALLAZGO
Se han identificado los distintos Departamentos con acceso a datos, incorporando su participación en el "ciclo de vida del dato"	Satisfactorio	Consta la información sobre Departamentos con acceso a datos, de manera actualizada, en el Registro de Actividades del tratamiento.
Los accesos de cada departamento están caracterizados por los principios de "necesidad de saber" y "mínimos privilegios" y son atribuidos sólo por personal autorizado	Satisfactorio	Sólo los Departamentos y sus integrantes, con participación en un tratamiento acceden a éste, y con la mínima extensión necesaria para el desempeño de su trabajo. Los permisos son establecidos por la Dirección.
Se ha elaborado un plan de contingencia que permite a la organización reaccionar ante las	No Aplica	Este requisito no aplica en la Organización

amenazas a los tratamientos con riesgo alto		

❖ **Información al personal de FUNDACION ACOBE sobre sus deberes y responsabilidades inherentes al tratamiento de datos personales**

CONTROL	VERIFICACIÓN	HALLAZGO
Se ha proporcionado formación de sensibilización a todo el personal con acceso a datos sobre política de protección de datos, confidencialidad y procedimientos	Satisfactorio	Consta documentada la participación del personal con acceso a datos en una "Formación de sensibilización en Protección de datos".
El personal es consciente de las consecuencias disciplinarias y de tipo legal que puede conllevar la contravención de la política de seguridad	Satisfactorio	El personal conoce las consecuencias de la contravención de la política de seguridad de la Organización.
La exigencia de formación se extiende a personal no vinculado al responsable por una relación laboral estable	Satisfactorio	También el personal voluntario, en prácticas, a los que se permite el acceso al sistema de información a realizado la formación de sensibilización oportuna.
El personal con acceso a datos ha formalizado los oportunos Acuerdos de confidencialidad	Satisfactorio	Las garantías de confidencialidad que ofrece el personal están reforzadas mediante un compromiso de confidencialidad.
Existe un procedimiento escrito para el alta, modificación o supresión de autorizaciones de acceso al sistema de información	Satisfactorio	La organización tiene claramente definido y documentado un procedimiento de modificación o establecimiento de permisos de acceso.
Se aplica un proceso de clasificación de información que permite discernir el grado de confidencialidad de la documentación	Satisfactorio	La documentación es clasificada indicando de manera expresa su grado de confidencialidad.
Los criterios de archivo permiten la localización y consulta a información personal de modo que se garantice la capacidad de respuesta ante ejercicio de	Satisfactorio	Los criterios de archivo están convenientemente trazados con el cumplimiento de la Normativa.

Derechos ARSLOP		

5. AUDITORÍA E INDICADORES CRÍTICOS

A resultas de la necesidad de establecer un proceso de comprobación de la idoneidad de lo ejecutado y planificado con los requisitos de la Organización para el cumplimiento global de esta Normativa, se establece en el artículo 32.1.d) RGPD la obligación de contar con *un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*.

En este sentido, para que los sistemas de información estén sometidos a procesos de mejora continua, se incluye como parte de éstos la realización de Verificaciones periódicas, y además se revisan en este apartado algunos indicares críticos por su estrecha relación con el régimen sancionador establecido en la Normativa.

- **Realización de la Verificación obligatoria**

CONTROL	VERIFICACIÓN	HALLAZGO
Se han realizado Auditorías/Verificaciones dentro del plazo anual establecido	Satisfactorio	La Organización tiene implementado un proceso de Verificación externa del cumplimiento de la Normativa de protección de datos, que se ejecuta de manera anual o cada vez que haya cambios sustanciales en el sistema de información.
En su caso se han solventado las deficiencias documentadas en Informes de Verificación anteriores	Satisfactorio	La Organización tienen incorporado en sus procesos de mejora continua la corrección de deficiencias en materia de Protección de datos.

- **Revisión de indicadores críticos relativos a "Violaciones de datos personales", Ejercicios de Derechos ARSLOP y Transferencias Internacionales de Datos**

CONTROL	VERIFICACIÓN	HALLAZGO
Han ocurrido "Violaciones de seguridad" de datos de carácter personal que han sido convenientemente documentadas, valoradas en cuanto a su gravedad, y comunicadas en su caso	Satisfactorio	Pese a no haberse producido ninguna violación de seguridad, la empresa cuenta con el procedimiento de "Notificación de violaciones de seguridad".

Se han producido solicitudes de ejercicio de Derechos ARSLOP, y éstas han sido atendidas según Normativa en relación a su plazo de respuesta, contenido, etc.	Satisfactorio	Pese a no haberse efectuado por parte de los interesados el ejercicio de ningún Derecho ARSLOP, la empresa cuenta con los modelos correspondientes para que los interesados puedan ejercer los mismos.
En relación a las Transferencias internacionales que realiza su Organiación, éstas han sido revisadas para asegurar que cumplen con todos los requisitos legales	No Aplica	Este requisito no aplica en la Organización

ASPECTOS TÉCNICOS

Los aspectos técnicos relativos al cumplimiento de la Normativa de Protección de Datos de Carácter Personal se basan en el Enfoque de Riesgo al que obliga el cumplimiento de la Normativa en el artículo 24.1 RGPD “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas (...)”.

A resultas de este enfoque se realiza un Análisis de Riesgo que determina las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado, extremo que será objeto de verificación a través de los siguientes apartados:

6. Protección de instalaciones
7. Adquisición de productos
8. Integridad y actualización del sistema
9. Protección de la información

La Verificación se fundamenta en los hallazgos realizados en el transcurso de la Auditoría, que una vez analizados permiten realizar una valoración por parte del Auditor, que se acompaña finalizando cada apartado.

6. PROTECCIÓN DE INSTALACIONES

Las amenazas a la integridad, confidencialidad y disponibilidad de la información, así como, relacionadas con estas, la protección de los derechos y libertades de los interesados en relación a sus datos, requiere la protección del sistema de información que debe sustentarse en un Enfoque de riesgo.

Esta protección implica la adopción tanto de medidas de seguridad físicas como lógicas. En este apartado se verifica la eficacia de la protección de la seguridad física de los locales de tratamiento, así como la seguridad lógica de los equipos destinados a ello.

Para la Verificación de este apartado se constata inicialmente la existencia de un único centro de trabajo.

- **Protección de instalaciones de FUNDACION ACOBE que alojan el sistema de información**

CONTROL	VERIFICACIÓN	HALLAZGO
Los locales cuentan con protección ante amenazas (incendio, inundación, robo, ...)	No satisfactorio	Las instalaciones que alojan el sistema de información están carentes de medidas de seguridad física cuando el local está cerrado.
El equipamiento informático ha sido instalado en áreas separadas, específicas para su función	Satisfactorio	Los servidores y mobiliario de almacenamiento de información se encuentran en estancias que reúnen condiciones de seguridad en cuanto a su ubicación en zonas acondicionadas, separadas de las de común acceso.
La zona en que se ubica el sistema de información está señalizada como "Acceso restringido"	Satisfactorio	Se ponen medidas para evitar acceso no autorizados al sistema de información, que no sean malintencionados, al tiempo que se contribuye a la creación de una cultura de seguridad de la información en la empresa.
Respecto a dichas áreas separadas, se controlan y registran los accesos	Satisfactorio	El acceso al sistema de almacenamiento está restringido a personal autorizado, y se documentan los accesos.
Se disponen de un mecanismo de control de acceso robusto a las estancias donde hay	Satisfactorio	Las estancias donde se alojan servidores o mobiliario de archivo están securizadas con un mecanismo de control de acceso y/o

equipamiento que forme parte del sistema de información		cerradura con llave.
Los archivadores u otros elementos de almacenamiento de documentación cuentan con llave u otro dispositivo de cierre equivalente	Satisfactorio	El mobiliario de almacenamiento cuenta con cerradura o mecanismo equivalente.
Se toman las medidas adecuadas en el traslado de documentación para evitar la sustracción, perdida o acceso indebido durante su transporte	Satisfactorio	El traslado de documentación se realiza con medidas que impiden el acceso o la manipulación.

- **Protección de equipos**

CONTROL	VERIFICACIÓN	HALLAZGO
Se exige que los puestos de trabajo permanezcan despejados, sin más información sobre la mesa de trabajo que el requerido para la actividad que se está realizando en cada momento. Por su parte el ordenador se bloquea al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso	Satisfactorio	La Organización adopta una Política de mesas y pantallas limpias.
Existe y se mantiene un inventario de soportes y ordenadores	Satisfactorio	Se mantiene un inventario actualizado de los soportes como base para su adecuada gestión segura.
Los ordenadores y soportes se encuentran etiquetados	Satisfactorio	Los soportes de información se encuentran etiquetados de modo que se de trazabilidad al inventario y permitan su identificación.
El etiquetado de los ordenadores y soportes es confidencial: no revela la información contenida	Satisfactorio	El etiquetado de los soportes cuenta con un sistema de etiquetado confidencial.
La información almacenada en ordenadores portátiles y soportes se encuentra cifrada	Satisfactorio	Los dispositivos de almacenamiento de información que permiten el tratamiento de datos fuera de las instalaciones están

		cifrados.
Los ordenadores y soportes reutilizados para otra información o liberados para un segundo uso son borrados de forma segura	Satisfactorio	Se toman medidas para impedir el acceso no autorizado a la información contenida en los soportes en caso de reasignación o reutilización.

ÁREAS DE MEJORA

Tras analizar los ítems, este Auditor ha detectado las siguientes áreas de mejora en la protección de las instalaciones de la Organización:

- La protección de las instalaciones e infraestructuras no está suficientemente garantizada, lo que afecta a la capacidad de la Organización para garantizar la confidencialidad, integridad, disponibilidad, y resiliencia permanentes de los sistemas y servicios de tratamiento (art. 32.1.b del RGPD).

7. ADQUISICIÓN DE PRODUCTOS

Los principios de protección de datos desde el diseño y por defecto requieren de un adecuado proceso de adquisición de material informático: productos, servicios y aplicaciones, ya que resulta una medida fundamental para permitir el cumplimiento de las obligaciones de protección de datos, tal y como establece el Considerando 78 del RGPD.

En este apartado, se procede a valorar los criterios en la adquisición de las herramientas de *hardware* y *software* identificadas por su involucración en los distintos tratamientos de datos para analizar a continuación el proceso de adquisición, encargo y en su caso renovación de productos.

CONTROL	VERIFICACIÓN	HALLAZGO
Se valora positivamente en la adquisición productos TIC que tengan certificada las funcionalidades de seguridad	Satisfactorio	La adquisición y renovación de material informático atiende, entre otros, a criterios de calidad y seguridad.
Sólo se adquieren productos de software debidamente licenciados que permitan actualizaciones	Satisfactorio	Los criterios de adquisición de productos de software forman parte de la estrategia de seguridad y cumplimiento legal de la Organización.

Se verifica que las empresas que realicen servicios de instalación o mantenimiento de equipos o sistemas de telecomunicaciones están registradas en el "Registro de instaladores" al efecto	Satisfactorio	La selección de proveedores TIC está alineada con las mejores prácticas en materia de seguridad.
Existe un inventario de licencias del software que trata datos con algún riesgo	No satisfactorio	No existe un control sobre el software que se incorpora a los tratamientos de datos con riesgo.
Se constata la prohibición de instalación y uso de hardware o software no autorizado	Satisfactorio	Consta la prohibición al personal de instalar software que pueda afectar a la seguridad del sistema.
La instalación de software se realiza de modo que proporciona la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcanza ninguna otra funcionalidad adicional	Satisfactorio	La instalación de software se realiza siguiendo el principio de "seguridad por defecto".
En la adquisición de mobiliario destinado al almacenamiento de información se valora que ofrezca un entorno seguro de trabajo	Satisfactorio	La adquisición de mobiliario destinado al almacenamiento de información tiene en cuenta las prestaciones en materia de seguridad y confidencialidad.

ÁREAS DE MEJORA

Tras analizar los ítems, este Auditor ha detectado las siguientes áreas de mejora en la adquisición de productos que pueden alinearse con el cumplimiento de la Normativa sobre protección de la propiedad intelectual:

- Debe considerarse aplicar un tratamiento específico a los proveedores TIC por la incidencia que su actividad puede tener en una adecuada gestión de la seguridad de la información en la Organización.

8. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

A resultas del Análisis de riesgo, deben determinarse las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado, que según el artículo 32 RGPD podrán incluir, entre otras:

a) *la seudonimización y el cifrado de datos personales;*
b) *la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
c) *la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; (...)*

Los sistemas de información están expuestos a amenazas que generan riesgos para los datos de carácter personal, por lo que se verificado la adopción y eficacia de los principales estándares en relación a la integridad y actualización del sistema.

- **Integridad y actualización del sistema**

CONTROL	VERIFICACIÓN	HALLAZGO
La Organización cuenta con antivirus actualizados	Satisfactorio	La eficacia de la protección antivirus es reforzada mediante la actualización de los mismos.
Los tratamientos de categorías especiales de datos aplican medidas de seudonimización	Satisfactorio	Los riesgos derivados del tratamiento de categorías especiales de datos se reducen con la aplicación de técnicas de seudonimización.
Los tratamientos de categorías especiales de datos aplican medidas de cifrado	Satisfactorio	La seguridad de los tratamientos de categorías especiales de datos se refuerza con técnicas de cifrado.
En el sistema operativo y demás software empleado en a Organización se instalan actualizaciones oficiales cada vez que éstas están disponibles	Satisfactorio	Los equipos de la organización acceden a "parches" de seguridad del fabricante a través de las actualizaciones del software.
El sistema de información se monitorea para detectar posibles situaciones sospechosas	Satisfactorio	La monitorización del sistema permite detectar patrones anormales.
Se realizan pruebas de intrusión en el sistema	Satisfactorio	La eficacia de las medidas de protección del sistema son verificadas.
Se configuran, revisan y mantienen "logs" de acceso al sistema	Satisfactorio	Se cuenta con medios de verificación de los accesos al sistema que son revisados periódicamente.

❖ **Protección de las Telecomunicaciones**

CONTROL	VERIFICACIÓN	HALLAZGO
El sistema de información de la Organización cuenta con un cortafuegos que separa la red interna del exterior	Satisfactorio	Las telecomunicaciones de la empresa están protegidas por un firewall.
Respecto de dicho cortafuegos se dispone de sistemas redundantes	Satisfactorio	La arquitectura del sistema reaccionaría al fallo de un firewall.
La conexión con sitios web externo está restringida a entornos securizados con protocolo seguro (SSL o TLS)	Satisfactorio	Las telecomunicaciones a través de aplicativos on-line se realizan sobre aplicaciones securizadas con protocolo SSL.
Los sitios web de su Organización que permiten tratamiento de datos están securizados con protocolo seguro	Satisfactorio	La captura y/o puesta a disposición de información a través de aplicaciones propias está securizada con protocolo SSL.
Las comunicaciones que incluyen categorías especiales de datos a terceros se realizan por protocolo seguro y/o mail cifrado	Satisfactorio	Las comunicaciones de datos a terceros se realizan de manera cifrada.

9. PROTECCIÓN DE LA INFORMACIÓN

Las garantías de la Organización en cuanto a la prevención y capacidad de respuesta ante la destrucción, pérdida o alteración accidental o ilícita de datos personales, exige certezas en cuanto a *la capacidad de restaurar la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico.*

Derivada de esta exigencia sumada así como de las otras inherentes a la aplicación del artículo 31 RGPD sobre seguridad del tratamiento, se verifican en este apartado la eficacia del sistema de copias de seguridad, de los mecanismos de identificación y autenticación, así como de la supresión de datos.

❖ **Copias de seguridad**

CONTROL	VERIFICACIÓN	HALLAZGO
Se realizan copias de respaldo que limitan el riesgo de destrucción, pérdida o alteración ilícita de datos personales	Satisfactorio	Se ha configurado un sistema de copia de seguridad que contribuye a la resiliencia y mantenimiento de la disponibilidad de los tratamientos de datos.

Respecto de dichas copias, se realizan con periodicidad al menos semanal	Satisfactorio	La periodicidad de la copia es como mínimo semanal.
Su Organización ha definido una copia de seguridad diaria para los tratamientos de datos con más riesgo. Este proceso es desasistido	Satisfactorio	Se garantiza la periodicidad diaria de la copia.
El alcance de las copias de seguridad es de todo el sistema de información que trata datos de carácter personal, a este respecto se verifica con periodicidad como mínimo semestral el alcance de la copia	Satisfactorio	Se verifica que la protección de la información mediante copia de seguridad se extiende a todos los tratamientos de datos.
Las copias disfrutan de la misma seguridad que los datos originales en lo que se refiere a permisos de acceso y cifrado, y autorización para recuperación de datos	Satisfactorio	Las copias de seguridad incorporan medidas tendentes a evitar accesos no autorizados.
Las copias de seguridad se conservan en un lugar seguro, diferente al de los equipos que los tratan	Satisfactorio	Las copias de seguridad se configuran como un auténtico sistema de respaldo ante incidentes físicos.
Se realizan pruebas de restauración de datos que verifican la capacidad de restaurar la información en caso de incidente, y en su caso se anotan los procesos de recuperación de datos	Satisfactorio	Se verifica y queda documentada la resiliencia del sistema en cuanto a su capacidad para restaurar información.

- **Identificación y autenticación**

CONTROL	VERIFICACIÓN	HALLAZGO
El acceso al sistema de información precisa de identificación y autenticación del usuario de manera personalizada	Satisfactorio	El acceso al sistema de información está protegido con un sistema de usuario y contraseña, o equivalente. Relacionado con una lista actualizada de usuarios y permisos de acceso.
Existe un procedimiento seguro de asignación, custodia y	Satisfactorio	La eficacia del sistema de identificación y autenticación se refuerza con un

distribución de contraseñas		procedimiento seguro que reduce el riesgo de accesos no autorizados.
Se realizan cambios periódicos de la contraseña, como mínimo anualmente	Satisfactorio	Las contraseñas son sustituidas por otras manteniendo los mismos criterios de seguridad.
El sistema de identificación y autenticación establece un límite de intentos reiterados de accesos no autorizados no superior a 3	Satisfactorio	El sistema de identificación y autenticación se configura con medidas adicionales para proteger la confidencialidad.
El sistema de identificación y autenticación aplica a personal ajeno con acceso al sistema de información	Satisfactorio	Se aplican los mismo protocolos de seguridad en el acceso al sistema para personal ajeno.

- **Supresión / Borrado de datos**

CONTROL	VERIFICACIÓN	HALLAZGO
Las aplicaciones cuentan con opciones usables de borrado de registros	Satisfactorio	El sistema de información está alineado con el cumplimiento de obligaciones de supresión/borrado de datos personales.
Periódicamente se revisan los registros para eliminar aquellos cuyo plazo de conservación ha caducado	Satisfactorio	Se adoptan medidas organizativas que permiten asegurar el cumplimiento de obligaciones de supresión/borrado de datos.
La documentación en papel se destruye de modo que queda completamente inutilizada	Satisfactorio	La destrucción de documentación es eficaz por cuanto no permite la recuperación de la información.
La gestión del Canal ético/denuncias es acorde a la Normativa en relación a la conservación y destrucción de registros	No Aplica	Este requisito no aplica en la Organización
Las redes wifi utilizadas en el entorno de trabajo se encuentran securizadas	Satisfactorio	Los accesos a la red wifi están securizados y se monitorizan.

NOTA FINAL

El presente Informe refleja su implicación en el cumplimiento de la Normativa de Protección de datos. Considérelo como una verdadera herramienta de valor orientada a asegurar el correcto tratamiento de datos realizado por su Organización, y no sólo como un medio de acreditación de su diligencia debida (responsabilidad proactiva) en este ámbito.

Desde ADEPLUS CONSULTORES S.L.U. seguiremos trabajando con Vd. en el cumplimiento de la normativa de Protección de Datos dentro de su Organización siguiendo la planificación prevista. En cualquier caso, nos mantenemos a su disposición para seguir asesorándole en materia de Protección de Datos.