DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL RGPD Y LOPD-GDD EN CUANTO A LA REALIZACIÓN DE LA EIPD PARA EL TRATAMIENTO DE DATOS PARA EL REGISTRO DE LA JORNADA LABORAL

CONSULTING & STRATEGY GFM S.L. (GFM SERVICIOS) con CIF B71198543, en calidad de representante legal de **SEÑORÍO DE ZUASTI GOLF CLUB S.A.,** con domicilio en Calle San Andrés, 1 – 31892 Zuasti (Navarra) y CIF A31470834.

DECLARA

Que dicha entidad pública ha implantado los requisitos y medidas que exige al REGLAMENTO (UE) 2016/679, de 27 de abril de 2016 del Parlamento Europeo y del Consejo relativo a la Protección de personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismo, en adelante (el RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante (la LOPDPGDD), en relación con la obligación que establece el artículo 35, RGPD UE 2016/679, de realizar una Evaluación de Impacto en la Protección de Datos (EIPD) en cuanto al tratamiento de datos biométricos, en este caso, tratamientos de datos para acceso mediante reconocimiento facial.

Artículo 35. Evaluación de impacto relativa a la protección de datos

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

En concreto, en la elaboración de la EIPD se han desarrollado los siguientes apartados:

ÍNDICE

RESUMEN DE EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

CONTROL DE ACCESOS MEDIANTE RECONOCIMIENTO FACIAL

1. DATOS DEL RESPONSABLE

Datos de contacto del responsable

SEÑORIO DE ZUASTI GOLF CLUB S.A.

A31470834

CL. SAN ANDRES 1 - 31892 - ZUASTI - NAVARRA

948302900

zuasti@zuasti.com

Delegado de Protección de Datos

CONSULTING & STRATEGY GFM S.L.

B71198543

CALLE BERROA, 19, PLANTA 5, OFICINA 509 – 31192 TAJONAR (NAVARRA)

dpo@gfmservicios.com

29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543)

Firmado digitalmente por 29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543)
Nombre de reconocimiento (DN): 2.5.4.13=Reg:31015 /Hoja:NA-34347 / Tomo:1732 /Folio:35 / Fecha:27/08/2014 /Inscripción:1, serialNumber=IDCES-29148475T, givenName=GONZALO, sn=FERNANDEZ MICHELTORENA ARAMENDIA, cn=29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543), 2.5.4.97=VATES-B71198543, o=CONSULTING & STRATEGY GFM SL, c=ES
Fecha: 2022.08.02 10:57:46 +02'00'

2. DATOS DE LA EIPD

2.1. NOMBRE DE LA EIPD

CONTROL DE ACCESOS MEDIANTE RECONOCIMIENTO FACIAL

2.2. NOMBRE DEL TRATAMIENTO SOBRE EL QUE SE HA REALIZADO

CONTROL DE ACCESOS MEDIANTE RECONOCIMIENTO FACIAL

2.3. FECHA DE REALIZACIÓN Y VERSIÓN

Fecha: 20/06/2022

Versión: V1

Estado: Finalizada

2.4. AUTOR/ES

Esta EIPD ha sido realizada por:

JABI GALLEGO CENOZ

Consultor / Responsable EIPD Consulting & Strategy GFM S.L.

2.5. REVISOR/ES

Esta EIPD ha sido revisada por:

GONZALO FDEZ.-MICHELTORENA

DPO SEÑORÍO DE ZUASTI GOLF CLUB S.A.

2.6. VALIDADOR/ES

Esta EIPD ha sido validada por:

GONZALO FDEZ.-MICHELTORENA

DPO SEÑORÍO DE ZUASTI GOLF CLUB S.A.

LEYRE TORRES

GERENTE SEÑORÍO DE ZUASTI GOLF CLUB S.A.

2.7. RESPONSABILIDADES EN EL PROYECTO

Para llevar a cabo este proyecto, ha sido necesaria la colaboración de los siguientes actores:

Identificación	Tipo	Descripción
SEÑORÍO DE ZUASTI GOLF CLUB S.A.	Responsable del tratamiento	Como Responsable de Tratamiento es la organización obligada a realizar la EIPD previa al tratamiento de datos para la utilización de sistemas de acceso mediante reconocimiento facial, empleando para ello datos biométricos (imagen facial).
DAS GATE	Encargado del tratamiento	Se trata de del proveedor del servicio relativo a los sistemas de acceso mediante reconocimiento facial. Como Encargado de Tratamiento, según el artículo 28 RGPD, debe cumplir las obligaciones en materia de protección de datos exigidas por el Derecho de la Unión y por el Derecho Nacional. Además, tiene la responsabilidad de haber realizado un análisis de riesgo de las tecnologías empleadas para realizar el control de acceso mediante sistemas de reconocimiento facial.
ASPECT CONSULTING	Encargado del tratamiento	Como Encargado de tratamiento, según el artículo 28 RGPD, debe cumplir las obligaciones en materia de protección de datos exigidas por el Derecho de la Unión y por el Derecho Nacional. Se trata de la empresa que facilita al

Identificación	Tipo	Descripción
		Responsable de Tratamiento los servicios para la apertura de los tornos y registro de las entradas y salidas de las personas usuaria de sus instalaciones.
CONSULTING & STRATEGY GFM S.L.	Tercero	Como DPO del Responsable de Tratamiento, además de las obligaciones generales establecidas por el RGPD para la figura del Delegado de Protección de Datos, en relación con la realización de una EIPD tiene la obligación de supervisarla y validarla, de forma que acredite que no existen riesgos para los derechos y libertades de las personas usuarias inherentes al tratamiento de datos analizado.

3. DESCRIPCIÓN DEL TRATAMIENTO

3.1. DATOS GENERALES

DATOS GENERALES DEL TRATAMIENTO

Nombre: CONTROL DE ACCESOS MEDIANTE RECONOCIMIENTO FACIAL

Finalidad: Control de acceso de las personas usuarias del club y sus trabajadores mediante sistemas de reconocimiento facial basados en la generación de un vector irreversibles a través de un sistema de inteligencia artificial.

Descripción detallada del tratamiento: El presente tratamiento se lleva a cabo con la finalidad de controlar los accesos y salidas de las instalaciones del responsable de tratamiento, teniendo su base legal en el consentimiento de las personas interesadas. Para realizar el presente tratamiento se requiere la lectura de la imagen facial de la persona interesada para la generación de un vector irreversible que, posteriormente, será almacenado en una base de datos; este vector quedará asociado a los datos identificativos de la persona interesada. A partir de ahí, cada vez que la persona interesada pretenda acceder/salir de las instalaciones del Responsable de Tratamiento, se generará un nuevo vector que buscará coincidencia con los vectores irreversibles almacenados, permitiendo la apertura de los tornos en caso de coincidencia.

BASE JURÍDICA

- Consentimiento del interesado: Artículo 6.1 a) RGPD: al tratarse de un sistema de acceso mediante datos biométricos y ser éstos una categoría especial de datos según el artículo 9.2 RGPD, es necesario que las personas usuarias den su consentimiento para el tratamiento de sus datos mediante esta tecnología.

CATEGORÍAS DE INTERESADOS

Personas usuarias del Club; Trabajadores del Club.

Categorías: Clientes y usuarios; Empleados

CATEGORÍAS DE DATOS PERSONALES

Identificación: NIF/DNI; Nombre y apellidos; Firma; Imagen/Voz; Dirección de correo electrónico.

Características personales: Datos de estado civil; De familia; Fecha y lugar de nacimiento; Edad; Sexo; Nacionalidad; Lengua Materna y Características física o antropométricas; Datos de empleo.

Datos especiales: Datos biométricos.

CATEGORÍAS DE DESTINATARIOS

Organizaciones o personas relacionadas directamente con el Responsable del tratamiento.

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Los datos se suprimirán a solicitud del interesado y, en todo caso, en los plazos legalmente previstos o al finalizar la relación contractual entre las partes.

3.2. VOLUMEN Y EXTENSIÓN DEL TRATAMIENTO

El volumen de interesados objeto del tratamiento, así como la extensión del mismo, se indican en la siguiente tabla:

Interesados objeto del tratamiento	Socios/as, abonados/as y trabajadores/as del Club
Duración del tratamiento	Años
Extensión geográfica del tratamiento	Nacional

4. ANÁLISIS DE LA NECESIDAD DE REALIZAR UNA EIPD

A continuación, se muestra el análisis que se ha realizado sobre cada uno de los tratamientos para valorar si es necesario, o no, realizar una evaluación de impacto relativa a la protección de datos.

CONTROL DE ACCESOS MEDIANTE RECONOCIMIENTO FACIAL
ANÁLISIS
• El tratamiento está incluido en la lista de actividades de tratamiento publicada por la AEPD que SÍ requieren de EIPD • Toma de decisiones automatizada con efecto jurídico significativo o similar: tratamiento destinado a tomar decisiones sobre los interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar». Por ejemplo, el tratamiento puede provocar exclusión o discriminación contra las personas. El tratamiento con poco o ningún efecto sobre las personas no coincide con este criterio específico • Datos sensibles o datos muy personales: esto incluye las categorías especiales de datos personales, así como datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas. Un ejemplo sería un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes. Más allá de estas disposiciones del RGPD, puede considerarse que algunas categorías de datos aumentan el posible riesgo para los derechos y libertades de las personas. Estos datos personales se consideran sensibles (dado que este término es de uso común) porque están vinculados a hogares y actividades privadas (como comunicaciones electrónicas cuya confidencialidad debe ser protegida), porque afectan al ejercicio de un derecho fundamental (como datos de localización cuya recogida compromete la libertad de circulación) o porque su violación implica claramente graves repercusiones en la vida cotidiana del interesado (como datos financieros que podrían usarse para cometer fraude en los pagos). En este sentido, puede resultar relevante que los datos ya se hayan hecho públicos por el interesado o por terceras personas. El hecho de que los datos personales sean de acceso público puede considerarse un factor en la evaluación si estaba previsto que estos se usaran para ciertos fines. Este criterio también puede incluir datos tales como documentos personales, correos electrónicos, diarios, notas de lectores de libros electrónicos equipados con opciones para tomar notas e información muy personal incluida en aplicaciones de registro de actividades vitales • Asociación o combinación de conjuntos de datos: por ejemplo procedentes de dos o más operaciones de tratamiento de datos realizadas para distintos fines o por responsables del tratamiento distintos de una manera que exceda las expectativas razonables del interesado • Datos relativos a interesados vulnerables: el tratamiento de este tipo de datos representa un criterio debido al aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento, lo cual implica que las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos, o de ejercer sus derechos. Entre los interesados vulnerables puede incluirse a niños (se considera que no son capaces de denegar o autorizar consciente y responsablemente el tratamiento

de sus datos), empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.), y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento

- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas: como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD

- Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato»: esto incluye operaciones de tratamiento destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. Un ejemplo de esto sería cuando un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo

- En primer lugar, hay que hacer referencia al artículo 35 del Reglamento (UE) 2016/679, en el que se establece que se requerirá la realización de una Evaluación de Impacto en la Protección de Datos (EIPD) en aquellos tratamientos de datos que puedan entrañar un alto riesgo para los derechos y libertades de las personas interesadas. Asimismo, este artículo establece la obligación de las autoridades de control nacionales, en este caso la Agencia Española de Protección de Datos (AEPD), de establecer un listado de tratamiento de datos que requerirán la realización de una EIPD previa al inicio del tratamiento de los datos. En este sentido, y en segundo lugar, la AEPD, atendiendo a las directrices establecidas por el Grupo de Trabajo del artículo 29 (GT29) en sus Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD), ha establecido la obligatoriedad de realizar una EIPD en aquellos tratamientos que se encuentren recogidos dentro de dos o más de los supuestos más arriba analizados. En definitiva, al tratarse de una utilización de datos biométricos para permitir el acceso y la salida de las personas usuarias de las instalaciones del Responsable de Tratamiento, y tratándose de una categoría de datos especialmente protegida, y en atención a las consideraciones antes expuestas, se ha determinado la necesidad de realizar una EIPD previa a la iniciación de dicho tratamiento.

CONCLUSIÓN

Se requiere EIPD, pues es un tratamiento que se va a llevar a cabo y se considera que es probable que exista un alto riesgo para los derechos y las libertades de los interesados

5. METODOLOGÍA DE LA EIPD

5.1. DOCUMENTACIÓN DE REFERENCIA

Para llevar a cabo esta Evaluación de Impacto relativa a la Protección de Datos (EIPD) se ha utilizado la siguiente documentación de referencia:

- Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD de la Agencia Española de Protección de Datos.
- Norma ISO/IEC 29134:2017. *Guidelines for privacy impact assessment*.
- Norma ISO/IEC 27005:2018. *Information security risk management*.
- Norma UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información.
- Norma UNE-EN ISO/IEC 27002:2017. Código de prácticas para los controles de seguridad de la información.
- Norma ISO/IEC 27701:2019. *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -Requirements and guidelines-.*
- Norma ISO/IEC 29151:2017. *Code of practice for personally identifiable information protection.*

5.2. METODOLOGÍA EMPLEADA

La presente EIPD se ha realizado siguiendo esta metodología:

1. **Determinar si es necesario realizar una EIPD:** en esta fase previa, se realiza un análisis preliminar de la necesidad de realizar una EIPD. Si no se necesita, se justifica y documenta por qué no es necesario realizar una EIPD y el proceso finaliza en este punto; en cambio, si el análisis revela que hay que realizar una EIPD, se justifica y documenta la necesidad de realizarla y se continua en el siguiente punto.
2. **Preparación de la EIPD:** se establece un equipo de trabajo y se le facilitan los recursos necesarios para su desempeño.

3. **Participación de los interesados:** si es necesaria la participación de los interesados en la EIPD, se identifican los interesados a los que se va a consultar y se establece un plan de consulta y comunicación, registrándose las respuestas y comentarios de los mismos.

4. **Análisis detallado del tratamiento:** en esta fase se describe todo el ciclo de vida de los datos personales (captura de datos, clasificación/almacenamiento, uso/tratamiento, cesión/transferencia de datos a un tercero y destrucción), incluyendo los siguientes aspectos:

    a. Datos tratados: se detallan las categorías de datos involucradas en cada fase del ciclo de vida de los datos.

    b. Actividades u operaciones: se detallan las distintas actividades u operaciones que se llevan a cabo sobre los datos personales, con el objetivo de comprender los posibles riesgos a los que se pueden ver expuestos los datos.

    c. Intervinientes: se detallan las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en el desarrollo de las actividades de tratamiento (responsables, áreas o empleados, encargados del tratamiento, etc.)

    d. Tecnología: se detallan, a un alto nivel, aquellos elementos tecnológicos que intervienen en las actividades de tratamiento de los datos. Se identifica la tecnología (cloud, BBDD, servidores), aplicaciones, dispositivos y técnicas empleadas en el procesamiento de los datos.

5. **Análisis de la necesidad y proporcionalidad del tratamiento:** se realiza un análisis para justificar, adecuadamente, la necesidad y proporcionalidad de las actividades de tratamiento en relación a las finalidades del mismo.

6. **Análisis y gestión de riesgos:** se realiza un análisis de los riesgos de privacidad y cómo se van a tratar dichos riesgos para reducirlos hasta un umbral aceptable. Esto comprende las siguientes actividades:

    - Identificar amenazas, vulnerabilidades y riesgos.

    - Evaluar los riesgos identificados.

- Tratar los riesgos.

7. **Medidas de seguridad:** se documentan detalladamente las medidas de seguridad que se aplicarán al tratamiento para reducir el riesgo hasta un umbral aceptable.

8. **Conclusión:** basándose en el riesgo residual obtenido durante la fase de análisis y gestión de riesgos, debe valorarse si éste es elevado o se considera aceptable y dentro de unos límites razonables.

9. **Comunicación y consulta a la autoridad de control:** en caso de que el riesgo residual del tratamiento sea alto o muy alto, debe realizarse una consulta a la Autoridad de Control mediante los canales de comunicación establecidos.

10. **Supervisión y revisión de la implantación:** como último paso de la EIPD, debe realizarse una adecuada supervisión y una posterior revisión de la implantación de las medidas de seguridad y control definidas en el punto 7 para reducir el riesgo inherente hasta un riesgo residual que permite llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas.

6. NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

El principio de "minimización de datos" establece que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que serán tratados".

La proporcionalidad es otro de los aspectos que deben evaluarse antes de realizar un tratamiento de datos personales: analizar si la finalidad puede conseguirse por otros medios que impliquen menos riesgos.

A continuación, se detalla el análisis realizado sobre estos aspectos.

6.1. LEGITIMACIÓN

La base jurídica que legitima el tratamiento se indica a continuación:

- Consentimiento del interesado: Artículo 6.1 a) RGPD: al tratarse de un sistema de acceso mediante datos biométricos y ser éstos una categoría especial de datos según el artículo 9.2 RGPD, es necesario que las personas usuarias den su consentimiento para el tratamiento de sus datos mediante esta tecnología.

6.2. EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

Se han analizado de forma metódica los datos recogidos, sus usos, las tecnologías empleadas y el periodo de conservación de los datos para analizar la necesidad y proporcionalidad del tratamiento.

8. ANÁLISIS Y GESTIÓN DE RIESGOS

8.1. OBJETO DEL ANÁLISIS DE RIESGOS

La gestión de riesgos, es el proceso de identificar, analizar y valorar la probabilidad e impacto derivados de la posibilidad de que se materialicen las distintas amenazas que acechan a la seguridad de los datos personales, para establecer las acciones correctivas que permitan minimizar la exposición al riesgo.

Para ello, se ha realizado un análisis de riesgos en el que se han identificado, de forma metódica, las amenazas a las que los datos personales están expuestos, así como las vulnerabilidades que pueden aprovechar dichas amenazas para tener éxito.

Se ha estimado también el daño que podrían producir las distintas amenazas en caso de que se materializasen, así como la probabilidad de su ocurrencia.

Con estos datos, se ha realizado una estimación del nivel de riesgo y se han tomado las decisiones pertinentes para gestionar estos riesgos, identificando las medidas de seguridad necesarias para eliminar o reducir aquellos riesgos que se ha decidido gestionar.

8.2. METODOLOGÍA DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Para realizar un análisis de riesgos, es preciso, en primer lugar, definir la metodología para evaluar y gestionar los riesgos a que están expuestos los tratamientos de datos personales.

La evaluación y gestión de los riesgos se aplica a todos los tratamientos de datos personales que la entidad realice y sobre todos los activos que están involucrados en los mencionados tratamientos de datos personales.

A continuación, se detalla la metodología utilizada para el análisis y gestión de los riesgos.

Para la elaboración de la metodología se han tenido en cuenta los siguientes documentos:

- Norma UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información.
- Norma ISO/IEC 27005:2018. *Information security risk management*.
- Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la AEPD.
- Norma UNE-EN ISO/IEC 27002:2017. Código de prácticas para los controles de seguridad de la información.
- Norma ISO/IEC 27701:2019. *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -Requirements and guidelines-.*
- Norma ISO/IEC 29151:2017. *Code of practice for personally identifiable information protection.*

8.2.1. DEFINICIONES

Para comprender la metodología del análisis y gestión de riesgos se han de tener claros los siguientes conceptos:

- **Análisis de riesgos:** utilización sistemática de la información disponible para identificar los peligros y estimar los riesgos.
- **Confidencialidad:** es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- **Integridad:** propiedad de la información, por la que se garantiza que no ha sido alterada de manera no autorizada.
- **Disponibilidad:** propiedad de la información, por la que se garantiza que está disponible para su uso a demanda de una entidad autorizada.
- **Seguridad de la información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- **Activo:** componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la seguridad de la información (son activos los datos, los servicios, las aplicaciones, los equipos, soportes, instalaciones o el personal, entre otros).
- **Amenaza:** toda circunstancia, evento o persona que tiene el potencial de causar daño en forma de robo, destrucción, divulgación, modificación de datos o denegación de servicio.
- **Vulnerabilidad:** debilidad o necesidad de un activo a través de la cuál una amenaza puede causar un daño.
- **Impacto:** es el daño que se produce al materializarse una amenaza.
- **Nivel de riesgo:** es la combinación de las consecuencias de un suceso (impacto) y de su probabilidad. Riesgo = Impacto x Probabilidad.
- **Control:** medida que modifica un riesgo.

8.2.2. PROCESO

El análisis de riesgos se ha realizado a través de un proceso metódico que sigue los siguientes pasos:

1. Se identifican todos los activos primarios de información involucrados en el tratamiento de los datos personales.
2. Se identifica y valora el impacto que podría suponer para los interesados, en las distintas dimensiones de la seguridad de la información (confidencialidad, integridad y disponibilidad) si a consecuencia de la materialización de alguna amenaza, resultasen dañadas.
3. Se identifican los distintos activos que dan soporte a los activos primarios de información (hardware, software, soportes, etc.) y se vinculan a los activos primarios de información concretos a los que prestan soporte.
4. Se identifican las distintas amenazas a que están expuestos esos activos que podrían comprometer la confidencialidad, integridad o disponibilidad de la información.

5. Se identifican las distintas vulnerabilidades de los activos que pueden aprovechar las mencionadas amenazas para causar su daño.
6. Se estima la frecuencia con que se presenta cada una de las amenazas, así como el grado de vulnerabilidad de los distintos activos para calcular la probabilidad de que las distintas amenazas se materialicen aprovechando las vulnerabilidades identificadas.
7. Se calcula el nivel de riesgo para cada par de amenaza-vulnerabilidad. Este nivel de riesgo se calcula en base al impacto y la probabilidad que se ha analizado en los pasos previos.
8. Se evalúa y decide cuáles son los riesgos que se van a gestionar en base a los criterios establecidos en la metodología.
9. Se identifican los controles necesarios para gestionar los riesgos.
10. Se vuelve a calcular el nivel de riesgo considerando los controles seleccionados para calcular el nivel de riesgo residual.
11. Si el nivel de riesgo residual no es aceptable, se repite de nuevo el proceso desde el punto 8.
12. Si no es posible bajar más el riesgo a un umbral aceptable, no se podría llevar a cabo el tratamiento y sería necesario activar el procedimiento de consulta previa a la Autoridad de Control.
13. Se deben describir en detalle las medidas de seguridad que se van a aplicar para una implantación efectiva de las mismas en la organización.
14. Se debe documentar todo el proceso, así como la conclusión del mismo.

A continuación veremos detalladamente cómo se recopila la información necesaria en cada uno de estos ámbitos y cómo se realizan los cálculos indicados anteriormente.

8.2.3. IDENTIFICACIÓN DE LOS ACTIVOS PRIMARIOS DE INFORMACIÓN

El primer paso que se debe dar en el análisis de riesgos es identificar todos los activos que están involucrados en el tratamiento de los datos personales.

Los activos pueden distinguirse en:

- Activos primarios:
  - Procesos de negocio y actividades.
  - Información.
- Activos de soporte (en los que se apoyan los activos primarios):
  - Hardware.
  - Software.
  - Comunicaciones.
  - Personal.
  - Instalaciones.

En esta fase se identificarán los activos primarios de información (que pueden ser los mismos en todo el ciclo de vida de la información, o no).

8.2.4. IDENTIFICACIÓN Y VALORACIÓN DEL IMPACTO

A continuación debe identificarse el daño que se podría causar a los interesados en caso de que se viese afectada la confidencialidad, integridad o disponibilidad de la información de los distintos activos primarios de información.

Se describirán los posibles daños, así como el impacto estimado en cada dimensión de la seguridad de la información.

Para estimar el impacto, el considerando 75 del Reglamento General de Protección de Datos de Europa y el artículo 28 de la Ley 3/2018, de Protección de Datos Personales y garantía de derechos digitales, indican una serie de factores o supuestos asociados a riesgos para los derechos y libertades de los interesados, que se detallan aquí:

- El tratamiento puede provocar daños y perjuicios físicos, materiales o inmateriales.
- El tratamiento puede dar lugar a problemas de discriminación.
- El tratamiento puede dar lugar a problemas de usurpación de identidad o fraude.
- El tratamiento puede dar lugar a problemas de pérdidas financieras.
- El tratamiento puede dar lugar a problemas de daño para la reputación.
- El tratamiento puede dar lugar a problemas de pérdida de confidencialidad de datos sujetos al secreto profesional.
- El tratamiento puede dar lugar a problemas de reversión no autorizada de la seudonimización.
- El tratamiento puede dar lugar a un perjuicio económico, moral o social significativo.
- Existe privación a los interesados de sus derechos y libertades.
- Se impide a los interesados ejercer el control sobre sus datos personales.
- Se produce un tratamiento no meramente incidental o accesorio de las categorías de datos siguientes:
    - Datos biométricos dirigidos a identificar de manera unívoca a una persona física.
    - Datos que revelan el origen étnico o racial.
    - Datos que revelan las opiniones políticas.
    - Datos que revelan la religión o las creencias filosóficas.
    - Datos que revelan la militancia en sindicatos.
    - Datos relativos a la salud.
    - Datos genéticos.
    - Datos relativos a la vida sexual o la orientación sexual.

    - Datos sobre condenas e infracciones penales o medidas de seguridad conexas.
    - Datos relacionados con la comisión de infracciones administrativas.
- Se evalúan aspectos personales con el fin de crear o utilizar perfiles personales de los mismos.
- Se realiza el análisis o predicción de aspectos referidos al rendimiento en el trabajo.
- Se realiza el análisis o predicción de aspectos referidos a la situación económica.
- Se realiza el análisis o predicción de aspectos referidos a la salud.
- Se realiza el análisis o predicción de aspectos referidos a preferencias o intereses personales.
- Se realiza el análisis o predicción de aspectos referidos a la fiabilidad o el comportamiento.
- Se realiza el análisis o predicción de aspectos referidos a la solvencia financiera.
- Se realiza el análisis o predicción de aspectos referidos a la localización o movimientos.
- Se tratan datos de grupos de personas en situación de especial vulnerabilidad (menores, discapacitados u otros).
- El tratamiento implica a un gran número de personas o conlleva la recogida de una gran cantidad de datos personales.
- Los datos personales son, habitualmente, objeto de transferencia a terceros países u organizaciones internacionales respecto de los que no se ha declarado un nivel adecuado de protección.

A la hora de estimar el impacto a cada activo primario de información se ha valorado, de forma metódica, la concurrencia de que una o varias de estas situaciones afecte a cada uno de los tratamientos que la organización realiza.

La escala utilizada para valorar el impacto es la siguiente:

IMPACTO	DESCRIPCIÓN
Muy bajo	La pérdida de la confidencialidad, disponibilidad o integridad apenas afecta a los derechos y libertades de los interesados.
Bajo	La pérdida de la confidencialidad, disponibilidad o integridad afecta de forma leve a los derechos y libertades de los interesados de forma reducida.
Medio	Se da alguno de los factores o supuestos asociados a los riesgos indicados anteriormente, pero de forma muy reducida.
Alto	Se da alguno de los factores o supuestos asociados a los riesgos indicados anteriormente.
Muy alto	Concurren dos o más de los factores o supuestos asociados a los riesgos indicados anteriormente.

8.2.5. IDENTIFICACIÓN DE LOS ACTIVOS DE SOPORTE

En esta fase se identificarán los activos de soportes, es decir, aquellos activos en los que se apoyan los activos primarios de información.

Se identificarán los activos de soporte y se asociarán a los activos primarios de información para vincular las dependencias entre ellos y que el impacto se traslade de los activos primarios de información a los activos de soporte.

Los activos de soporte que se deben identificar son, entre otros:

- Hardware.
- Software.
- Comunicaciones.
- Personal.
- Instalaciones.

Para mejorar la eficiencia del proceso, los activos de soporte se podrán agrupar en "grupos de activos" siempre que se cumplan estas tres condiciones:

1. Que los activos sean del mismo tipo (con lo cual, estarán expuestos a los mismos tipos de amenazas y tendrán idénticas vulnerabilidades).
2. Que los activos estén sometidos a las mismas condiciones y circunstancias (con lo cual, la frecuencia con la que se presentan las amenazas al activo y el grado de vulnerabilidad del activo serán similares).
3. Que dichos activos de soporte se utilicen para tratar los mismos activos primarios de información (con lo cual, el impacto que se traslade a dichos activos de soporte será idéntico).

8.2.6. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

El siguiente paso es identificar todas las amenazas y vulnerabilidades que están relacionadas con cada uno de los activos antes identificados. Hay que contemplar todas las amenazas que puedan afectar a la confidencialidad, integridad o disponibilidad de los datos personales que se están tratando.

Cada activo puede estar relacionado con varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

8.2.7. EVALUACIÓN DE LA PROBABILIDAD

Para calcular el riesgo, es también necesario evaluar la probabilidad de que se materialice cada una de las amenazas identificadas; es decir, la probabilidad de que una amenaza aproveche una vulnerabilidad del activo en cuestión para materializarse.

Los factores que hay que tener en cuenta para estimar la probabilidad son, entre otros, los siguientes:

- El contexto del tratamiento y de los activos involucrados (personal en la organización, accesibilidad de los activos, entorno, etc.).
- La frecuencia con que se presenta la amenaza.
- El grado de exposición del activo a la amenaza.
- La vulnerabilidad del activo frente a la amenaza.

- La facilidad de explotar la vulnerabilidad para el atacante.
- Lo apetecible o valiosa que es la información para terceros (que puede tener, o no, relación con el impacto valorado).
- El histórico de la organización (cuántas veces se ha materializado la amenaza anteriormente).

La probabilidad depende de la frecuencia con la que se presente la amenaza al activo en cuestión y de lo vulnerable que sea ese activo frente a esa amenaza concreta.

La escala utilizada para valorar la frecuencia de la amenaza es la siguiente:

FRECUENCIA AMENAZA	**DESCRIPCIÓN**
Nula	No es posible que la amenaza se presente.
Muy baja	La amenaza se presenta una vez al año.
Baja	La amenaza se presenta una vez cada seis meses.
Media	La amenaza se presenta una vez al mes.
Alta	La amenaza se presenta una vez a la semana.
Muy alta	La amenaza se presenta todos los días.

La escala utilizada para valorar el grado de vulnerabilidad es la siguiente:

GRADO VULNERABILIDAD	DESCRIPCIÓN
Nulo	El activo no tiene vulnerabilidades para esa amenaza.
Muy bajo	Es extremadamente difícil que una amenaza se materialice explotando la vulnerabilidad del activo.
Bajo	Es difícil que una amenaza se materialice explotando la vulnerabilidad del activo.
Medio	Es posible que una amenaza se materialice explotando la vulnerabilidad del activo.
Alto	Es fácil que una amenaza se materialice explotando la vulnerabilidad del activo.
Muy alto	Es extremadamente fácil que una amenaza se materialice explotando la vulnerabilidad del activo.

Para realizar el cálculo de la frecuencia y la vulnerabilidad, hay que realizarlo sin considerar las medidas de seguridad existentes.

Esto arrojará el riesgo “natural” de los activos a cada amenaza y vulnerabilidad identificadas si no hay medidas de seguridad que lo mitiguen.

8.3. PROCESO DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Todo el proceso de análisis y gestión de riesgos ha sido realizado de acuerdo a la metodología de análisis y gestión de riesgos detallada en el apartado anterior.

8.3.1. OBJETIVO DEL ANÁLISIS Y LA GESTIÓN DE RIESGOS

El objetivo del análisis de riesgos es identificar, de forma metódica, todos los activos involucrados en el tratamiento de datos personales en la organización, así como sus vulnerabilidades y las amenazas que pueden aprovechar esas vulnerabilidades para causar un daño.

El objetivo de la gestión de riesgos es definir, a través de medios sistemáticos, las medidas de seguridad y controles que son necesarios para eliminar o mitigar los riesgos identificados.

8.3.2. RECOLECCIÓN DE LA INFORMACIÓN

Durante el análisis de riesgos, se obtuvo la información a través de entrevistas con las personas responsables de los activos y/o de la seguridad de los activos. En los casos que se consideró necesario, se realizaron también consultas a los interesados.

8.3.3. BREVE RESUMEN DE LA METODOLOGÍA APLICADA

De forma resumida, el proceso se realizó de la siguiente manera:

1. Se identificaron todos los activos primarios de información involucrados en el tratamiento de los datos personales.
2. Se identificó y se valoró el impacto que podría suponer para los interesados la materialización de alguna amenaza.
3. Se identificaron los distintos activos que dan soporte a los activos primarios de información y se vincularon a los activos primarios de información concretos a los que prestan soporte.
4. Se identificaron las distintas amenazas a que están expuestos esos activos.
5. Se identificaron las distintas vulnerabilidades de los activos.

6. Se estimó la frecuencia con que se presenta cada una de las amenazas, así como el grado de vulnerabilidad de los distintos activos para calcular la probabilidad de que las distintas amenazas se materialicen aprovechando las vulnerabilidades identificadas.
7. Se calculó el nivel de riesgo para cada par de amenaza-vulnerabilidad en base al impacto y la probabilidad.
8. Se evaluó y decidió cuáles son los riesgos que se van a gestionar en base a los criterios establecidos en la metodología.
9. Se identificaron los controles necesarios para gestionar los riesgos.
10. Se volvió a calcular el nivel de riesgo considerando los controles seleccionados.
11. Si el nivel de riesgo no fue aceptable, se repitió de nuevo el proceso desde el punto 8.
12. Si no fue posible bajar el riesgo a un umbral aceptable, se realizó una consulta a la Agencia Española de Protección de Datos.
13. Se documentó todo el proceso, así como la conclusión del mismo.

9. MEDIDAS DE SEGURIDAD Y CONTROL

Como resultado del Análisis de Riesgos realizado, las medidas de seguridad y control que deben implantarse en la organización para mantener los riesgos en un umbral aceptable, son las que a continuación se enumeran.

8.1. COPIAS DE SEGURIDAD

8.2. FORMACIÓN DEL PERSONAL

8.3. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

8.4. BLOQUEO DEL SISTEMA DESATENDIDO

8.5. ACTUALIZACIÓN DE LOS SISTEMAS

8.6. CONFIGURACIÓN DE SEGURIDAD PROTEGIDA

La realización de una Evaluación de Impacto para la Protección de Datos Personales (EIPD)supone la determinación previa de las amenazas y vulnerabilidades, a través de un análisis de riesgos, con el objetivo de implantar una serie de medidas de seguridad que garanticen un riesgo residual aceptable para el tratamiento, de acuerdo con lo previsto en el Reglamento UE 2016/679 y la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.

En el caso de la EIPD relativa al tratamiento de datos para el acceso mediante reconocimiento facial a las instalaciones del club, se ha realizado un análisis de riesgo de todas las etapas del proceso; desde la utilización de la imagen de los socios y socias para la generación de un vector irreversible único que se almacenará en la base de datos de AWS y que estará conectada a los motores faciales del club, hasta la obtención de la imagen del socio/a que quiera acceder al club mediante lectores faciales que, a través del motor facial, asociarán ese nuevo vector creado al correspondiente vector irreversible. Analizados los riesgos, tanto para la confidencialidad como para la integridad y la disponibilidad de los datos personales de los socios/as, se han implantado una serie de medidas de seguridad, tanto técnicas como organizativas, que permiten garantizar el respeto a los derechos de las personas y que, a su vez, reducen los riesgos inherentes al tratamiento.

Por todo ello, en cumplimiento del artículo 35 del Reglamento UE 2016/679, se establece que la Evaluación de Impacto en materia de Protección de Datos (EIPD) es favorable en relación con el tratamiento de los datos personales necesarios para el acceso mediante reconocimiento facial a las instalaciones del Club, determinando que el riesgo residual existente en este tratamiento es bajo o muy bajo para los derechos de las personas.