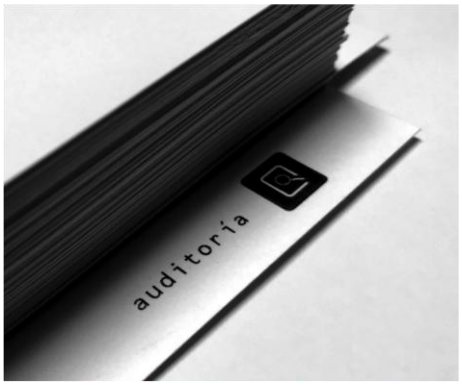
INFORME DE AUDITORÍA



aixacorpore

www.aixacorpore.es

administracion@aixacorpore.es www.aixacorpore.es Tel: 922 625 942
Fax: 922 623 878 C/ Fernández Navarro
19, Local 1, 38003 -
S/C de Tenerife

INDICE

I.ANTECEDENTES

I.1. ENTIDAD AUDITADA

Nombre	**COLEGIO OFICIAL DE QUIMICOS DE CANARIAS**
CIF	**Q3870003E**
Domicilio Social	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
Actividad	Colegio profesional
Responsable de Seguridad	Iñigo Jaudenes Ruíz de Atauri

I.2. ENTIDAD AUDITORA

Nombre	**AIXA CORPORE, S.L.**
CIF	**B38741625**
Domicilio Social	C/ Fernández Navarro 19, Local 1, 38003 – Santa Cruz de Tenerife
Actividad	Consultoría/Auditoría RGPD
Auditores que han participado	

I.3. OBJETIVOS DE LA AUDITORÍA

Hemos recibido el encargo profesional para la realización de una auditoría **LEGAL EXTERNA** de los sistemas de información e instalaciones de tratamiento de datos para verificar el cumplimiento de:

- Reglamento vigente en materia de protección de datos, por el que se aprueba el Reglamento de Medidas de Seguridad.
- Procedimientos vigentes en materia de seguridad de datos.
- Instrucciones vigentes en materia de seguridad de datos.

I.4. ALCANCE DE LA AUDITORÍA

I.4.1. Tratamientos auditados.

1	**Nombre**	**ASOCIADOS**
	Ubicación	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
	Finalidad	Finalidad no encontrada.

2	**Nombre**	**CONTACTOS**
	Ubicación	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
	Finalidad	Finalidad no encontrada.

3	**Nombre**	**GESTION CONTABLE Y FISCAL**
	Ubicación	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
	Finalidad	Gestión de los datos necesarios para la gestión contable y fiscal de la entidad.

4	**Nombre**	**COLEGIADOS**
	Ubicación	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
	Finalidad	Finalidad no encontrada.

I.4.2. Centros de trabajo auditados.

Nombre	**COLEGIO OFICIAL DE QUIMICOS DE CANARIAS**
Dirección	CALLE CASTRO 11 - 1º IZQUIERDA, 38006 – Santa Cruz de Tenerife
Actividad del centro	Colegio profesional

I.5. LIMITACIONES EN LA EJECUCIÓN DEL TRABAJO

A continuación, detallamos todas aquellas circunstancias que han limitado la ejecución del trabajo de auditoría.

I.6. METODOLOGÍA DEL TRABAJO DE AUDITORÍA

Las etapas de ejecución del trabajo de auditoría han sido las siguientes:

A) LA EJECUCIÓN DE LA AUDITORÍA

- **Recogida de evidencias.**

  Se realiza mediante cuatro estrategias:

  1. Análisis de documentación aportada por la auditada.
  2. Comprobación de registros.
  3. Inspección visual de los sistemas de la información y entorno físico.
  4. Entrevistas con el personal (responsables y usuarios).

- **Documentación de los resultados.**

B) EL INFORME DE AUDITORÍA

El informe de auditoría constituye el resultado de las conclusiones obtenidas a través de las diversas evidencias del auditor.
Las medidas a adoptar en el presente informe se definen como obligatorias o recomendables. Asimismo, las recomendaciones aportadas son de varios tipos:

- Normativas
- Organizativas
- Objetivos y procedimientos de control
- Necesidades tecnológicas

II.ANÁLISIS

II.1. ANÁLISIS DEL CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD

A continuación, analizamos el debido cumplimiento de cada una de las medidas de seguridad aplicables a los tratamientos de la empresa, según el reglamento de protección de datos vigente.

Hemos englobado dichas medidas a analizar en las siguientes áreas temáticas:

1. **Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.**
2. **Ficheros temporales o copias de trabajo de documentos.**
3. **Documento de Políticas de Seguridad.**
4. **Funciones y obligaciones del personal.**
5. **Registro de incidencias**.
6. **Identificación y autenticación**.
7. **Control de acceso**.
8. **Gestión de soportes y documentos**.
9. **Copias de respaldo y recuperación**.
10. **Telecomunicaciones**.
11. **Videovigilancia**.
12. **Criterio de archivo**.
13. **Dispositivos de almacenamiento**.
14. **Custodia de soportes**.
15. **Almacenamiento de la información**.
16. **Copia o reproducción**.
17. **Acceso a la documentación**.
18. **Traslado de la documentación**.

Se analizarán las áreas aplicables, para identificación de todas las deficiencias encontradas y propuesta de las medidas correctoras o complementarias correspondientes, así como de las recomendaciones del auditor, con indicación del correspondiente fichero.

Posteriormente, en el **Anexo I**, se acompañan cuadros resúmenes de la totalidad de estas medidas y recomendaciones.

Artículo	Aplica
Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.	X
Autorización del tratamiento fuera de los locales del responsable del fichero.	X
Existencia en el documento de políticas de seguridad de las autorizaciones para el tratamiento de datos en el exterior de la empresa.	X
Ficheros temporales o copias de trabajo de documentos.	X
Nivel de seguridad de los ficheros temporales	X
Eliminación de los ficheros temporales	X
Documento de Políticas de Seguridad.	X
Existencia de documento de políticas de seguridad en la entidad	X
Fijación del ámbito de aplicación del documento	X
Medidas, normas, procedimientos de actuación, reglas y estándares de seguridad del sistema.	X
Identificación del responsable de seguridad	X
Procedimiento de realización de controles periódicos.	
Actualización del documento de políticas de seguridad.	X
Funciones y obligaciones del personal.	X
Descripción de las funciones de los usuarios con acceso a los datos	X
Conocimiento del personal de sus funciones y obligaciones	X
Registro de incidencias.	X
Procedimiento de Gestión de incidencias	X
Contenido del Procedimiento de Recuperación de Datos.	
Autorización para la recuperación de datos.	
Identificación y autenticación.	X
Identificación del personal que accede a datos.	X
Procedimiento de identificación inequívoca y personalizada de los usuarios.	X
Método de distribución de contraseñas.	X
Periodicidad de cambio de las contraseñas	X
Limitación de accesos fallidos al sistema.	
Control de acceso.	X
Perfiles de acceso.	X
Sistema de control de acceso.	X
Personal autorizado a modificar la permisología	X

Personal Ajeno	X
Aplicaciones de acceso a datos	X
Acceso físico.	
Información de los registros de acceso (contenido y duración).	
Información de los registros de acceso (revisión).	
Realización de los registros de acceso.	
Gestión de soportes.	X
Inventario de soportes	X
Etiquetado de soportes	X
Inventario de equipos	X
Almacenamiento de soportes	X
Personal autorizado a enviar recibir soportes	X
Traslado de documentación	X
Eliminación de soportes	X
Registro de entrada de soportes o documentos.	
Registro de salida de soportes o documentos.	
Salida de soportes por operaciones de mantenimiento.	
Salida de soportes cifrada .	
Copias de respaldo y recuperación.	X
Periodicidad de copias de seguridad	X
Procedimiento de recuperación de datos.	X
Verificación de las copias de seguridad	X
Actualización / implantación de nuevo software. Pruebas con datos reales.	X
Ubicación de las copias de seguridad.	
Telecomunicaciones.	X
Acceso a través de redes de telecomunicaciones	X
Transmisión de datos de nivel alto a través de redes de telecomunicaciones.	
Artículo 22 LOPDGDD. Tratamientos con fines de videovigilancia	
Cartelería	
Información adecuada	
Calidad de las imágenes	
Captura de imágenes del exterior	
Plazos de eliminación de imágenes	
Bloqueo y conservación	
Cesión de imágenes a terceros	
Criterio de archivo de documentos.	X
Almacenamiento de la documentación.	X
Custodia de soportes	X

Almacenamiento de documentos con datos de nivel alto.	
Copia y reproducción de documentos.	
Acceso a la documentación (Registros de acceso).	
Traslado de documentación.	

INFORME DE CONCLUSIONES CON OPINIÓN FAVORABLE CON SALVEDADES.

En S/C de Tenerife a 20/04/2026

Hemos realizado una auditoría **LEGAL EXTERNA** de los sistemas de información e instalaciones de tratamiento de datos de carácter personal de la entidad **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** para verificar el cumplimiento del reglamento de protección de datos vigente, así como de los procedimientos e instrucciones vigentes en materia de protección de datos.

En nuestra opinión profesional, las instalaciones y tratamientos de la entidad **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** se adecuan a la legislación aplicable en seguridad de tratamiento de datos de carácter personal, salvo por las deficiencias observadas, que se detallan en el **Anexo I** del presente informe, que además incluye las correspondientes medidas correctoras o complementarias.

Por último, se recuerda a la entidad **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS**, que sus Responsables de Seguridad deben analizar el presente informe de auditoría y elevar a la Dirección, las conclusiones que resulten para que ésta adopte las medidas correctoras adecuadas.

Firma

III.ANEXO I. TABLA RESUMEN DE MEDIDAS CORRECTORAS O COMPLEMENTARIAS

IDENTIFICACIÓN Y AUTENTIFICACIÓN			
FICHERO	OBSERVACIÓN	MEDIDA CORRECTORA O COMPLEMENTARIA	VALORACIÓN
TODOS	Existe una relación de usuarios con acceso a datos en el documento de políticas de seguridad de la entidad pero no se encuentra actualizada.	Revisar el listado de usuarios en el documento de políticas de seguridad con el fin de detectar inconsistencias. Actualizarlo de manera que sea fiel a la realidad.	OBLIGATORIO
TODOS	Los nombres de usuarios asignados no identifican de forma inequívoca y personalizada a los usuarios de los sistemas de información.	Crear cuentas personalizadas, revisar los usuarios del sistema dar de alta nuevas cuentas para los usuarios que usan las antiguas y bloquear/eliminar las cuentas de los usuarios que ya no están trabajando para la empresa.	OBLIGATORIO
TODOS	Al asignar las contraseñas están son conocidas por personas adicionales a parte del propio usuario, por lo que no se pueden considerar confidenciales.	Utilizar la política de contraseñas del sistema operativo de cambio al primer acceso u otro sistema equivalente.	OBLIGATORIO
TODOS	No se realizan cambios de contraseñas en un periodo de tiempo adecuado.	Realizar cambios de contraseñas cada 180 días como indica el documento de políticas de seguridad. Esta recomendación es aplicable tanto en los sistemas operativos como en las aplicaciones utilizadas.	OBLIGATORIO

CONTROL DE ACCESO			
FICHERO	OBSERVACIÓN	MEDIDA CORRECTORA O COMPLEMENTARIA	VALORACIÓN
TODOS	En el documento de políticas de seguridad de la empresa no se encuentra una relación actualizada de usuarios junto con los accesos que tiene autorizados.	Se deben establecer unos perfiles de acceso donde cada grupo de usuarios tenga permitidos una serie de accesos acordes con las tareas desempeñadas en cada departamento.	OBLIGATORIO
TODOS	No concuerdan los usuarios dados de alta en el sistema con los que se encuentran en el documento de políticas de seguridad de LA EMPRESA.	El responsable de seguridad debe revisar los listados de usuarios con sus accesos para mantenerlos actualizados en el sistema de información.	OBLIGATORIO
TODOS	No existe permisología en los sistemas de información de la entidad por lo que aumenta la	Configurar permisos en las aplicaciones así como utilizar antivirus y otros medios para evitar accesos no autorizados. Configurar los	OBLIGATORIO

	posibilidad de que se produzca un acceso no autorizado.	salvapantallas para bloquear los equipos cuando el usuario no esté presente. Instalar destructoras de papel.	
TODOS	Los sistemas de información no están llevando a cabo el registro de acceso a los datos de carácter personal de nivel alto.	Los accesos a datos en las aplicaciones y en los documentos en papel deben ser registrados identificando al usuario, fecha y hora del acceso, fichero accedido y tipo de acceso.	OBLIGATORIO
TODOS	Los registros de acceso a los datos de carácter personal de nivel alto no se conservan por un tiempo superior a los dos años.	Modificar la duración de los registros de acceso, estos deben conservarse durante al menos 2 años.	OBLIGATORIO
TODOS	El responsable no está revisando los registros de accesos generados para los datos de carácter personal de nivel alto.	Revisar los registros de acceso al menos mensualmente y realizar informes de lar revisiones, para esto se puede utilizar la plantilla de controles periódicos del documento de políticas de seguridad.	OBLIGATORIO

COLEGIO OFICIAL DE QUIMICOS DE CANARIAS
Iñigo Jaudenes Ruíz de Atauri

AIXA CORPORE, S.L
Héctor Peña

IV.ANEXO II. MODELO DE FICHA DE CONCLUSIONES DEL RESPONSABLE DE SEGURIDAD

Con fecha ___ de _____ de _____, el Responsable de Seguridad recibió informe de auditoría emitido por AIXA CORPORE, S.L. con fecha 20/04/2026 en cumplimiento de lo establecido en el reglamento de protección de datos.

El informe de auditoría describe las siguientes deficiencias, que detallamos de forma resumida y que valoramos según nuestra opinión para elevarlas al Responsable del Fichero:

INFORMACIÓN DEL AUDITOR
Área Auditada.
Deficiencia detectada.
Medidas correctoras o complementarias propuestas por el auditor.
Recomendaciones propuestas por el auditor.
ANÁLISIS DEL RESPONSABLE DE SEGURIDAD
Valoración de la deficiencia.
Valoración de las medidas correctoras o complementarias propuestas por el auditor.
Valoración de las recomendaciones propuestas por el auditor.
Propuesta de medidas alternativas y adicionales.

COSTES ESTIMADOS PARA LA IMPLANTACIÓN DE MEDIDAS					
	Coste Activos	Costes materiales fungibles	Coste personal propio	Coste entidades externas	Coste total medida
Se deben establecer unos perfiles de acceso donde cada grupo de usuarios tenga permitidos una serie de accesos acordes con las tareas desempeñadas en cada departamento.					
El responsable de seguridad debe revisar los listados de usuarios con sus accesos para mantenerlos actualizados en el sistema de información.					
Configurar permisos en las aplicaciones así como utilizar antivirus y otros medios para evitar accesos no autorizados. Configurar los salvapantallas para bloquear los equipos cuando el usuario no esté presente. Instalar destructoras de papel.					
Revisar el listado de usuarios en el documento de políticas de					

seguridad con el fin de detectar inconsistencias. Actualizarlo de manera que sea fiel a la realidad.					
Crear cuentas personalizadas, revisar los usuarios del sistema dar de alta nuevas cuentas para los usuarios que usan las antiguas y bloquear/eliminar las cuentas de los usuarios que ya no están trabajando para la empresa.					
Utilizar la política de contraseñas del sistema operativo de cambio al primer acceso u otro sistema equivalente.					
Realizar cambios de contraseñas cada 180 días como indica el documento de políticas de seguridad. Esta recomendación es aplicable tanto en los sistemas operativos como en las aplicaciones utilizadas.					
Los accesos a datos en las aplicaciones y en los documentos en papel deben ser registrados identificando al usuario, fecha y hora del acceso, fichero accedido y tipo de acceso.					
Modificar la duración de los registros de acceso, estos deben conservarse durante al menos 2 años.					
Revisar los registros de acceso al menos mensualmente y realizar informes de lar revisiones, para esto se puede utilizar la plantilla de controles periódicos del documento de políticas de seguridad.					

CONCLUSIONES		
Fecha de entrega	Firma: Responsable Seguridad	Recibí: Responsable Fichero

CERTIFICADO. SELLO DE ADHESIÓN AL CÓDIGO ÉTICO

COLEGIO OFICIAL DE QUIMICOS DE CANARIAS

S/C de Tenerife, a 20/04/2026

AIXA CORPORE, S.L. certifica que **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** con CIF **Q3870003E** ha pasado con éxito la Auditoría de Protección de Datos, realizada de conformidad con lo exigido y establecido en el reglamento de protección de datos vigente.

El resultado del informe de auditoría efectuado a **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** con fecha **20/04/2026** ha sido FAVORABLE CON SALVEDADES, y detectándose una serie de deficiencias, si bien no son de todas de obligado cumplimiento, aconsejamos sean valoradas.

De esta forma los titulares de los ficheros de las empresas detalladas en la tabla al final de este documento cumplen con el deber de diligencia exigido por la Agencia Española de Protección de Datos al titular del fichero que debe velar porque el encargado del tratamiento, en el presente supuesto, **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** cumple las medidas de seguridad requeridas por el reglamento de protección de datos vigente.

Como prueba de la correcta adecuación de la mencionada entidad a lo establecido en el citado reglamento, entregamos el correspondiente sello de adecuación al Código Ético de Protección de Datos que se otorga a aquellas entidades que cumplen lo establecido en la citada normativa y en especial respetan lo dispuesto en el Art. 18.4 de la Constitución Española.
Y en prueba del mismo, firma el representante de **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** en el lugar y fecha indicados en el encabezamiento.

CLIENTE	Nº CÓDIGO ÉTICO
COLEGIO OFICIAL DE QUIMICOS DE CANARIAS	**261303**

CLIENTE: COLEGIO OFICIAL DE QUIMICOS DE CANARIAS

Persona que recibe:
Iñigo Jaudenes Ruíz de Atauri

AIXA CORPORE S.L.

Auditor:
Héctor Peña

S/C de Tenerife, a 20/04/2026

Iñigo Jaudenes Ruíz de Atauri**,** en calidad de responsable de seguridad de **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** con **CIF Q3870003E** acredita mediante la firma del presente documento que ha recibido de AIXA CORPORE, S.L., el informe de auditoría favorable, por lo que en el presente acto se entrega el Sello de Código Ético otorgado por AIXA CORPORE, S.L. a **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** con fecha **20/04/2026**, que certifica la correcta adecuación de **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS** tanto a lo establecido en el reglamento actual de protección de datos, como a lo dispuesto en el Art. 18.4 de la Constitución Española.
En la siguiente tabla se detallan el número de miembro adherido al código ético de protección de datos de Aixa Corpore, S.L. entregado.

CLIENTE	Nº CÓDIGO ÉTICO
COLEGIO OFICIAL DE QUIMICOS DE CANARIAS	**261303**

CLIENTE: COLEGIO OFICIAL DE QUIMICOS DE CANARIAS

Persona que recibe:
Iñigo Jaudenes Ruíz de Atauri