

INFORME DE AUDITORÍA



info@conversia.es
T. 902 877 192
F. 902 877 042
www.conversia.es

 **CONVERSIA**
CONSULTING GROUP

- A. ALCANCE DE LOS TRABAJOS
- B. ADECUACIÓN DE LAS MEDIDAS Y CONTROLES AL REGLAMENTO 1720/2007 DE DESARROLLO DE LA LEY 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, IDENTIFICACIÓN DE LAS DEFICIENCIAS Y PROPUESTA DE MEDIDAS CORRECTORAS
 - 1. ASPECTOS GENERALES
 - 2. DOCUMENTO DE SEGURIDAD
 - 3. ENCARGADO DE TRATAMIENTO
 - 4. PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES
 - 5. DELEGACIÓN DE AUTORIZACIONES
 - 6. RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO
 - 7. FUNCIONES Y OBLIGACIONES DEL PERSONAL
 - 8. REGISTRO DE INCIDENCIAS
 - 9. CONTROL DE ACCESO
 - 10. GESTIÓN DE SOPORTES Y DOCUMENTOS
 - 11. IDENTIFICACIÓN Y AUTENTIFICACIÓN
 - 12. COPIAS DE RESPALDO Y RECUPERACIÓN
 - 13. CRITERIOS DE ARCHIVO
 - 14. ALMACENAMIENTO DE LA INFORMACIÓN
 - 15. CUSTODIA DE SOPORTES
 - 16. AUDITORÍA
- C. LUGAR DE REALIZACIÓN DEL TRABAJO
- D. FASES DEL TRABAJO DE AUDITORÍA
- E. MEDIDAS REVISADAS
- F. DOCUMENTACIÓN ENTREGADA

A. ALCANCE DE LOS TRABAJOS

OBJETO

El presente informe se elabora y entrega como resultado del encargo de trabajo que se produjo tras la aprobación de la correspondiente propuesta realizada a FEDERACION GALEGA DE TAEKWONDO el año 2016, para la realización de una auditoría de los sistemas de información e instalaciones de tratamiento de datos y un informe de auditoría independiente del cumplimiento del Reglamento de Desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre de protección de datos de carácter personal, de los procedimientos e instrucciones vigentes en materia de seguridad de datos.

NORMATIVA

La auditoría ha sido realizada para la comprobación del cumplimiento de la legislación vigente en materia de seguridad en protección de datos de carácter personal relativos a las personas físicas, utilizando como normativa de referencia y contraste los siguientes documentos:

- a) Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.
- b) Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley 15/1999 de Protección de Datos de Carácter Personal.
- c) Resoluciones vigentes en materia de seguridad de datos.
- d) Recomendaciones vigentes de la Agencia Española de Protección de Datos.
- e) Informes jurídicos de la Agencia Española de Protección de Datos.
- f) Ley orgánica 34/2002 de 11 de Julio, Servicios de la Sociedad de la Información y de Comercio Electrónico.
- g) Real decreto 1332/94 de 20 de junio por el que se desarrollan algunos preceptos de la Ley Orgánica.

ESTÁNDARES UTILIZADOS

En los últimos años se ha incrementado la atención sobre los controles internos, tanto para los auditores, los gerentes, o para las entidades reguladoras en general. Como resultado de un continuo y trabajoso esfuerzo, se han desarrollado varios documentos para definir, valorar, reportar y mejorar el control interno, y ser utilizados como marco de referencia en las organizaciones. Para el desarrollo de la presente auditoría, se han tomado en consideración los siguientes estándares:

- a) Informe COSO - (Committee of Sponsoring Organizations), de la Comisión de Estudios de Controles Internos.
- b) SAC - (Systems Auditability and Control), de la Fundación de Investigación del Instituto de Auditores Internos.
- c) SAS 55 y SAS 78 - Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA).
- d) COBIT (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de ellos ha sido definido para una audiencia en particular: el "COSO" fue diseñado para la Gerencia; el "SAC" para los auditores internos; los SAS 55 y SAS 78 para los auditores externos, y finalmente el "COBIT" enfocado principalmente a los auditores de sistemas de información.

FECHA DE LA AUDITORÍA

Se realiza la auditoría de los sistemas de información e instalaciones de tratamiento de datos para la anualidad de 2016 y la entrega del presente informe a 5 de febrero de 2016.

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

RAZÓN SOCIAL: FEDERACION GALEGA DE TAEKWONDO

CIF: G15237233

DIRECCIÓN FISCAL: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)

FICHEROS O TRATAMIENTOS OBJETOS DE LA AUDITORÍA

Los tratamientos auditados objeto del presente informe responsabilidad de FEDERACION GALEGA DE TAEKWONDO han sido los correspondientes al nivel básico de seguridad, de acuerdo con los criterios establecidos en el Reglamento 1720/2007.

A continuación, se describen brevemente algunas características de los tratamientos que se desprenden de los formularios de inscripción presentados en el Registro General de Protección de Datos:

Fichero: ALUMNOS
Tratamientos: GESTIÓN DE ALUMNOS
Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)
Finalidad: FICHERO CON DATOS DE CARÁCTER PERSONAL DE ALUMNOS
Medidas de Seguridad: BÁSICO

Fichero: PATROCINADORES
Tratamientos: GESTIÓN DE PROVEEDORES
Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)
Finalidad: MANTENIMIENTO Y GESTION DE PATROCINADORES QUE COLABORAN EN LOS DIFERENTES EVENTOS DEPORTIVOS
Medidas de Seguridad: BÁSICO

Fichero: NOMINAS
Tratamientos: GESTIÓN DEL PERSONAL
Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)
Finalidad: FICHERO CON DATOS DE CARÁCTER PERSONAL DE LOS EMPLEADOS
Medidas de Seguridad: BÁSICO

Fichero: RECURSOS HUMANOS
Tratamientos: GESTIÓN DE LOS CANDIDATOS A EMPLEADOS
Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)
Finalidad: FICHERO CON DATOS DE CARÁCTER PERSONAL DE EMPLEADOS Y/O CANDIDATOS A EMPLEADOS
Medidas de Seguridad: BÁSICO

Fichero: ACTAS
Tratamientos: GESTIÓN DE ACTAS
Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)
Finalidad: FICHERO CON DATOS DE CARÁCTER PERSONAL DE ACTAS REALIZADAS EN LA ENTIDAD
Medidas de Seguridad: BÁSICO

Fichero: DEPORTISTAS

Tratamientos: GESTIÓN DE DEPORTISTAS

Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)

Finalidad: FICHERO CON DATOS DE CARÁCTER PERSONAL DE ISTAS FEDERADOS PARTICIPANTES EN LAS COMPETICIONES OFICIALES

Medidas de Seguridad: BÁSICO

Fichero: PERSONAL TECNICO

Tratamientos: GESTIÓN DE CLIENTES

Ubicación Principal: PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA)

Finalidad: ELACION DE ARBITROS ENTRENADORES JUECES Y RESTO DE PERSONAL TECNICO

Medidas de Seguridad: BÁSICO

LISTA DE DISTRIBUCIÓN

Este informe de auditoría debe ser entregado a las siguientes personas pertenecientes a la organización del Responsable del fichero:

NOMBRE Y APELLIDOS	CARGO Y DEPARTAMENTO
JUAN CARLOS CAINZOS	ADMINISTRATIVO

B. ADECUACIÓN DE LAS MEDIDAS Y CONTROLES AL REGLAMENTO 1720/2007 DE DESARROLLO DE LA LEY 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, IDENTIFICACIÓN DE LAS DEFICIENCIAS Y PROPUESTA DE MEDIDAS CORRECTORAS

Respecto a los ficheros auditados de acuerdo con lo dispuesto en el Reglamento de Desarrollo de la Ley 15/1999 de protección de datos de carácter personal, a continuación se ponen de manifiesto los hechos, datos y observaciones revisados y comprobados por el auditor respecto a la adecuación de los mismos a las medidas de seguridad establecidas en el Real Decreto 1720/2007, así como la identificación de todas las deficiencias encontradas y la propuesta de medidas correctoras o complementarias que recomienda el auditor.

A continuación, se enumeran las medidas de seguridad exigidas en el Real Decreto 1720/2007 y su situación actual en FEDERACION GALEGA DE TAEKWONDO.

1. ASPECTOS GENERALES

DEFINICIÓN

Artículo 81. Aplicación de los niveles de seguridad.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.
2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:
 - a. Los relativos a la comisión de infracciones administrativas o penales.
 - b. Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, 13 de diciembre.
 - c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
 - d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
 - e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
 - f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán a los siguientes ficheros o tratamientos de datos de carácter personal:
 - a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
 - b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
 - c. Aquéllos que contengan datos derivados de actos de violencia de género.
4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- a. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- b. Se trate de ficheros o tratamientos en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptara el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que, en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación, en cada caso, el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el nivel de seguridad establecido tanto en el Documento de Seguridad como en los ficheros inscritos en la Agencia de Protección de Datos, observándose cada uno de los aspectos contenidos en el artículo 81.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha constatado que la clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

2. DOCUMENTO DE SEGURIDAD

DEFINICIÓN

Artículo 88. Documento de Seguridad.

1. El responsable del fichero elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa de acuerdo con la normativa vigente que será de obligado cumplimiento por el personal con acceso a los datos informatizados de carácter personal y a los sistemas de información.

2. El Documento de Seguridad podrá ser único y conformado por todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborar diferentes Documentos de Seguridad agrupando ficheros o tratamientos según los sistemas de tratamiento utilizados por la organización, o bien atendiendo criterios organizativos del responsable del fichero. En todo caso, tendrá carácter de documento interno de la organización.

3. El documento deberá recoger, como mínimo, los siguientes aspectos:

- a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- b) Medidas, Normas, Procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad establecidos en el Reglamento de desarrollo de la Ley Orgánica 15/1999
- c) Funciones y obligaciones del personal.
- d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los traten.
- e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
- f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- g) Las medidas que sean necesarias adoptar para el transporte de soportes y documentos, así como la destrucción o reutilización de éstos

4. En el supuesto de que fueran de aplicación los ficheros de seguridad de nivel medio o alto, el Documento de Seguridad deberá contener:

- a) Identificación del responsable o responsables de seguridad.
- b) Los controles periódicos que se hayan de realizar para verificar el cumplimiento de dicho documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento deberá incluir la identificación de los ficheros o tratamientos en concepto de encargado de tratamiento, o bien un documento que regule las condiciones de prestador de servicios.

6. En los casos en que los datos de carácter personal de un fichero o tratamiento se incorporen y se traten de forma exclusiva en los sistemas del encargado de tratamiento, el responsable lo deberá hacer constar en el documento de seguridad.

7. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en los sistemas de información o en la organización del mismo.

8. El contenido del documento se deberá adecuar, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el Documento de Seguridad de FEDERACION GALEGA DE TAEKWONDO, revisando cada una de las disposiciones obligatorias que requiere el Artículo 88 del Real Decreto 1720/2007.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha comprobado la existencia del Documento de Seguridad y se ha verificado que el contenido es conforme a lo dispuesto en el artículo 88 del Real Decreto 1720/2007.

Se verifica que el contenido del documento de seguridad cumple con las exigencias del Real Decreto 1720/2007 que son las siguientes: ámbito de aplicación del documento con especificación detallada de los recursos protegidos, medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento, funciones y obligaciones del personal, estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan, procedimiento de notificación, gestión y respuesta ante las incidencias y procedimientos de realización de copias de respaldo y de recuperación de los datos.

Todos los cambios producidos en FEDERACION GALEGA DE TAEKWONDO han quedado reflejados en el documento de seguridad después de haberlo comprobado con el Responsable de Seguridad.

Hemos comprobado que el contenido del documento de seguridad se adecua a la normativa vigente en materia de protección de datos.

Se ha comprobado que todos los usuarios existentes en FEDERACION GALEGA DE TAEKWONDO disponen de una contraseña propia.

FEDERACION GALEGA DE TAEKWONDO cambian las contraseñas de los equipos informáticos tal y como establece el Real Decreto 1720/2007.

Las contraseñas se cambian con una periodicidad inferior al año.

Después de revisar el "Nombramiento del Responsable de Seguridad" se constata que FEDERACION GALEGA DE TAEKWONDO dispone de Responsable de Seguridad.

El nombramiento ha sido firmado por FEDERACION GALEGA DE TAEKWONDO y por el Responsable de Seguridad.

Se constata que existe un único Responsable de Seguridad en FEDERACION GALEGA DE TAEKWONDO. Y este hecho queda reflejado en el Documento de Seguridad

Después de haber entrevistado al Responsable de Seguridad, se ha verificado que es la única persona autorizada en FEDERACION GALEGA DE TAEKWONDO para conceder, alterar o anular los accesos a datos o recursos de FEDERACION GALEGA DE TAEKWONDO.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

3. ENCARGADO DE TRATAMIENTO

DEFINICIÓN

Artículo 82. Encargado de tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero, deberá hacerse constar esta circunstancia en el Documento de Seguridad de dicho responsable, comprometiéndose, el personal del encargado, al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos en el artículo 88 de este reglamento, o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

DATOS, HECHOS Y OBSERVACIONES

Se comprueba que existen terceras personas o empresas que prestan un servicio por cuenta de FEDERACION GALEGA DE TAEKWONDO.

VERIFICACIÓN DE SU CUMPLIMIENTO

Después de haber entrevistado al Responsable del Fichero, se observa que existen terceras personas o empresas que prestan un servicio por cuenta de FEDERACION GALEGA DE TAEKWONDO.

Tras la revisión de los correspondientes Contratos de Prestación de Servicios se observa que éstos están debidamente firmados y su contenido se adecua a lo exigido por el art. 12 de la LOPD.

Se ha observado que no existe, por parte del encargado de tratamiento, un acceso remoto a los sistemas de información de FEDERACION GALEGA DE TAEKWONDO.

SALVEDADES

No existen.

PROPUESTAS DE MEDIDAS CORRECTORAS

No existen.

PROPUESTAS DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR.

Se recomienda a FEDERACION GALEGA DE TAEKWONDO que en el caso de tener nuevos prestadores de servicios que accedan a datos de carácter personal será necesario formalizar un contrato de prestación de servicios según lo establecido en el artículo 12 LOPD.

4. PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES

DEFINICIÓN

Artículo 83. Prestadores de servicios sin acceso a datos personales.

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los recursos del sistema de información, para realización de trabajos que no impliquen el tratamiento de datos personales. Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y a la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

DATOS, HECHOS Y OBSERVACIONES

Se comprueba que no existen terceras personas o empresas que prestan un servicio sin acceso a datos personales por cuenta de FEDERACION GALEGA DE TAEKWONDO.

VERIFICACIÓN DE SU CUMPLIMIENTO

Tras entrevistar al Responsable de Seguridad, se constata que no existen servicios prestados por un tercero sin acceso a datos de carácter personal.

SALVEDADES

No existen.

PROPUESTAS DE MEDIDAS CORRECTORAS

No existen.

PROPUESTAS DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR.

No existen.

5. DELEGACIÓN DE AUTORIZACIONES

DEFINICIÓN

Artículo 84. Delegación de autorizaciones.

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto.

En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

DATOS, HECHOS Y OBSERVACIONES

Se ha comprobado que no es el propio responsable del fichero quién autoriza los procedimientos que tiene atribuidos y que se encuentran descritos en el Documento de Seguridad.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se ha verificado con el responsable del fichero que se han delegado las autorizaciones que tiene atribuidas y que este hecho consta en el Documento de Seguridad.

SALVEDADES

No existen.

PROPUESTAS DE MEDIDAS CORRECTORAS

No existen.

PROPUESTAS DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR.

No existen.

6. RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

DEFINICIÓN

Artículo 86. Régimen de trabajo fuera de los locales de ubicación de los ficheros.

1. Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del fichero o tratamiento o encargado de tratamiento será precisa la autorización previa del responsable del fichero o tratamiento y deberá garantizar el nivel de seguridad correspondiente al tipo de fichero tratado.

2. Esta autorización deberá constar en el Documento de Seguridad.

DATOS, HECHOS Y OBSERVACIONES

Se comprueba que no existen terminales portátiles en la entidad FEDERACION GALEGA DE TAEKWONDO.

VERIFICACIÓN DE SU CUMPLIMIENTO

En FEDERACION GALEGA DE TAEKWONDO no existen dispositivos portátiles que permitan trabajar desde fuera de los locales de ubicación de los ficheros que contienen datos de carácter personal.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

7. FUNCIONES Y OBLIGACIONES DEL PERSONAL

DEFINICIÓN

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de FEDERACION GALEGA DE TAEKWONDO, requiriéndole acerca de las medidas de seguridad, controles y procedimiento que debería cumplir en esta materia.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se comprueba la existencia de un modelo de Circular Interna donde se advierte a los empleados de las normas de seguridad que afectan al desarrollo de sus funciones y su obligación de cumplirlas así como de las consecuencias de su incumplimiento conforme a lo dispuesto en la LOPD.

Se comprueba que los empleados han firmado el Documento de Compromiso de Confidencialidad, en el que éstos adquieren el compromiso de velar por la seguridad, y el buen uso de los datos y donde se adquieren los consentimientos necesarios para tratar los datos de los mismos.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

Se recomienda a FEDERACION GALEGA DE TAEKWONDO que cuando se incorpore nuevo personal se les entregue la Circular Interna y se les haga firmar el correspondiente compromiso de confidencialidad para que el responsable del fichero pueda garantizar que se cumplirá con el deber de secreto regulado en el artículo 10 LOPD.

8. REGISTRO DE INCIDENCIAS

DEFINICIÓN

Artículo 90. Registro de incidencias.

El procedimiento de notificación y gestión de incidencias deberá tener necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en qué se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que hubieran derivado de la misma.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar el Documento de Seguridad y a preguntar a las personas entrevistadas de FEDERACION GALEGA DE TAEKWONDO, preguntando sobre el procedimiento del registro de incidencias y han manifestado que existe un procedimiento de registro de incidencias.

VERIFICACIÓN DE SU CUMPLIMIENTO

Una vez revisado el registro de incidencias elaborado por FEDERACION GALEGA DE TAEKWONDO se constata que no se ha producido ninguna incidencia que se deba registrar.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

Registrar todas las incidencias, si se producen, y llevar a cabo la resolución con la mayor brevedad posible.

9. CONTROL DE ACCESO

DEFINICIÓN

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que se necesiten para el desarrollo de sus funciones.
2. El responsable del fichero o tratamiento se encargará de la existencia de una relación de usuarios y perfil de usuarios con sus respectivos accesos autorizados
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos diferentes a los autorizados.
4. Exclusivamente el personal autorizado en el documento de seguridad podrá conceder, modificar o anular el acceso autorizado sobre los datos y recursos, de acuerdo con los criterios establecidos por el responsable del fichero.
5. En el supuesto de que existan personas ajenas al responsable del fichero que tengan acceso a los recursos, tendrán que cumplir con las mismas obligaciones y condiciones de seguridad que el personal propio.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de la empresa para conocer las funciones propias de cada empleado y si únicamente estos acceden a los datos que estrictamente necesitan para el desarrollo de sus funciones.

VERIFICACIÓN DE SU CUMPLIMIENTO

Todos los usuarios de los equipos informáticos de FEDERACION GALEGA DE TAEKWONDO disponen de un nombre de usuario propio para poder acceder a los mismos.

Los accesos están restringidos, de modo que solo pueden acceder a los recursos necesarios para el desarrollo de sus funciones.

Tras revisar la relación de usuarios, se comprueba que dicha relación de usuarios está actualizada y recoge todos los usuarios que disponen de acceso a los recursos informáticos.

En la relación se reflejan los recursos a los cuales puede acceder cada usuario.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

10. GESTIÓN DE SOPORTES Y DOCUMENTOS

DEFINICIÓN

Artículo 92 Gestión de soportes.

1. Los apoyos informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenados en un lugar con acceso restringido al personal autorizado en el documento de seguridad.
2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero o debidamente autorizada en el Documento de Seguridad.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de la empresa para conocer el protocolo implantado para la identificación, inventariado y almacenaje de los soportes que contienen información, así como la salida de éstos fuera de FEDERACION GALEGA DE TAEKWONDO.

VERIFICACIÓN DE SU CUMPLIMIENTO

Tras entrevistar al Responsable de Seguridad, se verifica que las salidas de soportes y documentos fuera de FEDERACION GALEGA DE TAEKWONDO son autorizadas previamente por el Responsable de Fichero.

Se comprueba que en el Documento de Seguridad de FEDERACION GALEGA DE TAEKWONDO, existe una relación preestablecida de aquellos soportes y documentos, la salida de los cuales está previamente autorizada por el Responsable de Fichero.

Se cerciora que FEDERACION GALEGA DE TAEKWONDO adopta las medidas necesarias para evitar el acceso o recuperación de los soportes y/o documentos desechados.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

11. IDENTIFICACIÓN Y AUTENTIFICACIÓN

DEFINICIÓN

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que esté autorizado.
3. cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso superará el año, con la que tienen que ser cambiadas las contraseñas que, mientras sean vigentes habrán de ser guardadas de forma ininteligible.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al responsable de seguridad de FEDERACION GALEGA DE TAEKWONDO, requiriéndole acerca de la existencia de una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de procedimientos de identificación y autenticación para dicho acceso. Asimismo se requiere el procedimiento de asignación, distribución y almacenamiento de contraseñas así como su periodicidad de cambio.

VERIFICACIÓN DE SU CUMPLIMIENTO

FEDERACION GALEGA DE TAEKWONDO dispone de un mecanismo de acceso de los usuarios a los equipos informáticos que permite su identificación de forma inequívoca y personalizada.

Se comprueba que FEDERACION GALEGA DE TAEKWONDO dispone de un procedimiento de asignación, distribución y almacenamiento de contraseñas.

Mientras las contraseñas están en vigor, FEDERACION GALEGA DE TAEKWONDO las almacena de forma ininteligible.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

Que el propio sistema informático solicite el cambio de contraseña dentro del tiempo mínimo establecido.

12. COPIAS DE RESPALDO Y RECUPERACIÓN

DEFINICIÓN

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actualización como mínimo de forma semanal de las copias de respaldo, excepto si en este periodo no se hubiera producido ninguna actualización de los datos.
2. Los procedimientos establecidos para la realización de copias de seguridad y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en qué se encontraban en el momento de producirse la pérdida o destrucción.
3. El responsable del fichero se encargará de verificar semestralmente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de las copias de respaldo.
4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten datos de carácter personal no se realizarán con datos reales, excepto si se asegura el nivel de seguridad por el tratamiento realizado y se anote su realización en el Documento de Seguridad.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a analizar y comparar los procedimientos establecidos en el Documento de Seguridad sobre las copias de seguridad y los procedimientos de recuperación, con los procedimientos establecido físicamente y llevados a cabo diariamente por el personal de FEDERACION GALEGA DE TAEKWONDO.

VERIFICACIÓN DE SU CUMPLIMIENTO

Se comprueba que FEDERACION GALEGA DE TAEKWONDO realiza copias de respaldo de los sistemas de información que tratan datos de carácter personal.

Se ha desarrollado un procedimiento para la realización de las mismas, el cual se ha hecho constar en el Documento de Seguridad.

Las copias se realizan como mínimo semanalmente.

El Responsable de Fichero verifica semestralmente la correcta definición, funcionamiento y aplicación del procedimiento de copias de respaldo.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

Que el Responsable del Fichero realice, por lo menos semestralmente un informe de verificación.

13. CRITERIOS DE ARCHIVO

DEFINICIÓN

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de FEDERACION GALEGA DE TAEKWONDO para conocer si existe una norma aplicable para determinar los criterios de archivo.

VERIFICACIÓN DE SU CUMPLIMIENTO

Tras entrevistar al Responsable de Seguridad de FEDERACION GALEGA DE TAEKWONDO, se corrobora la existencia de un criterio de archivo para los soportes y documentos no automatizados que contienen datos personales. Y dicho criterio permite el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por parte del interesado.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

14. ALMACENAMIENTO DE LA INFORMACIÓN

DEFINICIÓN

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de FEDERACION GALEGA DE TAEKWONDO para conocer si dispone de mecanismo que obstaculice la apertura de los dispositivos de almacenamiento.

VERIFICACIÓN DE SU CUMPLIMIENTO

FEDERACION GALEGA DE TAEKWONDO dispone de mecanismos que obstaculizan la apertura en los dispositivos de almacenamiento.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

15. CUSTODIA DE SOPORTES

DEFINICIÓN

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al personal de FEDERACION GALEGA DE TAEKWONDO para corroborar que se custodia la documentación mientras no se encuentra archivada en los dispositivos de almacenamiento

VERIFICACIÓN DE SU CUMPLIMIENTO

Se constata que FEDERACION GALEGA DE TAEKWONDO custodia correctamente la documentación cuando ésta no se encuentra archivada en los dispositivos de almacenamiento.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

Se recomienda que FEDERACION GALEGA DE TAEKWONDO informe a todo el personal que tenga acceso a la documentación que mientras no esté archivada tiene que custodiarla de forma que impida en todo momento que la documentación pueda ser accedida por persona no autorizada.

16. AUDITORÍA

DEFINICIÓN

Artículo 96. Auditoría.

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

DATOS, HECHOS Y OBSERVACIONES

Se ha procedido a entrevistar al Responsable de Seguridad para comprobar las conclusiones de las anteriores Auditorías.

VERIFICACIÓN DE SU CUMPLIMIENTO

Tras entrevistar al Responsable de Seguridad, se verifica que la actual auditoría se encuentra dentro del plazo establecido por el Real Decreto 1720/2007, desde la anterior.

El presente informe dictamina sobre las medidas de seguridad implantadas por la empresa y constan las medidas correctoras o complementarias que se deberán adoptar para subsanar las incidencias detectadas, además, dicho informe será analizado por el Responsable de Seguridad que propondrá las conclusiones al Responsable del Fichero que adoptará las medidas correctoras necesarias.

Tras el examen realizado a la documentación aportada por FEDERACION GALEGA DE TAEKWONDO, se constata que se han implantado las medidas correctoras propuestas en las auditorías anteriores.

SALVEDADES

No existen.

PROPUESTA DE MEDIDAS CORRECTORAS

No existen.

PROPUESTA DE MEDIDAS COMPLEMENTARIAS

No existen.

RECOMENDACIONES DEL AUDITOR

No existen.

C. LUGAR DE REALIZACIÓN DEL TRABAJO

El desarrollo de la auditoría se ha realizado para la revisión in situ de las instalaciones de tratamiento de datos y sistemas de información en las oficinas de FEDERACION GALEGA DE TAEKWONDO situadas en PLAZA DE AGUSTIN DIAZ 3 15008, CORUÑA, A (A CORUÑA) y para la revisión de la documentación entregada en las oficinas del auditor.

Tanto el trabajo de auditoría como la elaboración del informe de auditoría han sido desarrollados por un equipo de personas constituido por Ingenieros de Telecomunicación y Abogados, trabajándose simultáneamente los aspectos técnicos y organizativos de la seguridad así como los legales.

Para la ejecución de este encargo de auditoría, se han llevado a cabo las siguientes acciones:

- Realización de la auditoría mediante entrevistas, revisión de documentos, y análisis y revisión de las medidas, controles y procedimientos de seguridad de FEDERACION GALEGA DE TAEKWONDO.
- Elaboración del informe de auditoría.

D. FASES DEL TRABAJO DE AUDITORÍA

El trabajo de auditoría se ha desarrollado cumpliendo los plazos establecidos. Las fases en que se ha dividido el desarrollo de las distintas actuaciones han sido las siguientes:

- Identificación de los interlocutores.
- Recogida de información.
- Estudio y análisis de la información.
- Aclaraciones.
- Entrega del informe.

E. MEDIDAS REVISADAS

La realización de la auditoría en FEDERACION GALEGA DE TAEKWONDO, así como el presente informe de auditoría se han llevado a cabo respecto a las siguientes medidas procedimientos y controles en materia de seguridad de datos:

Controles

Para todos los niveles de seguridad:

- Control de acceso de los usuarios a los datos y recursos que precisan para el desarrollo de sus funciones.
- Controles periódicos para verificar el cumplimiento de lo que dispone el Documento de Seguridad.
- Control de la existencia y cumplimiento de las medidas definidas en el documento de seguridad por el responsable de seguridad.
- Dictamen del informe de auditoría para comprobar la existencia de los controles al cumplimiento del reglamento.

Procedimientos

Para todos los niveles de seguridad:

- Procedimiento de notificación, gestión y respuesta delante de las incidencias.
- Procedimiento de realización de las copias de respaldo.
- Procedimiento de recuperación de los datos.
- Procedimiento de identificación para el acceso de los usuarios al sistema de información.
- Procedimiento de autenticación para el acceso de los usuarios al sistema de información.
- Procedimiento de asignación, distribución y almacenamiento de contraseñas.

Medidas

Para todos los niveles de seguridad:

- Acceso a datos a través de las redes de comunicación.
- Régimen de trabajo fuera de los locales de ubicación del fichero. Ficheros temporales.
- Documento de Seguridad.
- Funciones y obligaciones del personal.
- Gestión de soportes.
- Nombramiento de uno o varios responsables de Seguridad.
- Realización de una auditoría bianual.

Calendario de entrevistas

Para el desarrollo del trabajo de auditoría y elaboración del informe se han realizado las siguientes entrevistas:

LUGAR	AÑO	NOMBRE Y APELLIDOS	CARGO Y DEPARTAMENTO	DOCUMENTACIÓN APORTADA
CORUÑA, A	2016	JUAN CARLOS CAINZOS	ADMINISTRATIVO	DOCUMENTO SEGURIDAD

F. DOCUMENTACIÓN ENTREGADA

Para el desarrollo del trabajo de auditoría y elaboración del informe se ha analizado la siguiente documentación:

TITULO DEL DOCUMENTO	ORIGINAL O COPIA	BREVE REFERENCIA DEL CONTENIDO
DOCUMENTO DE SEGURIDAD	COPIA	DOCUMENTO DE SEGURIDAD DE LA EMPRESA
COMPROMISO DE CONFIDENCIALIDAD	COPIA	DOCUMENTO DE CONFIDENCIALIDAD DE LA EMPRESA
COMUNICADO INTERNO	COPIA	DOCUMENTO UTILIZADO PARA LA EMPRESA PARA COMUNICAR FUNCIONES Y OBLIGACIONES RELATIVAS A LA LOPD
CONTRATOS DE PRESTACIÓN DE SERVICIOS	COPIA	CONTRATOS DE PRESTACIÓN DE SERVICIOS CON LOS PRESTADORES DE LA EMPRESA
RELACIÓN DE USUARIOS	COPIA	RELACIÓN DONDE CONSTA EL NOMBRE DE USUARIO, SU IDENTIFICACIÓN Y LA APLICACIÓN A LA QUE ACCEDE.
TRATAMIENTO DE DISPOSITIVOS PORTÁTILES	COPIA	RELACIÓN DONDE CONSTAN LOS DISPOSITIVOS PORTÁTILES DE LA EMPRESA.

CONVERSIA, con plena libertad, ha aceptado el encargo de FEDERACION GALEGA DE TAEKWONDO para realizar una auditoría de medidas de seguridad y el informe correspondiente sobre la misma, de acuerdo con el artículo 96 del RD 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley 15/1999 de protección de Datos de Carácter Personal, al objeto de verificar si los sistemas de información e instalaciones de tratamiento de datos propiedad de FEDERACION GALEGA DE TAEKWONDO cumplen con lo establecido en el citado Reglamento, los procedimientos en el mismo obrantes, así como las instrucciones vigentes dictadas por la Agencia Española de Protección de Datos en materia de seguridad de datos.

CONVERSIA garantiza que dicha auditoría ha sido realizada conforme a las condiciones, duración, alcance y régimen económico establecidos y bajo los criterios de independencia, imparcialidad y objetividad, y sin otras limitaciones que las impuestas por la ley, las normas éticas y deontológicas.

CONVERSIA ha cumplido con su objetivo de realizar la auditoría de medidas de seguridad y el informe correspondiente sobre la misma con el máximo celo y diligencia. Guardará el secreto profesional por tiempo indefinido sobre todos los datos, hechos y observaciones de los que tenga conocimiento así como sobre las valoraciones que realice por razón de cualquiera de las modalidades de su actuación profesional. Ha acometido este encargo ateniéndose a las exigencias técnicas, deontológicas y éticas adecuadas a la tutela de dicho asunto, habiéndose apoyado para ello en sus colaboradores y otros compañeros, quienes han actuado bajo su responsabilidad, guardando el mismo nivel de secreto y con las mismas exigencias técnicas, deontológicas y éticas.

La realización de la auditoría se ha realizado debidamente, sin limitaciones ni restricciones que pudieran entorpecer la labor del auditor.

En CORUÑA, A a 5 de febrero de 2016,

Para finalizar el presente informe de auditoría independiente del cumplimiento de medidas de seguridad de las instalaciones y tratamientos de datos de carácter personal de personas físicas, a continuación se presentan las conclusiones del mismo para un rápido conocimiento de la situación en que se encuentra FEDERACION GALEGA DE TAEKWONDO.

En opinión del auditor, la situación de FEDERACION GALEGA DE TAEKWONDO con relación al nivel de cumplimiento de la legislación vigente en materia de seguridad de los datos de carácter personal respecto de sus instalaciones y tratamientos es FAVORABLE.

Además, se han propuesto una serie de recomendaciones respecto a las medidas de seguridad que se adecuan a la legislación vigente a fin de mejorar la seguridad de los datos de FEDERACION GALEGA DE TAEKWONDO, que si bien no son de obligado cumplimiento, sí recomendamos que sean valoradas.

Se pone en conocimiento de FEDERACION GALEGA DE TAEKWONDO que se encuentra sujeta al régimen sancionador establecido en la Ley Orgánica de Protección de Datos, así como que las infracciones en materia de seguridad y, en concreto, mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad establecidas en el Reglamento de Medidas de Seguridad, están tipificadas por la LOPD como infracción grave con sanción de desde CUARENTA MIL UN EUROS A TRESCIENTOS MIL EUROS (40.001 a 300.000 €).

Por último, se recuerda a FEDERACION GALEGA DE TAEKWONDO, por un lado, que el responsable de seguridad de FEDERACION GALEGA DE TAEKWONDO debe analizar el presente informe de auditoría y elevar a FEDERACION GALEGA DE TAEKWONDO las conclusiones que resulten para que ésta adopte las medidas correctoras adecuadas y, por otro lado, que ambos informes –el que elabore el responsable de seguridad y el presente documento- deberán estar a disposición de la Agencia Española de Protección de Datos.

Firmado:

Departamento Auditoría