INFORME DE AUDITORIA EN EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS:

"AMICA Y SUS CENTROS ESPECIALES DE EMPLEO”

OBJETO DE LA AUDITORIA

El presente documento tiene por objeto comprobar el grado de adecuación de la entidad a la normativa en protección de Datos y a la Ley Orgánica 3/2018 de 5 de Diciembre de protección de datos personales y Garantía de los Derechos Digitales y al Reglamento 679/2016 de 27 de Abril.

El objetivo final de la auditoria es verificar el grado de adecuación de la entidad a las medidas y controles de la normativa en Protección de Datos, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias. A su vez, incluye los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los puntos básicos a revisar en este documento:

- **Aspecto Técnico:** se revisa el cumplimiento de las medidas de seguridad que deben reunir los tratamientos de datos.

- **Aspecto Organizativo:** se revisan los procedimientos normativos y reglas de seguridad elaborados e implantados por la entidad.

- **Aspecto Jurídico:** se revisa la tipología de los datos almacenados en los sistemas de información y aplicaciones informáticas, y se realiza un análisis de riesgos y se determina si la entidad debe de contar con Evaluaciones de impacto de algunos de los tratamientos que realiza y con un Delegado de protección de datos.

FASES EN LA REALIZACIÓN DE LA AUDITORÍA

La auditoría y el listado de cumplimiento normativo se han realizado con visitas presenciales del auditor que ha constado de las siguientes fases:

1. Conocimiento genérico de la entidad, su ámbito de negocio, los sistemas de información de que disponen, su estructura administrativa y el organigrama de sus trabajadores, sus relaciones con organismos oficiales, asociaciones, instituciones y empresas.
2. Elaboración de un programa de trabajo en el que se detallan las actividades o tareas a auditar, teniendo para ello en cuenta, por un lado, los requisitos de revisión impuestos por el Reglamento en relación con la auditoría, y por el otro, el ámbito de negocio y sistemas de la entidad.
3. Realización del trabajo de campo, esto es, la revisión práctica de las actividades incluidas en el plan de trabajo.
4. Análisis de los puntos débiles y obtención de conclusiones y recomendaciones.
5. Elaboración del informe.

PLAN DE TRABAJO

A partir del hecho de que la auditoría debe verificar el cumplimiento del Reglamento y la normativa de Protección de Datos, el Plan de Trabajo deberá incluir específicamente la comprobación de todos los artículos de aquel que sean de aplicación a tenor del tipo de tratamientos de que disponga Amica y sus centros especiales de empleo.

Para la realización organizada de esta auditoría se ha preparado una tabla de control o de "checklist" basada en alguno de los modelos propuestos por la Agencia Española de protección de datos y desarrollada de manera independiente.

A continuación, se incluye la tabla "checklist" de los puntos auditados de las áreas anteriormente mencionadas, así como los resultados obtenidos para cada apartado.

1.- PRINCIPIOS RELATIVOS AL TRATAMIENTO

2.- LICITUD DEL TRATAMIENTO

3.- CONDICIONES PARA EL CONSENTIMIENTO

4.- CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

5.- TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS

6.- TRATAMIENTOS RELATIVOS A CONDENAS E INFRACCIONES PENALES

7.- TRATAMIENTOS QUE NO REQUIEREN IDENTIFICACIÓN

8.- DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN

9.- DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO

10.- DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS NO SE OBTIENEN DEL INTERESADO

11.- DERECHOS DEL INTERESADO:

a. DERECHO DE ACCESO

b. DERECHO DE RECTIFICACIÓN

c. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)

d. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

CONCLUSIONES FINALES

Una vez realizada la auditoría en materia de protección de datos de Amica y sus centros especiales de empleo y verificado el cumplimiento de todos los ítems detallados con anterioridad y basándonos en el nivel de cumplimiento en los diversos apartados comprobados:

CERTIFICAMOS

QUE SE HA REALIZADO:

- ✓ Identificación de las Actividades de Tratamiento realizadas en tanto en calidad de Responsable, como de Encargado del Tratamiento, así como la elaboración del Registro de Actividades del Tratamiento, conforme indica el art. 30 del RGPD. Se han tenido en consideración los tratamientos para terceros.
- ✓ Revisión de los consentimientos para que sean expresos y en todo caso legitimación de los tratamientos basada en las otras circunstancias de licitud del art. 6.1del RGPD.
- ✓ Adaptación de las cláusulas de información a los requisitos de los arts. 13 y 14 del RGPD, para informar en todos los tratamientos de datos de:
    - La identidad del Responsable del Tratamiento.
    - Los datos de contacto del Responsable del Tratamiento.
    - La finalidad del tratamiento.
    - La legitimación para el tratamiento.
    - Los destinatarios o las categorías de destinatarios de los datos personales.
    - Las transferencias de datos personales a terceros países previstas.
    - Los plazos de conservación previstos.
    - Los derechos que asisten al interesado y la forma de ejercerlos.
    - El derecho a reclamar ante la AEPD.
- ✓ Revisión de la información solicitada, así como la recibida, para cumplir con el principio de minimización y de privacidad por defecto (art. 25 RGPD)
- ✓ Determinación de los plazos de conservación, teniendo en consideración los plazos mínimos de conservación marcados por la normativa que resulta de aplicación.
- ✓ Concienciación y comunicación a los trabajadores sobre la observancia de los principios recogidos en el art. 5 del RGPD, así como de su participación en las solicitudes de ejercicio de derechos, la notificación de las violaciones de seguridad y los requisitos necesarios para la comunicación de datos y las Transferencias Internacionales de Datos.

- ✓ Adaptación del procedimiento de atención de solicitudes de ejercicio de derechos para que sea ejercido, preferiblemente, por medios electrónicos y que incluya el ejercicio de todos los derechos reconocidos en los arts. 15 a 22 del RGPD:
    - o Acceso.
    - o Rectificación.
    - o Supresión.
    - o Limitación del tratamiento
    - o Portabilidad
    - o Oposición.
    - o Derecho a no ser objeto de decisiones automatizadas.
- ✓ Generación e implementación de un procedimiento específico para la revisión de los nuevos tratamientos de datos, para garantizar que los mismos cumplen con las obligaciones del RGPD desde el diseño (Privacidad desde el diseño art. 25 RGPD).
- ✓ Creación de contratos específicos con los Encargados de Tratamiento o de confidencialidad, en función del tipo de servicio que se presten. (Art. 28 del RGPD)
- ✓ Realización del análisis de riesgos, conforme a la metodología. (art. 32 RGPD). El resultado del mismo determina que el riesgo es aceptable.
- ✓ Identificación y aplicación de las medidas de seguridad idóneas para mitigar los riesgos identificados,
- ✓ Generación del procedimiento de notificación de violaciones de seguridad a la Autoridad de Control, así como a las personas interesadas, partiendo del Registro de Incidencias, en cumplimiento de los artículos 33 y 34 del RGPD.
- ✓ Determinación de la necesidad de realizar Evaluación del Impacto relativa a la Protección de Datos en aquellos tratamientos de datos que entrañan un alto riesgo para los derechos y libertad de las personas físicas. (Art. 35 RGPD), y realización de la misma, así como valoración de las conclusiones.

En Torrelavega a 3 de mayo de 2022

Firmado: Luis Angel González Pérez
Abogado- Consultor en Protección de Datos.