INFORME DE EVALUACIÓN DE IMPACTO

EN LA PROTECCIÓN DE DATOS

IMF

CONTENIDO

1. RESUMEN EJECUTIVO

2. DESCRIPCIÓN DEL TRATAMIENTO

3. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

4. METODOLOGÍA DE LA EIPD

5. ANÁLISIS DEL TRATAMIENTO

6. ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

7. MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

8. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

9. CONCLUSIONES Y RECOMENDACIONES

ANEXO I: DETALLE DE PREGUNTAS GENERALISTAS DESTINADAS A LA CONFIGURACIÓN DEL PERFIL BIOMÉTRICO Y ESQUEMA DE FUNCIONALIDAD DE ADR.

ANEXO II: ACUERDO DE CONFIDENCIALIDAD FIRMADO POR LOS EMPLEADOS

ANEXO III: CONTRATO DE SERVICIO Y DE ENCARGADO DE TRATAMIENTO FIRMADO CON LA ENTIDAD ADR

ANEXO IV: CLÁUSULAS INFORMATIVAS DESTINADAS A INFORMAR A LOS ALUMNOS, ASÍ COMO A RECABAR SU CONSENTIMIENTO.

ANEXO V: INFORME ACTUALIZADO DE EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS. INSTITUTO DE CIENCIAS EMPRESARIALES.

1. RESUMEN EJECUTIVO

El tratamiento de datos que en IMF International Business School, S.L. (en adelante IMF), se desea implantar consiste en el establecimiento de un procedimiento de verificación de identidad de los alumnos combinando las técnicas de reconocimiento facial y de reconocimiento de patrón de tecleo para poder verificar así, con todas las garantías exigidas, la identidad de las personas que están cursando sus estudios.

Los datos personales objeto de tratamiento se corresponden con las categorías especiales previstas en el artículo 9 del RGPD y más concretamente con datos biométricos.

Desde IMF sé es consciente de que los sistemas de verificación elegidos para comprobar la identidad de sus alumnos, requieren un alto grado de protección, en tanto son objeto de tratamiento, datos biométricos (pertenecientes a las categorías especiales de datos a que se refiere el artículo 9 RGPD) y además se emplean nuevas tecnologías.

Asimismo, el tratamiento objeto de análisis tiene cabida en el tercer caso de los enumerados en el artículo 35.3 del RGPD, en su apartado b: "tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9".Adicionalmente, el tratamiento coincide con uno de los supuestos incluidos en el listado publicado por la Agencia Española de Protección de Datos en virtud del art. 35.4 RGPD, en los que se requiere la realización de una Evaluación de Impacto relativa a la Protección de Datos. Concretamente se refiere a "Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física"

Por eso y de cara a garantizar la privacidad de los interesados afectados por el tratamiento de datos personales, se ha decidido llevar a cabo la presente Evaluación de Impacto relativa a la Protección de Datos (en adelante EIPD), con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento, así como los orígenes del riesgo.

La EIPD ha sido desarrollada de manera conjunta por un equipo multidisciplinar con conocimientos tanto en el ámbito jurídico, como técnico, permitiendo abordar la evaluación de los riesgos desde diferentes perspectivas y permitiendo con ello establecer los riesgos a los que está expuesto el tratamiento objeto del presente informe.

En este sentido, se ha llevado a cabo un análisis de riesgos empleando para ello una metodología contrastada en el mercado, ya que combina las recomendaciones de la Agencia Española de Protección de Datos, especialmente aquéllas previstas en la *"Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD"* de la misma, así como metodologías de evaluación de riesgos como *"Normas ISO-29134 "Directrices para la evaluación de impacto sobre la privacidad"*, ISO-31000 *"Gestión del riesgo. Principios y directrices"* e ISO-31010 "*"Gestión del riesgo. Técnicas de evaluación de riesgos".*

En cuanto al contexto de la EIPD, se desea destacar que IMF está integrada por un conjunto de empresas dedicadas al desarrollo, impartición y comercialización de una amplia oferta en formación de postgrado de calidad, orientada a la mejora profesional, con una experiencia educativa diferenciada aunando, formación tecnología y compromiso con la sociedad.

Adicionalmente, para la gestión de tratamiento se va a utilizar FACEidentity que es un sistema de reconocimiento facial que se puede utilizar en diferentes situaciones en las que sea necesaria la verificación de identidad del usuario.

Son numerosos los beneficios que se obtendrán con la implantación y se desarrollarán a lo largo del informe, pero cabe mencionar los siguientes:

- Mayor garantía de éxito derivado del sistema de evaluación continua.

- Reducción de costes derivados del desplazamiento para los alumnos.

- Reducción de esfuerzos para los alumnos.

- Innovación tecnológica.

- Máxima seguridad y garantías en la realización de exámenes.

- Mayor accesibilidad a los servicios ofrecidos por la entidad.

- Mejora reputacional de la entidad.

2. DESCRIPCIÓN DEL TRATAMIENTO

A. Fecha de realización de la EIPD

HISTORIAL DE CAMBIOS				
AUTORES	VERSIÓN	FECHA	HORA	OBSERVACIONES
IMF Business School, S.L.- Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	1.0	13/02/2020	12:00h	Documentación Inicial
IMF Business School, S.L.- Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	2.0	25/02/2020	15:30h	Revisión fichero
IMF Business School, S.L.- Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	3.0	24/03/2020	10:00h	Revisión y adaptación a plantilla EIPD - AEPD
IMF Business School, S.L.- Dirección	4.0	30/03/2020	16:00h	Revisión definitiva

Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.				

B. Nombre y Descripción del Tratamiento

El tratamiento de datos personales cuyo análisis nos ocupa recibe la denominación de Reconocimiento facial y dinámica del tecleo.

En primer lugar, resulta indispensable proceder a identificar claramente el tratamiento de datos personales que se pretende efectuar y asimismo, se debe analizar a qué finalidad responde el mismo, así como los medios a través de los cuáles se llevará a cabo:

En este sentido, cabe resaltar aquí que el nuevo tratamiento de datos que en IMF se desea implantar consiste en el establecimiento de un procedimiento de verificación de identidad de los alumnos y que combina las técnicas de reconocimiento facial y de reconocimiento de patrón de tecleo para poder verificar así, con todas las garantías exigidas, la identidad de las personas que están cursando sus estudios, y que mayoritariamente serán mayores de edad.

Por un lado, el sistema de reconocimiento facial hace posible la identificación de una persona mediante las características biométricas de su rostro. Se trata de una tipología de identificación biométrica que hace uso de los rasgos fisiológicos para verificar la identidad de los usuarios. El sistema que se utiliza emplea un conjunto de datos biométricos que logran la identificación de las personas a través de la medición de puntos estratégicos en la forma y estructura únicas de sus rostros.

Por su parte, el reconocimiento por patrón de tecleo, se trata de un sistema de reconocimiento biométrico consistente en medir la fuerza con la que el usuario teclea, el tiempo de pulsación y el plazo que transcurre entre dos pulsaciones de teclado.

Las implicaciones que se derivan de esta implementación serán las siguientes:

1. Registro del perfil biométrico: la primera vez que accede el alumno a la plataforma, se le solicitará la toma de tres fotografías en distintas posturas para su registro, además de la escritura de un breve texto para la identificación de su patrón de tecleo.

2. Identificación continua en el Campus: para la obtención de un correcto patrón de teclado, al tratarse de una formación online y debido a la necesidad de completar un número determinado de trabajos en la plataforma, el sistema continuo registra el patrón de teclado.

3. Identificación intensiva en el examen online: se trata del principal objetivo de la implementación del citado sistema y consiste en garantizar de la forma más fehaciente posible que la persona que se dispone a realizar el examen online es aquella que está cursando los estudios y ninguna otra. Al proceder a su acceso al examen online, el usuario debe identificarse mediante una fotografía, y en caso de que el sistema no lo reconozca, no podrá realizar el mismo. Una vez que el usuario haya accedido con éxito al examen, se irán tomando fotografías de forma aleatoria durante la realización de este para su identificación, además de que se registrará su patrón de teclado. Esta información es contrastada por el sistema con los datos del perfil biométrico y con el patrón de teclado que se ha ido definiendo a lo largo del curso.

Se facilita a continuación el contenido del registro de actividades de tratamiento con el que se pretende dar cumplimiento a la obligación establecida en el artículo 30 RGPD:

Nombre del tratamiento	Reconocimiento facial y dinámica del tecleo
Responsables de Tratamiento	International Business School S.L.
Dirección del Responsable	C/ Bernardino Obregón 25, 28012 Madrid
Delegado de Protección de Datos	Pablo Perancho Ruíz dpd@imf.com
Descripción finalidad del tratamiento	Utilización de las técnicas de reconocimiento facial y dinámica del tecleo con el objetivo de autentificar a los alumnos en la plataforma del Campus y poder verificar así la identidad de los mismos a la hora de realización de pruebas online (exámenes).
Categoría de Interesados	Alumnos y supervisores.
Descripción tipo de datos	Datos biométricos: Datos relativos al reconocimiento facial y dinámica del teclado
Descripción Encargados de Tratamiento	ADR Infor S.L. (administración de la plataforma) DPD: Alberto Manuel García Martín datos@adrformacion.com
Cesión	No aplica
En el caso de cesiones, indique destinatario de los datos y finalidad	No aplica
Transferencias internacionales	No hay transferencias internacionales
Destinatario de los datos, país y finalidad de la TI	No aplica
Documentación de garantías adecuadas en la TI	No aplica
Origen de Datos	Del propio interesado, su representante legal.

Plazo de conservación	Plazo Supresión: Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades derivadas del tratamiento. Posteriormente, la supresión se realiza conforme a la normativa de documentación y archivos.
Cantidad de datos tratados	De 100 a 15.000 alumnos.
Accesibilidad a los datos	En un inicio únicamente tendrán acceso dos Técnicas de Formación encargadas del seguimiento del alumnado y la responsable de la Secretaría Académica, así como los administradores de la plataforma de ADR Infor S.L.
Información a los interesados	A través de cláusulas informativas conforme al artículo 13 RGPD, destinadas a recabar el consentimiento de los mismos.
Causa legitimadora del tratamiento	RGPD: 6.1.a) El interesado dio su consentimiento para el tratamiento de sus datos personales para los fines específicos.
Medidas de seguridad	Desarrolladas a lo largo del presente informe
Riesgo	**Es necesario realizar PIA**

Política de plazos de conservación/Plazos de supresión

Información personal	**Plazo de conservación**	**Justificación**
Perfil biométrico	Duración del curso académico, así como un año adicional.	Posible existencia de reclamaciones y/o gestiones que el alumnado deba realizar dentro de la plataforma
Identificación continua en el Campus	Plazo de un mes	Posible necesidad de depurar algún error existente

Identificación durante el examen	Duración del curso académico	Posibles invalidaciones de exámenes. Una vez cerradas las Actas del curso, ya no hay posibilidad de modificaciones.
Identificación a través de Key Identity	Se conservará mientras el alumno se encuentre matriculado en los estudios que cursa.	Los registros resultantes de Key Identity son ininteligibles.

C. Categorías de datos

Cabe plantearse aquí qué datos personales serán objeto de tratamiento y quiénes serán los interesados afectados por dicho tratamiento, así como las operaciones que se realizarán sobre los mismos, destacando en cualquier caso, que siempre será previo otorgamiento del consentimiento expreso por parte del interesado. La recogida de datos se realiza a través de dos herramientas implementadas dentro del campus virtual y cuyo funcionamiento se detalla a continuación:

FACEidentity es un sistema de reconocimiento facial que permite verificar la identidad del usuario. Cuando el alumno accede por primera vez al campus el sistema le solicita que realice 3 fotografías con las que se crea el perfil biométrico del usuario. Estas fotografías deben cumplir con unos requisitos para la correcta creación del perfil: una correcta iluminación, que los ojos estén abiertos o que solo aparezca una persona en la foto. Una vez que el usuario tiene creado su perfil, en los siguientes accesos se realiza una fotografía, la cual se valida contra dicho perfil. Estas fotografías también deben de cumplir los requisitos oportunos. No importa los cambios de apariencia (pelo, barba, gafas), los parámetros biométricos recogidos por FACEidentity permiten identificar correctamente al usuario. El proceso de reconocimiento consta de diferentes pruebas de vida que aseguran la presencia física del usuario frente a la cámara, como pueden ser girar la cabeza o sonreír. Si en el proceso se encuentra una foto errónea, bien sea porque no cumple los requisitos o porque ha fallado la prueba de vida, el servicio pedirá al usuario que repita la fotografía, solucionando el error generado.

KEYidentity es un servicio de reconocimiento del patrón de tecleo mediante inteligencia artificial. No se tiene en cuenta lo que el usuario escribe, sino cómo lo escribe. Para la creación

del perfil biométrico, el alumno accede a una pantalla donde se le realizan unas preguntas generalistas y debe responder escribiendo un texto. Durante el desarrollo de las actividades en las que el alumno tiene que escribir (elaboración de trabajos, participación en foros, etc) el sistema captura los ritmos del usuario, los envía al servidor de KEYidentity y comprueba, contra su perfil biométrico, la identidad del mismo. Se aporta a través del **Anexo I,** la relación de preguntas generalistas a las que se hace mención.

Para la realización de los exámenes el alumno accederá a la plataforma siguiendo el proceso descrito anteriormente. Una vez dentro, tendrá acceso a examen en las fechas y requisitos establecidos para ello. Al iniciar el examen, comienza un proceso de monitoreo que consiste en que el sistema irá tomando fotografías en un intervalo de tiempo determinado. Cada fotografía se envía al servidor de FACEidentity y se valida contra su perfil. Asimismo, todo lo que escriba en la resolución de examen se envía al servidor de KEYidentity y comprueba, contra su perfil biométrico, la identidad del mismo. Al terminar la monitorización continua, el supervisor de la plataforma podrá observar en el panel de administración los resultados de dicha sesión.

En este sentido, las categorías de interesados de los que se tratarán los datos personales necesarios para dar cumplimiento al tratamiento indicado anteriormente serán únicamente los alumnos y supervisores del Campus de IMF quiénes deberán verificar su identidad a la hora de realizar las pruebas y exámenes online que los cursos en los que están realizando sus estudios, exigen. Cabe precisar que la condición de supervisor del Campus se limita a tres personas: dos Técnicas de Formación encargadas del seguimiento del alumnado (se irá incrementando proporcinalmente al número de alumnos en una ratio de un técnico por 100 alumnos) y la responsable de la Secretaría Académica. Se aporta a través del **Anexo II,** el acuerdo de confidencialidad firmado por los empleados de la entidad.

Asimismo, procede destacar que los datos personales objeto de tratamiento se corresponden con las categorías especiales de datos personales previstos en el artículo 9 del RGPD y más concretamente con datos biométricos, en tanto se trata, tanto de los rasgos faciales de los interesados, como de su dinámica del tecleo y ambos a través de medios técnicos específicos, permiten la identificación o la autenticación unívocas de las personas físicas.

En este sentido, si se hace hincapié en que la finalidad que se pretende lograr a través del presente tratamiento requiere de todos los datos objeto de tratamiento, ya que de lo contrario no sería posible la identificación unívoca del interesado y en consecuencia, no se podría determinar sin margen de error, que el alumno que realiza el examen es efectivamente aquel

que se encuentra matriculado en el curso. Ello porque los métodos alternativos como tarjetas identificativas, contraseñas o similares podrían ser utilizados por otros individuos, dando lugar con ello a posibles suplantaciones de identidad.

D. Identificación del Responsable-RGPD

En el presente tratamiento intervienen las siguientes figuras:

El responsable de tratamiento respecto al tratamiento objeto de análisis es IMF International Business School, S.L. En este sentido cabe destacar que IMF Institución Académica se trata de un grupo de empresas propias y participadas por la empresa de IMF International Business School, S.L. donde la EIPD se desarrolla desde la empresa que ejerce el control.

Se facilita a continuación el listado de las empresas del grupo, así como los principales datos de interés sobre cada una de ellas. No obstante, se puede consultar información adicional a través del siguiente enlace: https://www.imf-formacion.com/grupo

Nombre comercial	Razón Social	Cif	Actividad	Dirección
Escola	Escuela Catalana de Formación S.L.	B63504732	Formación	Plaza Gal·la Placidia, 5 - PLT 15, 08006 Barcelona
ESESA IMF	Escuela Superior de Estudios de Empresa, S.A.	A29268111	Formación online	Av. Sor Teresa Prat Nº 15, 29003 Málaga
CESCOMPOL	Centro de Estudios Superiores de Política y Gobiernos S.L	B18830547	Formación online (másteres)	C/ Bernardino Obregón Nº 25, 28012 Madrid
IMF International Business School	IMF International Business School S.L	B83074146	Formación online (másteres y FP)	C/ Bernardino Obregón Nº 25, 28012 Madrid
Asociación Antiguos Alumnos IMF	Asociación Antiguos Alumnos IMF Business School	G87554325	Asociación antiguos alumnos	C/ Bernardino Obregón Nº 25, 28012 Madrid
PREVENLEX	Asesoría Jurídica en Prevención Prevenlex, S.L	B85041267	Formación online (másteres)	C/ Bernardino Obregón Nº 25, 28012 Madrid
CEUPE	Estudios Europeos de Postgrado y Empresa, S.L	B86256419	Formación online (másteres)	Costanilla de San Pedro Nº 2, 28005 Madrid
Instituto de Ciencias Empresariales IMF	Instituto de Ciencias Empresariales IMF, S.L.	B86344108	Formación universitaria online (grados y másteres)	Costanilla de San Pedro Nº 2, 28005 Madrid
EIPE	Esc. Int. de Profesionales y Empresas Business School S.L	B87097671	Formación online (másteres)	C/ Bernardino Obregón Nº 25, 28012 Madrid
Mejora tu carrera	Educación por un Mundo Mejor S.L	B87889150	Publidad	C/ Batalla del Salado Nº 14, 28045 Madrid
IUTA	Fundación Privada Instituto Universitario de Tecnología Aplicada IMF	G87758884	Formación universitaria online (grados y másteres)	C/ Batalla del Salado Nº 14, 28045 Madrid
Learning	Learning IMF, S.L.	B84019793	Formacion	C/ Bernardino Obregón Nº 25, 28012 Madrid

Ediciones Roble	Ediciones Roble, S.L.	B83601831	Editorial	C/ San Isidro Labrador Nº 18, 28005 Madrid
IMF Business School Colombia	IMF Business School SAS	RUT 900700448-4	Formación	C/ 26 A 13 97 OF 505 Bogotá (Colombia)
IMF Business School Portugal	IMF Portugal Instituto de Formação	NIPC 509718159	Formación	Rua Domingos Sequeira, 27, 5ºAndar Esc. D, 1350-119 Lisboa, Portugal
Open Uide UideOpen CIA. LTDA	Open Uide UideOpen CIA. LTDA	RUC: 1792885914001	Formación universitaria online	C/ Javier Arauz 111 y Germán Alemán, Quito (Ecuador)

E. Contexto interno del tratamiento en la organización

A pesar de que el responsable de tratamiento respecto a la EIPD objeto del presente informe es IMF International Business School, S.L., se realizar una breve reseña sobre el contexto interno de IMF INSTITUCIÓN ACADÉMICA, en adelante IMF. IMF está integrada por un conjunto de empresas dedicadas al desarrollo, impartición y comercialización de una amplia oferta en formación de postgrado de calidad, orientada a la empleabilidad y con una excelente relación calidad-precio.

- IMF Business School, que forma parte de los principales rankings mundiales y es miembro de prestigiosas asociaciones como The Association to Advance Collegiate Schools of Business (AACSB) o Association of MBAs, además de colaborar con empresas de reconocido prestigio como Deloitte, EY o Indra

Dispone de programas en las áreas más demandadas del mercado: Ciencias Técnicas e Ingeniería, Ciencias de la Salud y la Educación, Ciencias Económicas y Empresariales, Ciencias Jurídicas y Ciencias Sociales y Humanidades. Para ello, cuentan con un equipo de expertos integrado por doctores universitarios y profesionales en activo, especializados en cada área para dar asistencia tutorial y pedagógica a los alumnos, garantizando que en todo momento obtengan una atención personalizada y completa.

Cuenta entre sus recursos con una innovadora plataforma educativa, con más de 900 cursos propios disponibles y diversas herramientas tecnológicas diseñadas para facilitar el estudio desde cualquier dispositivo y lugar del mundo; con una plataforma de empleo y prácticas, con constante actualización de ofertas y candidatos, de la que tanto nuestros clientes particulares, como las empresas pueden beneficiarse, utilizándola como lugar de encuentro en el mercado laboral; y una biblioteca virtual con más de 30.000 referencias bibliográficas.

En el área de consultoría a empresas hemos desarrollado trabajos para organizaciones como Acciona, Navantia, Adecco, Cintra, Iberdrola, John Deere, Johnson and Johnson, Telefónica, etc.

Se cuenta con una línea de RSC que contempla un Plan Internacional de Becas que concede y gestiona, al año, más de 6 millones de euros para facilitar el acceso a la formación oficial y profesional a quien pueda estar interesado en desarrollarse profesionalmente sin barreras económicas; así como de una financiación del 100% sin intereses.

Misión IMF

Es nuestra misión y compromiso elaborar una formación accesible y de calidad orientada a la mejora profesional, con una experiencia educativa diferenciada aunando, formación tecnología y compromiso con la sociedad.

Por medio de:

- Formación on line: Con metodología centrada en el estudiante. En ella, la tecnología y acción tutorial se unen para facilitar y ayudar a construir el aprendizaje. Se adapta a la vida, circunstancias y horarios del alumno por medio del campus virtual disponible 24 horas, contacto con tutor, clases online en directo impartidas en streaming. Con más de 30.000 referencias en la biblioteca virtual, masterclass y eventos gratuitos.

- Formación presencial El profesor basándose en una fundamentación teórica, dirige la formación al desarrollo de competencias de forma práctica. Los docentes son profesionales en activo. Su amplia experiencia que enriquece la impartición en cada curso. Cuenta con Masterclass, eventos, mesas redondas, prácticas profesionales en empresa, en horarios flexibles.

- Formación semipresencial Esta modalidad suma a las ventajas de la metodología online (flexibilidad, acceso 24/7 al campus virtual...), la oportunidad de asistir a sesiones presenciales beneficiándote del networking con profesionales del sector y en horarios compatibles.

Hitos clave históricos y logros alcanzados

Desde su fundación, el Grupo IMF ha experimentado un gran crecimiento y diversificación de sus líneas de negocio. El éxito de este crecimiento se basa en la calidad de nuestra formación y en la experiencia de nuestro equipo de especialistas, que han convertido al grupo en un referente:

HITOS IMF

2001- Nace IMF con los masters de Prevención de Riesgos Laborales y RRHH.

2004- Línea de Consultoría a Empresas.

2005- Comienzo de la implantación de un SGC ISO 9001.

2007- Convenios de Formación. Plataforma virtual con la empresa.

2009- Marco de colaboración San Pablo CEU: Ofrecer servicios de masters oficiales

2010- IMF inicia el desarrollo de un proyecto formativo asociado al Catálogo Nacional de las Cualificaciones, niveles 1, 2 y 3

2011- Comienzo de expansión internacional: Lisboa y México DF. Consecución del Sello Madrid Excelente

2012- Acuerdo con CEU Cardenal Herrera. Se realiza la primera Autoevaluación según Modelo EFQM. Se inicia con la presentación de convocatorias estatales, tanto de menores de 30 años como la de Ocupados.

2013- Nace el proyecto COI. Centro de educación superior del sistema universitario español adaptado al Espacio Europeo de Educación Superior (EEES), adscrito a la universidad Camilo José Cela. Participación de IMF con el 85% de participación. IMF alcanza 38 certificados de profesionalidad acreditados (Madrid Sevilla y Valencia). Se abre el primer centro acreditado para impartición de certificados de profesionalidad

2104- Formar parte de AEEN. Se acredita Bilbao para CdP IMF cuenta con 68 certificados acreditados, y forma parte de AACSB INTERNATIONAL: certificar la calidad académica de las facultades Lanzamiento de CELA OPEN INSTITUTE con 5 programas:

2015 Sello de Emprendimiento y Empleo Joven - http://www.imf-formacion.com/noticias/imf-consigue-el-sello-de-emprendimiento-y-empleo-joven

Escuela de negocios más reconocida por Mundo Posgrado - http://www.imf-formacion.com/noticias/imf-es-la-escuela-de-negocios-con-mayor-reconocimiento-por-los-usuarios-de-mundo-posgrado

Autorización como Agencia de Colocación - http://www.imf-formacion.com/noticias/grupo-imf-autorizado-como-agencia-de-colocacion

Socio corporativo de MKT - http://www.imf-formacion.com/noticias/imf-nuevo-socio-corporativo-de-mkt

Sello Cum Laude por Emagister - http://www.imf-formacion.com/noticias/imf-reconocido-con-el-sello-cum-laude-por-emagister

Socio de ATI - http://www.imf-formacion.com/noticias/imf-se-convierte-en-socio-de-ati

Sello EFQM 400+ - http://www.imf-formacion.com/noticias/imf-recibe-el-sello-efqm-400

Acuerdo con Moda España - http://www.imf-formacion.com/noticias/imf-firma-un-acuerdo-con-modaespana

2016 Business School entrega sus Premios IMF 2015 - http://www.imf-formacion.com/noticias/entrega-premios-imf-2015

Firma un acuerdo con SEGITTUR - http://www.imf-formacion.com/noticias/acuerdo-imf-segittur

IMF lanza la línea Executive Education en sus campus de Madrid, Bilbao, Valencia y Sevilla - http://www.imf-formacion.com/noticias/nueva-linea-executive-education

MBA de IMF repite los primeros puestos del Ranking de PortalMBA - http://www.imf-formacion.com/noticias/imf-ranking-portalmba-2016

IMF y SENATI firman un convenio para ofrecer cursos semipreseciales en Perú - http://www.imf-formacion.com/noticias/imf-senati-semipresenciales-peru

IMF crea una Aceleradora de Empresas - http://www.imf-formacion.com/noticias/imf-emprende-aceleradora-empresas

IMF inaugura su nuevo campus en Madrid - http://www.imf-formacion.com/noticias/nuevo-campus-imf-madrid

IMF en el TOP 20 del ranking de formación online en español - http://www.imf-formacion.com/noticias/imf-ranking-formacion-online-espanol-2016

Retos y Estrategia

- Visión:

La visión de IMF consiste en posicionarnos nacional e internacionalmente y ser reconocidos en la comunidad educativa a través del prestigio, accesibilidad, notoriedad y calidad educativa, contribuyendo a maximizar el valor para nuestros alumnos y colaboradores académicos, accionistas y empleados

Dicha Visión se desarrolla en cinco líneas de actuación:

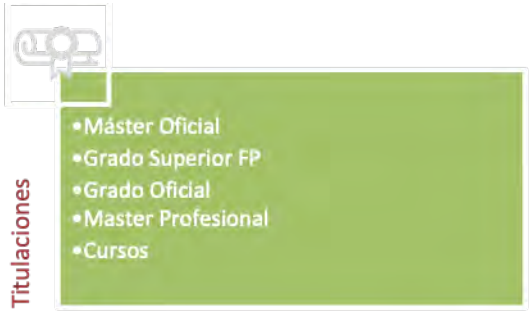
- Prestigio basado en la profesionalización constante y el uso de metodologías innovadoras con estándares tecnológicos definidos.
- Accesibilidad entendida desde criterios de sostenibilidad económica, social y el compromiso con las personas que trabajan en IMF contribuyendo a su bienestar y desarrollo profesional.

- Notoriedad por medio del desarrollo de alianzas con instituciones educativas de referencia tanto a nivel nacional como internacional y de la potenciación de la imagen de marca.
- Calidad Educativa que contemple la potenciación de la formación presencial, la calidad del plantel de profesorado y del catálogo formativo.

Mercados, servicios ofrecidos, clientes

Mercados y servicio

- Los servicios de formación ofrecidos por IMF son:



Clientes

Los clientes a los que va destinada esta formación:

- Particulares: (estudiantes, trabajadores o desempleados): con descuentos, promociones y financiación sin ningún tipo de interés o incluso a coste cero, si es a través de Convenios de Formación Continua. Esta línea supone el 80% del total de la facturación.

- Empresas: ofreciendo un asesoramiento, tanto técnico, como académico. Ejemplo de ello es la gestión de bonificaciones para la formación. Todo este servicio de formación y consultoría se soporta sobre una amplia estructura de Colaboradores y Expertos, un Fondo Editorial propio extenso y heterogéneo, unas metodologías de impartición adaptadas al tipo de perfil del alumno y una Bolsa de Trabajo que ofrece a las empresas profesionales capacitados por IMF.

- Sector público e institucional: Convenios de formación: convocatorias nacionales y regionales, Ayuntamientos, Federaciones, etc… (en forma de proyectos especiales)

Estructura de gestión y actividades directivas

IMF cuenta con una estructura de liderazgo definida y que consta de distintos niveles de liderazgo:

1-LIDERAZGO

NIVELES DE LIDERAZGO

Como se ha identificado en la información clave existen cinco niveles de liderazgo definidos en IMF de los cuales destacamos los tres primeros:

NIVEL 1:

Ocupado por Carlos Martínez (Presidencia) y Belén Arcones (Dirección General). Carlos se ocupa además de las Relaciones institucionales y comerciales; abriendo oportunidades de negocio y gestionando todo tipo de alianzas. Por otro lado, Belén además lidera la gestión de la parte académica, operativa y estratégica. Desde los comienzos, ambos han liderado el crecimiento siendo fieles a unos valores fuertemente arraigados en la cultura organizacional:

NIVEL 2

Ocupado por Ignacio Castillo Cebrián es el director ejecutivo de IMF, se asegura del despliegue estratégico en la organización, control y seguimiento de la ejecución de las actividades de IMF así como la propuesta de asignación de recursos. Es el responsable de Recursos Humanos del grupo.

NIVEL 3

Compuesto por todos los directores de IMF. Se puede consultar el organigrama en el siguiente enlace: https://www.imf-formacion.com/nuestro-equipo

COMITÉ DE DIRECCIÓN

Durante los dos últimos años se ha fortalecido la estructura de comité de dirección, formado por los tres primeros niveles de liderazgo,

Existe una sistemática de reuniones semanales donde se abordan los aspectos relacionados con la dirección, mejora y rendimiento de IMF.

Los miembros del comité de dirección son los responsables de imbuir el espíritu de equipo, propugnar las buenas prácticas y alimentar la disciplina del seguimiento de resultados, la gestión de la innovación y la mejora e de los procesos, actividades, herramientas y buenas prácticas.

CONCEPTO AMPLIO DE LIDERAZGO

Haciendo una lectura más allá de la nomenclatura de los cargos, la acción del liderazgo se hace extensiva a personas que no tienen cargos directivos, pero que asumen la coordinación de equipos de mejora, aportan a la identificación e implantación de las mejores prácticas y se implican e implican a otros en la consecución de las metas y objetivos, siendo un referente profesional para los empleados.

CERCANÍA Y MEJORA

Desde el punto de vista de la comunicación, en IMF se cuenta con una cultura de accesibilidad a los líderes para cualquier miembro del personal. Este hecho se ha mantenido a pesar del vertiginoso crecimiento acontecido durante poco más de diez años. Actualmente se mantiene una cultura de accesibilidad y cercanía entre los líderes y el resto del personal.

En el Espacio de Atención Tutorial (EAT) de IMF International Business School, S.L situado en la calle Bernardino Obregón 25, de Madrid, el Centro dispone de aulas completamente equipadas que son utilizadas en diversas actividades formativas (conferencias, clases teóricas y prácticas, seminarios, talleres, foros de debate, etc..), que luego son registradas y puestas a disposición del alumnado del programa correspondiente.

Dicho espacio cuenta con los preceptivos servicios y está plenamente adaptado a las normas de accesibilidad, seguridad y prevención de riesgos.

El Centro ofrece los recursos para el aprendizaje y la investigación a través de la biblioteca virtual ODILO, una plataforma digital puntera de aprendizaje colaborativo, que permite poner a disposición del alumnado y el profesorado una gran biblioteca digital de contenido empresarial con miles de libros, revistas, artículos, informes y vídeos, así como herramientas para que saquen el máximo provecho a los contenidos e interactúen con otros universitarios en un espacio de formación abierto.

Por último, para la gestión de tratamiento se va a utilizar FACEidentity que es un sistema de reconocimiento facial que se puede utilizar en diferentes situaciones en las que sea necesaria la verificación de identidad del usuario, como por ejemplo acceso a área privada, exámenes online o webinars.

Se utiliza para identificar a los usuarios, por ejemplo, en los accesos al campus. En esta integración, se toma una fotografía y se valida contra el perfil del usuario, permitiéndole acceder si el resultado es correcto. También se utiliza para monitorización continua, por ejemplo, para

validar la autoría de un examen online ya que el sistema irá tomando fotos del usuario cada cierto periodo de tiempo y las validará contra su perfil.

En caso de que se desee conocer información adicional sobre IMF International Business School, S.L, se puede consultar a través del siguiente enlace: https://www.imf-formacion.com/. En último lugar, cabe mencionar aquí las posibles relaciones del tratamiento cuyo análisis nos ocupa con otros tratamientos de datos de la propia organización y en concreto con los siguientes tratamientos personales identificados en el registro de actividades:

El tratamiento denominado "Alumnos" tiene como finalidad la grabación de matrículas, impartición, seguimiento y evaluación de los cursos de los alumnos que participan en ellos y se ha identificado como interesados a los alumnos de la entidad.

Asimismo, se encuentra relación con el tratamiento denominado "Gestión financiera", cuya finalidad es llevar a cabo correctamente toda la gestión de los clientes y alumnos de la entidad desde el punto de vista comercial, contable, fiscal y administrativa. Se identifica como interesados, entre otros, a los alumnos de la entidad.

F. Contexto externo de la organización y el tratamiento.

El objetivo principal de IMF es dar un servicio de calidad a los alumnos que demandan formación superior, focalizando de forma ágil sus problemas y prestando una atención y servicio excelentes, así como la búsqueda constante de ocasiones para mejorar los productos y servicios y crear nuevas oportunidades de formación

La organización cree que la experiencia del alumnado y las relaciones éticas van de la mano, prestando la máxima importancia a la seguridad y protección de los datos.

La estrategia de IMF está orientada a garantizar las necesidades y expectativas de los alumnos adoptando para ello un enfoque diferenciador, dinámico, eficiente y responsable. En este sentido se pretende:

- Mejorar la relación con los alumnos, simplificando la interacción mediante herramientas colaborativas que permiten ir adquiriendo un mejor conocimiento de los alumnos.
- Diversificar mediante la optimización de nuestros activos explorando nuevas oportunidades de mejora, con el fin de anticipar las necesidades esenciales de nuestros alumnos y, simultáneamente, seguir trabajando en nuestro anhelo de mejora continua.

Grupo IMF lo constituyen centros de formación universitaria sólidos y estables, que ha podido ampliar sus servicios de una forma continuada y sostenida aún en tiempos de crisis económica, debido a su interés por la mejora e innovación y su afán de servicio a la comunidad.

Asimismo, no se quiere dejar de hacer mención a la actual coyuntura por la situación que se está viviendo, tanto a nivel nacional, como internacional a raíz del COVID-19 y que está afectando a todos los parámetros políticos, sociales, empresariales y económicos.

En este contexto, IMF se encuentra analizando exhaustivamente la situación con el propósito de, no solo tomar las decisiones más óptimas para la seguridad de los empleados, sino también para poder continuar ofreciendo sus servicios con las mayores garantías.

En este sentido, las tendencias actuales a nivel mundial se dirigen a la necesidad inminente de transformar tecnológicamente el sector de la educación. Dicha transformación debe concretarse en la posibilidad de ofrecer un servicio de educación en la modalidad online caracterizada principalmente por la realización del trabajo fuera de las aulas y oficinas, pero manteniendo el mismo nivel de garantías en lo que a derechos y deberes de alumnos y profesores se refiere.

Desde IMF se tiene el fiel convencimiento del papel crucial que juega la tecnología actualmente, toda vez que resultará ser la herramienta fundamental que nos permitirá asumir con éxito el gran reto que se presenta por delante, dado que la competitividad y el rendimiento de la entidad, así como la satisfacción de nuestros clientes no deben verse mermados por la actual coyuntura que acontece.

3. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

Tal y como establece el RGPD, el tratamiento de datos personales debe ser lícito y, por tanto, se ha de asegurar que se cuenta con una causa legítima correctamente aplicada para el mismo, de modo que los datos personales se traten de acuerdo con las condiciones recogidas en el RGPD.

En este sentido, el artículo 6 del RGPD, recoge los supuestos en los que se considera que el tratamiento de datos personales es lícito y entre los mismos, se encuentra el consentimiento.

Siguiendo el literal del art 9 RGPD que versa sobre las categorías especiales de datos personales, entre los que se encuentran los datos biométricos, se puede observar que se establece, como regla general, la prohibición del tratamiento de datos biométricos con la finalidad de identificar de manera unívoca a una persona física.

No obstante, el RGDP en el apartado 2. a) del artículo 9 continúa indicando que “lo dispuesto anteriormente no será de aplicación cuando concurran una serie de circunstancias”. Entre las

circunstancias previstas y que podrían constituir una excepción a la prohibición, se prevé expresamente la identificación del consentimiento como base legitimadora del tratamiento de datos biométricos.

Se podría invocar el consentimiento como causa legitimadora del tratamiento que se quiere llevar a cabo, pero es conveniente asegurar que se dan todas las condiciones para que el consentimiento sea válido, y por tanto libre, específico, informado e inequívoco.

En esta línea, el artículo 7 RGPD establece las siguientes condiciones:

"1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales"

> Para dar cumplimiento a este primer punto, el responsable de tratamiento IMF, en cumplimiento del principio de responsabilidad proactiva, ha procedido a elaborar las cláusulas destinadas a recabar el consentimiento explícito e informado de los interesados en un formato que permita a posteriori poder demostrar el cumplimiento de esta obligación en caso de ser necesario y ello antes del inicio del tratamiento. Para ello, se habilitarán casillas destinadas a ser marcadas por aquellos interesados que decidan otorgar su consentimiento de forma libre, explícita e informada.

"2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento"

> En función de lo dispuesto en el segundo de los requisitos, es condición indispensable para que el consentimiento sea válido, que la solicitud se presente de forma separada respecto del resto de información en su caso y que el usuario pueda acceder y entender esta información de forma clara y fácil. En este sentido, se garantiza que la cláusula destinada a recabar dicho consentimiento se presentará de forma separada respecto al resto de información que se proporcione al interesado.

"3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo"

Con el objetivo de dar cumplimiento a este punto, IMF, en el caso de que los alumnos no deseen prestar su consentimiento al tratamiento en cuestión o lo retiren posteriormente, fijará anualmente dos fechas que permitirán la realización de los exámenes de forma presencial como alternativa y con las mismas garantías, a celebrar en Madrid, España.

"4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato"

En este sentido, se puede afirmar sin lugar a duda que el interesado puede hacer una elección real y no existe ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta ello porque, en caso de que el interesado no desee prestar su consentimiento al tratamiento indicado, podrá realizar el examen de forma presencial y con los mismos derechos y deberes que asisten a aquellos alumnos que se decantan por la opción online. Se garantiza que la prestación del servicio no depende de modo alguno del consentimiento en cuestión. Asimismo, también se da cumplimiento al art. 6 de la LOPDGDD.

4. METODOLOGÍA DE LA EIPD

A. Implicados en la ejecución de la EIPD

La EIPD ha sido desarrollada de manera conjunta por un equipo multidisciplinar con conocimientos en el ámbito jurídico y técnico, permitiendo abordar la evaluación de los

riesgos desde diferentes ámbitos, permitiendo con ello establecer los riesgos a los que está expuesto el tratamiento objeto del presente informe.

Los recursos que han participado son los siguientes:

- DPD: el Delegado de Protección de Datos tiene atribuidas las siguientes funciones:
    - Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
    - Supervisar el cumplimiento de la normativa.
    - Asesorar respecto de la evaluación de impacto relativa a la protección de datos.
    - Cooperar con la autoridad de control.
    - Actuar como punto de contacto para cuestiones relativas al tratamiento.
    - Difundir y comunicar las prácticas de protección de datos personales implementadas a los usuarios del interior de la organización, formando y concienciando a todo el personal sobre las mismas.
    - Efectuar el análisis de riesgos de cada tratamiento y aplicar las medidas de seguridad necesarias, y en su caso, aplicación de las oportunas políticas de protección de datos.
    - Supervisar las auditorías correspondientes.
- Responsable del Tratamiento: el responsable de tratamiento, con un perfil jurídico tiene que velar por:
    - Asegurar que las prácticas de protección de datos personales en la compañía cumplan con la Ley y otras normas aplicables.
    - Difundir y comunicar las prácticas de protección de datos personales implementadas a los usuarios del interior de la organización, formando y concienciando a todo el personal sobre las mismas.
    - Asegurar el cumplimiento de los principios de protección de datos.
    - Cumplir con la obtención del consentimiento inequívoco.
    - Garantizar los derechos del tratamiento de los menores de edad.
    - Cumplir con el nuevo deber de información de forma integral.

- Establecer y gestionar procedimientos para la recepción, tramitación, seguimiento y atención de las solicitudes para el ejercicio de los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.
- Establecer y gestionar procedimientos para la recepción, tramitación, seguimiento y atención de los nuevos derechos de los afectados.
- Llevanza del registro de actividades del tratamiento.
- Regularizar las relaciones con los encargados de tratamiento conforme al RGPD.
- Efectuar las evaluaciones de impacto de los tratamientos de datos personales.
- Elegir únicamente encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD.
- Consultar y facilitar la información necesaria, a la autoridad de control sobre los tratamientos que entrañarían un alto riesgo, como resultado de la evaluación, si el responsable no toma medidas para mitigarlo.

- Encargado de tratamiento (**Anexo III**):
  - Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional;
  - Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
  - Aplicar todas las medidas y controles de seguridad necesarias;
  - Asistir al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para

que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;

- Ayudar al responsable a garantizar el cumplimiento de las obligaciones;
- A elección del responsable, suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales.
- Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

El tratamiento implica el uso de tecnologías novedosas a la hora de evaluar al alumnado de manera remota a través de FACEidentity, el cual identifica a un usuario mediante las características faciales extraídas de una imagen captada por su webcam. FACEidentity se basa en uno de los más avanzados sistemas de Inteligencia Artificial para reconocimiento facial que existen en la actualidad, AWS Rekognition.

De un modo sencillo se registra el perfil biométrico del usuario mediante 3 fotografías. Una vez creado el perfil, durante el proceso de identificación el servicio solicita diferentes acciones que aseguran la presencia física del usuario frente a la cámara.

Con FACEidentity se puede s asegurar que la persona que está delante del dispositivo es quien dice ser sin importar sus posibles cambios de apariencia.

Para la gestión de dicha tecnología se cuenta con el DPD de IMF que a su vez es el Responsable de Seguridad, que cuenta con un perfil tecnológico capaz de controlar y gestionar con el proveedor de servicios cualquier evento funcional de la plataforma, así como el impacto a la privacidad de los interesados y que asimismo, se encuentra respaldado por un departamento de protección de datos bajo su coordinación, contando con el asesoramiento de una consultora integral para el asesoramiento en materia de protección de datos y un abogado en ejercicio experto en protección de datos.

B. Guías, herramientas, metodologías, normas y dictámenes utilizados en la evaluación

El tratamiento de Reconocimiento Facial y dinámica de tecleo implica la gestión de datos biométricos mediante una tecnología de evaluación novedosa en el mercado.

Debido a ello se ha llevado a cabo un análisis de riesgos contrastada en el mercado ya que combina las recomendaciones de la Agencia de Protección de Datos y metodologías de evaluación de riesgos propuesta por la norma ISO 31000.

La metodología de Análisis de Riesgos se he realizado de manera analítica con los responsables del tratamiento en el cual se han tenido en cuenta las siguientes dimensiones:

- Finalidad del tratamiento: donde se tiene en cuenta el tipo de finalidad a la que están destinados los tratamientos, en especial aquellos que pueda suponer riesgos para los derechos o libertades de los interesados, categorías especiales de datos o datos relativos a condenas o delitos penales.
- Cantidad de datos tratados: se evalúa la cantidad de datos de los interesados que se gestionan, ya que a mayor volumen de tratamientos mayor es el riesgo para los interesados.
- Plazo de conservación: se define un plazo de conservación de los datos que se debe limitar únicamente a lo estrictamente necesario y cuanto mayor sea el periodo de almacenamiento, mayor será el riesgo de producirse alguna vulneración de los derechos.
- Accesibilidad: se valora el número de personas que tienen acceso al tratamiento, ya sean empleados o encargados del tratamiento.
- Tipos de datos tratados: se diferencian los tipos de datos tratados, teniendo en cuenta la existencia de datos especialmente protegidos o aquellos que puedan darnos datos de personalidad, comportamientos, etc.
- Transferencias internacionales: se evalúa la existencia o no de transferencias internacionales teniendo en cuenta el hecho objetivo, no si existen medidas para que se realicen de forma legal.

Derivado de dicho análisis se establece la necesidad de realizar una evaluación de impacto del tratamiento objeto del presente informe. Para ello se ha analizado en profundidad las

implicaciones de dicho tratamiento para el responsable de tratamiento. En este sentido partiendo del Tratamiento se han definido los recursos necesarios para gestionarlo.

Es por ello que se han identificado aquello recursos hardware, software, instalaciones, encargados de tratamiento necesarios, estableciendo para cada uno de ellos un listado de riesgos que pueden afectar a los interesados. Estos riesgos han sido evaluados mediante los siguientes criterios:

- Probabilidad: probabilidad de que un riesgo se materialice en función de la experiencia existente en situaciones similares y de los controles preventivos existentes.
- Impacto: determina el daño o la degradación que produciría en los procesos de la organización la materialización de la amenaza.

La metodología empleada en el análisis de riesgos debe perseguir un objetivo claro: obtener un valor que nos indique el riesgo asociado a los tratamientos y los activos que lo soportan y que nos permita tomar decisiones priorizadas. Estas decisiones tienen que tomarse por comparación con un umbral de riesgo definido.

El cálculo del riesgo de una amenaza se realiza mediante la siguiente tabla teniendo en cuenta la probabilidad y el impacto obtenidos:

PROBABILIDAD					
Muy Alta	Medio	Medio	Alto	Muy alto	Muy alto
Alta	Medio	Medio	Alto	Alto	Muy alto
Media	Bajo	Bajo	Medio	Alto	Alto
Baja	Muy Bajo	Bajo	Bajo	Medio	Medio
Muy Baja	Muy bajo	Muy bajo	Bajo	Bajo	Medio
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
	IMPACTO				

Una vez realizado el análisis de riesgos, la Dirección debe aprobar los resultados obtenidos.

Para aquellos tratamientos que no se asuman sus riesgos asociados, se establece un plan de tratamiento que incluye la definición de medidas de seguridad a implementar, plazos, responsables y descripción de las actividades a realizar.

Una vez ejecutado el plan de tratamiento se debe reevaluar la situación para verificar que se han mitigado las amenazas tratadas e identificar el riesgo residual existente que debe ser aprobado por Dirección.

5. ANÁLISIS DEL TRATAMIENTO

Se indica a continuación el ciclo de vida relacionado con el tratamiento objeto de análisis

CAPTURA DE LOS DATOS

Actividades
La recogida de datos se realiza a través de dos herramientas integradas dentro del campus virtual y cuyo funcionamiento se detalla a continuación: FACEidentity es un sistema de reconocimiento facial que permite verificar la identidad del usuario y monitorizarlo cuando realiza los exámenes. <u>Creación del perfil biométrico en FaceIdentity.</u> Cuando el alumno accede por primera vez al campus el sistema le solicita que realice 3 fotografías con las que se crea el perfil biométrico del usuario. Estas fotografías deben cumplir con unos requisitos para la correcta creación del perfil: una correcta iluminación, que los ojos estén abiertos o que solo aparezca una persona en la foto. Una vez que el usuario tiene creado su perfil, en los siguientes accesos se realiza una fotografía, la cual se valida contra dicho perfil. <u>Identificación con FaceIdentity.</u> El proceso de identificación se usa para validar la identidad del usuario cada vez que hace login en el campus. Es usado por tanto como doble factor de autenticación.

El proceso de reconocimiento consta de diferentes pruebas de vida que aseguran la presencia física del usuario frente a la cámara, como pueden ser girar la cabeza o sonreír. Si en el proceso se encuentra una foto errónea, bien sea porque no cumple los requisitos o porque ha fallado la prueba de vida, el servicio pedirá al usuario que repita la fotografía corrigiendo el error generado. En este proceso el Faceidentity captura una fotografía de la webcam del usuario que se registra. Esta fotografía se envía a AWS Rekognition, es analizada y comparada con el perfil biométrico ya creado y devuelve un porcentaje de similitud con el modelo. En función de este resultado FaceIdentity devuelve al campus si la identificación ha sido positiva, negativa o incertiumbre.

Monitorización con FaceIdentity.

Este proceso solamente se realiza durante la realización del examen.

FaceIdentity muestra la imagen de la webcam del usuario a través de un iframe que va capturando fotografías del alumno cada cierto tiempo mientras este realiza el examen. Estas fotografías capturadas son enviadas al servicio FaceIdentity que las almacena y a su vez procesa con AWS Rekognition. En este procesado se verifica la identidad del usuario para cada una de las imágenes, así como otros detalles adicionales: que solamente aparece una persona en la pantalla, la dirección en la que mira, que el rostro se muestre completo.

Los datos capturados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

KEYidentity es un servicio de reconocimiento del patrón de tecleo mediante inteligencia artificial. No se tiene en cuenta lo que el usuario escribe, sino cómo lo escribe.

Creación del perfil biométrico.

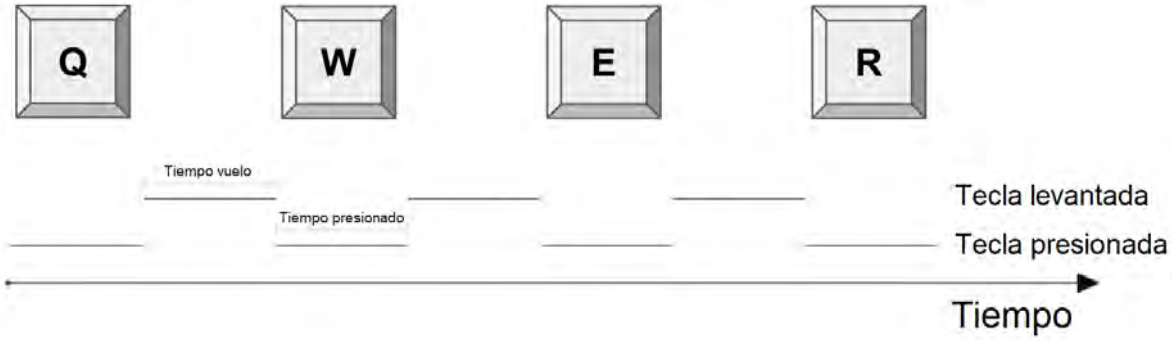
Para la creación del perfil biométrico, el alumno accede a una pantalla donde se le realizan unas preguntas generales a las que tiene que responder escribiendo un texto. A partir de estas muestras en las que se registra una matriz de datos con los tiempos de pulsación y vuelo de cada tecla el sistema genera un modelo biométrico de los ritmos de escritura del usuario.

Monitorización de la identidad con keyidentity.

Durante el desarrollo de las actividades en las que el alumno tiene que escribir (elaboración de trabajos, participación en foros, etc) el sistema captura los ritmos del usuario, los envía al servicio

de KEYidentity y comprueba contra su perfil biométrico la identidad del mismo. El resultado de las identificaciones es almacenado en la base de datos del servicio.

KEYidentity usa tecnología JavaScript para la captura de tiempos de vuelo y pulsación de cada tecla. El servicio Keyidentity almacena estas matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario



Datos Tratados

<u>FaceIdentity</u>

Los datos capturados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

Para el servicio FACEidentity, se utilizan las tablas USUARIOS y LOGS. En la tabla USUARIOS se guardan:

- El id biométrico
- El id externo del usuario
- El id del cliente
- El número de fotos que ha utilizado el usuario para entrenarse (0 no está entrenado, 3 si está entrenado)
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)

Si el usuario está verificado (el cliente ha validado el perfil biométrico desde la consola de supervisor)

En la tabla LOGS, se almacenan los siguientes datos:

El id de la identificación
El id biométrico del usuario
La fecha en la que se ha realizado la comprobación
El porcentaje de similitud con cada una de las fotos del entrenamiento
El resultado obtenido (positivo, negativo o incertidumbre)
La prueba de vida a la que se ha sometido el usuario (gesto en la fotografía)
Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
El id enlazado, id de la anterior comprobación si sigue en la misma sesión
Si la foto está almacenada o no.
El user agent.
El posicionamiento de la cara respecto a la cámara, para saber si el usuario está mirando a la pantalla o no.
El tipo de registro (identificación o monitorización)

Keyidentity

Para el servicio keyidentity los datos que se capturan son las matrices de tiempos de cada usuario, el useragent, ip del usuario.

Para el servicio KEYidentity, se utilizan las tablas KEYSTROKE_USUARIOS_TEXTO y KEYSTROKE_LOGS_TEXTO.

En la tabla KEYSTROKE_USUARIOS_TEXTO se guardan:

El id biométrico
El id del cliente
El id externo del usuario
Si el usuario está entrenado o no
El número de registros que lleva el usuario
El porcentaje actual de identificaciones correctas y el porcentaje de intentos ilícitos detectados en una prueba interna que se realiza para comprobar su robustez.

Si el usuario se ha marcado como sospechoso y un comentario de porque se ha marcado así.

El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)

Si el usuario tiene que contar para la facturación.

En la tabla KEYSTROKE_LOGS_TEXTO, se almacenan los siguientes datos:

El id de la identificación

El id biométrico del usuario

Los datos de los tiempos de tecleo de la identificación

El tipo de registro (entrenamiento o identificación)

El porcentaje de similitud con el modelo entrenado

La fecha en la que se ha realizado la comprobación

Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros

La IP, el navegador, el SO y la ciudad (basada en su IP) del usuario para saber de dónde vienen los datos

El número de caracteres que tiene el registro

Si la pantalla es táctil o no.

El user agent.

Las categorías de datos personales objeto de tratamiento son las siguientes:

- Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica de tecleo.

Origen de los Datos

Los datos personales únicamente son proporcionados por el propio interesado una vez que ha sido informado de todos los aspectos relativos al tratamiento de datos personales.

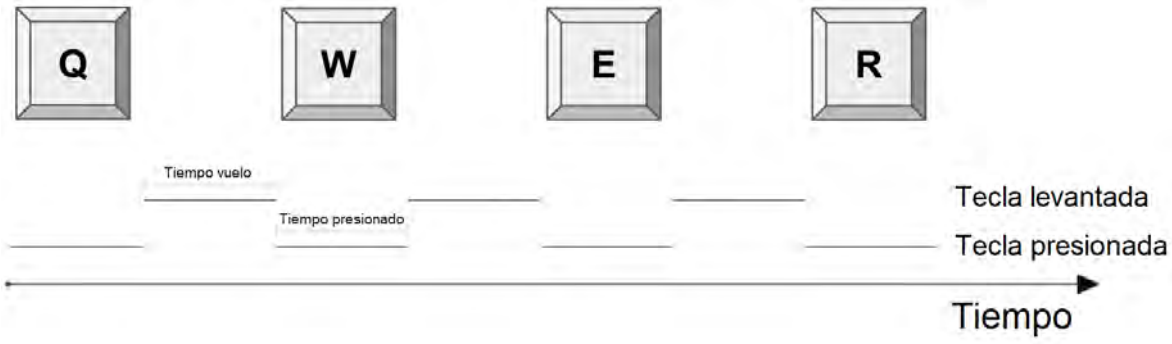
Tecnologías Intervinientes

FACEidentity y KEYidentity son desarrollos propios de nuestro partner tecnológico ADR Infor, S.L. alojados en la nube AWS. Los datos están alojados en Irlanda con centro de respaldo en París.

Para la captura de las fotografías se utiliza un iframe que envía los datos al servicio FaceIdentity.

Para la captura de los ritmos de tecleo se utiliza una función Javascript que captura los ritmos de tecleo en los editores de texto donde el alumno responde a las preguntas escribiendo con el teclado. Una vez se ha llenado el buffer de datos con la captura de tiempos esta es enviada al servicio KeyIdentity para su registro e identificación.

KEYidentity usa tecnología JavaScript para la captura de tiempos de vuelo y pulsación de cada tecla.



CLASIFICACIÓN Y ALMACENAMIENTO

Actividades

FaceIndetity

El servicio FaceIdentity almacena fotografías capturadas asociadas a un Id de usuario. Los datos biométricos no son gestionados por el servicio sino que son generados a partir de la fotografía por el api de AWS Rekognition. El api AWS Rekognition es la que genera el modelo biométrico, lo almacena en una colección interna y lo compara con el del usuario devolviendo a Faceidentity el porcentaje de similitud entre modelos. FaceIdentity por tanto no gestiona ni almacena estos datos biométricos.

Keyidentity

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Con estos datos se construye un modelo biométrico

formado por tres archivos asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Cuando el servicio recibe nuevas matrices de tiempos estas son procesadas y comparadas con el modelo almacenado en el bucket S3. Como resultado de este proceso Rekognition genera un nuevo registro en la base de datos guardando el porcentaje de similitud con el modelo y la matriz de tiempos procesada.

Datos Tratados

El servicio FaceIdentity almacena fotografías capturadas asociadas a un Id de usuario. Los datos biométricos no son gestionados por el servicio sino que son generados a partir de la fotografía por el api de AWS Rekognition. El api AWS Rekognition es la que genera el modelo biométrico y lo compara con el del usuario devolviendo a Faceidentity el porcentaje de similitud entre modelos. FaceIdentity por tanto no gestiona ni almacena estos datos biométricos.

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Con estos datos se construye un modelo biométrico formado por tres archivos asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Como resultado de este proceso Rekognition genera un nuevo registro en la base de datos guardando el porcentaje de similitud con el modelo y la matriz de tiempos procesada.

Ubicación de los datos

<u>FACEidentity</u>

En el punto anterior se explica que FaceIdentity almacena fotografías, pero no gestiona ni trata datos biométricos, ya que estos son únicamente generados y gestionados por el servicio AWS Rekognition. Los datos que almacena FaceIdentity son las fotografías que se almacenan en S3 y los resultados de las identificaciones de dichas imágenes que se almacenan en AWS RDS.

Información sobre AWS Rekognition. Con las tres fotografías iniciales el servicio construye un modelo biométrico a partir del análisis de los rasgos faciales de estas fotografías. AWS Rekognition almacena internamente estos datos biométricos en una colección. Cada vez que se llama a Rekognition se le envía una fotografía y este servicio extrae los metadatos y los compara con las del modelo original devolviendo a FaceIdentity el porcentaje de similitud. Amazon Rekognition no conserva los bytes de las imágenes reales.

KeyIdentity.

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Estos datos son almacenados en registros de una base de datos en AWS RDS (Relational Database Service).

Con estos datos se construye un modelo biométrico formado por tres archivos que está asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Tecnologías Intervinientes

FACEidentity

FaceIdentity es por tanto un servicio que hace de interfaz entre el campus virtual, (capturando y almacenando las imágenes) y el servicio AWS Rekognition que realiza el análisis de las mismas.

Para el almacenamiento de los datos se utiliza AWS RDS como base de datos.

Para el almacenamiento de las imágenes se utiliza un bucket S3.

KeyIdentity

Para la construcción de los modelos biométricos se utiliza Deep Learning que es un modelo computacional basado en redes neuronales. Para la implementación de este desarrollo se han utilizado las librerías Keras y Tensor Flow.

Para el almacenamiento interno de las matrices de datos capturados se utiliza como base de datos AWS RDS.

Para el almacenamiento de los modelos se utiliza un bucket S3 de AWS.

Todos los datos están alojados en una cuenta de AWS Irlanda.

Actividades
FACEIdentity El servicio FaceIdentity tiene dos modos de funcionamiento: Identificación y monitorización. En la identificación FaceIdentity recibe una fotografía con el IdUsario al que se quiere identificar. La fotografía se procesa al api de Rekognition y es comparada con el modelo creado obteniendo el porcentaje de similitud. Este porcentaje es registrado en la base de datos RDS y a su vez se devuelve al campus como resultado una identificación positiva, negativa o incertidumbre. En la monitorización el sistema va recibiendo cada pocos segundos, imágenes a identificar, que son procesadas internamente por el api de Rekognition y los resultados registrados en la base de datos. En este caso no se devuelve al campus ninguna información en tiempo real. Es el campus quién solicita información sobre los resultados de esta secuencia de imágenes procesadas durante un examen. En este caso la información devuelta es el número de imágenes que no han superado la identificación en relación al total de imágenes capturadas en el examen. Si este valor está por encima de un umbral el resultado del examen se marca a REVISAR para que el supervisor pueda acceder al panel de supervisor de FaceIdentity y comprobar que ha sucedido tras una visualización manual de las fotografías capturadas. En caso contrario se considera que el comportamiento durante el examen ha sido el esperado y el examen queda autovalidado. En cualquier caso el supervisor puede acceder a la consola de Faceidentity y revisar las imágenes capturadas de cualquier examen. Consola de Supervisor Como hemos mencionado previamente el servicio FaceIdentity tiene una consola de Supervisión que muestra un listado con todos los usuarios registrados en el servicio y varios botones de acción con las siguientes funciones: Verificar.

Permite verificar el modelo biométrico. Para ello el supervisor debe comprobar que las 3 fotografías con las que se ha construido el modelo corresponden a la persona que se desea identificar.

Detalle.

Permite mostrar todos los registros de identificación de un usuario, mostrando la fecha y hora, el resultado de la identificación, y la fotografía si estuviera disponible (dado que se van eliminando según el periodo max de almacenamiento).

Resetear.

Permite eliminar el modelo biométrico del usuario de forma que en el próximo acceso le solicitará la creación de un nuevo modelo.

Eliminar.

Elimina completamente todos los datos registrados de un usuario.

Además, el servicio cuenta con una serie de parámetros de configuración para ajustarse a los requisitos de cada cliente.

Configuración

Para la parte de uso, se puede configurar los siguientes parámetros:

Configuración	Descripción	Posibles valores
Fotos de monitorización	Guardar las fotos.	-Todas -Solo las no positivas -Ninguna
Intervalo	Intervalo de tiempo en el cual se va a tomar una foto aleatoria en segundos.	-Valor numérico (30)
Permitir pasar fallos	En la pantalla previa al examen donde se validan los requisitos biométricos, permitir acceder al	-Permitir pasar -Repetir la foto

	examen, aunque el alumno no sea quien dice ser o no.		
Texto a mostrar	En la pantalla previa al examen donde se validan los requisitos biométricos, mostrar un texto informativo (útil para dar pautas al alumno antes de realizar un examen).	-Texto -No mostrar nada	

Alertas

El servicio FACEidentity dispone de un sistema de alertas por correo electrónico. Este sistema de alertas se puede configurar para enviar un correo electrónico en el caso de que se detecte una suplantación de identidad.

También se pueden configurar alertas para controlar el número de identificaciones que se han realizado en cada servicio. Si las identificaciones superan un determinado límite se enviaría un correo avisando al supervisor de la plataforma de que se ha superado el límite. Estos correos son meramente informativos.

KeyIdentity

El servicio de KeyIdentity tiene solamente un modo de funcionamiento: monitorización.

Este servicio va recibiendo las muestras de tiempos capturadas a medida que el usuario va escribiendo y el buffer está completo (unos 70 caracteres como mínimo). Cada una de estas muestras recibidas es comparada con el modelo biométrico del usuario y tanto la muestra como el porcentaje de similitud obtenido es almacenado en un nuevo registro de la base de datos.

Consola de Supervisor

Como hemos mencionado previamente el servicio KeyIdentity tiene una consola de Supervisión que muestra un listado con todos los usuarios registrados en el servicio y varios botones de acción con las siguientes funciones:

Detalle.

Permite mostrar todos los registros de identificación de un usuario, mostrando la fecha y hora, el resultado de la identificación.

Eliminar.

Elimina completamente todos los datos registrados de un usuario.

DATOS TRATADOS

Las categorías de datos personales objeto de tratamiento son las siguientes:

- Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.

FaceIdentity

Los datos tratados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

Para el servicio FACEidentity, se utilizan las tablas USUARIOS y LOGS. En las tabla USUARIOS se guardan:

- El id biométrico
- El id externo del usuario
- El id del cliente
- El número de fotos que ha utilizado el usuario para entrenarse (0 no está entrenado, 3 si está entrenado)
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)
- Si el usuario está verificado (el cliente ha validado el perfil biométrico desde la consola de supervisor)

En la tabla LOGS, se almacenan los siguientes datos:

- El id de la identificación
- El id biométrico del usuario
- La fecha en la que se ha realizado la comprobación

- El porcentaje de similitud con cada una de las fotos del entrenamiento
- El resultado obtenido (positivo, negativo o incertidumbre)
- La prueba de vida a la que se ha sometido el usuario (gesto en la fotografía)
- Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
- El id enlazado, id de la anterior comprobación si sigue en la misma sesión
- Si la foto está almacenada o no.
- El user agent.
- El posicionamiento de la cara respecto a la cámara, para saber si el usuario está mirando a la pantalla o no.
- El tipo de registro (identificación o monitorización)

Keyidentity

Para el servicio keyidentity los datos que se tratan son las matrices de tiempos de cada usuario, el useragent, ip del usuario.

Para el servicio KEYidentity, se utilizan las tablas KEYSTROKE_USUARIOS_TEXTO y KEYSTROKE_LOGS_TEXTO.

En la tabla KEYSTROKE_USUARIOS_TEXTO se guardan:

- El id biométrico
- El id del cliente
- El id externo del usuario
- Si el usuario está entrenado o no
- El número de registros que lleva el usuario
- El porcentaje actual de identificaciones correctas y el porcentaje de intentos ilícitos detectados en una prueba interna que se realiza para comprobar su robustez.
- Si el usuario se ha marcado como sospechoso y un comentario de porque se ha marcado así.
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)
- Si el usuario tiene que contar para la facturación.

En la tabla KEYSTROKE_LOGS_TEXTO, se almacenan los siguientes datos:

- El id de la identificación
- El id biométrico del usuario
- Los datos de los tiempos de tecleo de la identificación
- El tipo de registro (entrenamiento o identificación)
- El porcentaje de similitud con el modelo entrenado
- La fecha en la que se ha realizado la comprobación
- Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
- La IP, el navegador, el SO y la ciudad (basada en su IP) del usuario para saber de dónde vienen los datos
- El número de caracteres que tiene el registro
- Si la pantalla es táctil o no.
- El user agent.

QUIÉN TRATA LOS DATOS

El tratamiento se efectúa por la propia entidad responsable de tratamiento.

Asimismo, interviene ADR Infor S.L. proveedor que actúa en calidad de encargado de tratamiento.

TECNOLOGÍAS INTERVINIENTES

Política de seguridad de servicios biométricos.

Tecnología

Toda la tecnología utilizada en el proyecto está alojada en el cloud de Amazon Web Services.

El servicio en producción está alojado en AWS Irlanda y el plan de contingencia en AWS París.

Identificación de accesos al sistema

Autenticación por doble factor

Se ha establecido con carácter obligatorio la autenticación por doble factor para el acceso a la consola de supervisor de la plataforma a los servicios de identificación biométrica. Cada supervisor

de la plataforma, aparte de disponer de unas claves únicas, tendrá que superar el reconocimiento facial para poder acceder al panel de administrador. Si no supera dicha autenticación, el equipo de administradores de ADR recibe un correo alertando del intento de suplantación para poder tomar las medidas oportunas.

Dentro de ADR Formación, únicamente tienen acceso a dicho panel el equipo de administradores y solamente es utilizado para comprobar su correcto funcionamiento y dar soporte al cliente (IMF).

Logs de accesos al sistema.

Se guardan los logs de acceso al sistema durante un año. Estos logs se pueden analizar posteriormente si se ha detectado alguna irregularidad. En estos logs, se pueden filtrar los accesos de usuarios de la entidad gracias a que cada uno de ellos accede a través de un dominio diferente.

Los usuarios acceden a través de los dominios: faceidentity.adrformacion.com y keyidentity.adrformacion.com

El acceso a la consola de supervisor de la plataforma, en el acceso de administrador entran al dominio identify.adrformacion.com

Con estos logs, podemos realizar técnicas de análisis forense gracias a AWS Athena, un servicio de consultas interactivo que facilita el análisis de datos y permite verificar la legitimidad de los accesos.

Sistemas de seguridad

ADR Infor dispone de varias herramientas para la detección de intrusos y protección antimalware:

CLAMAV Es un antivirus que permite detectas troyanos, virus, malware y otras amenazas maliciosas.

WAF Es un firewall para aplicaciones web que nos ayuda a protegernos contra ataques web comunes que pueden afectar a la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. AWS WAF brinda control sobre cómo el tráfico llega a nuestras aplicaciones permitiéndonos crear reglas de seguridad que bloquean los patrones de ataque comunes, como la inyección de SQL o las secuencias de comandos entre sitios, y las reglas que filtran patrones de tráfico específicos que defina.

Cloudwatch con alarmas de umbrales definidas Es un servicio de monitorización y observación que ofrece datos e información procesable para monitorizar nuestra aplicación. Gracias a las alarmas definidas, podemos saber si hay cambios en los patrones de normalidad de uso del servicio.

DESTRUCCIÓN DE LOS DATOS

Actividades

Borrado automático de datos

FaceIdentity

Periodo de almacenamiento de fotografías.

Se ha programado un esquema para que el responsable de tratamiento pueda configurar los periodos de almacenamiento máximo para los diferentes tipos de imagen en cada configuración del servicio (identificación o monitorización). Transcurrido ese periodo de días, las imágenes son eliminadas de FaceIdentity.

ASIGNAR BORRADOFOTOS

Cliente	ADR Formación
Identificación	
Positivas	15 días
Incertidumbre	90 días
Negativas	90 días
Gesto incorrecto	90 días
Foto no válida	90 días
Monitorización	
Positivas	15 días
Incertidumbre	90 días
Negativas	90 días
Foto no válida	90 días

Para la eliminación del modelo biométrico almacenado en AWS Rekognition IMF dispone de una consola para eliminar de forma manual todos los datos registrados del usuario.

KeyIdentity Periodo de almacenamiento. Se ha programado un esquema para que el responsable de tratamiento pueda configurar los periodos de almacenamiento máximo para las muestras de datos almacenadas en RDS. Transcurrido ese periodo los datos serán eliminados de manera automática. Para la eliminación del modelo biométrico almacenado en Keyidentity IMF dispone de una consola que elimina todos los datos registrados del usuario.
Datos Tratados
Las categorías de datos personales objeto de tratamiento son las siguientes: - Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.
¿Quién destruye los datos?
Políticas automáticas definidas en el apartado anterior.
Tecnologías Intervinientes
Borrado automático de datos Si el responsable de tratamiento lo desea, puede guardar las imágenes para su posterior análisis, y para este caso, se ha programado un esquema para cada cliente en el que se pueden configurar los periodos de almacenamiento máximo para los diferentes tipos de imagen en cada configuración del servicio (identificación o monitorización). Transcurrido ese periodo de días, las imágenes son eliminadas definitivamente. Del mismo modo sucede con las matrices de tiempos registradas en el servicio KeyIdentity.

Cesión o transferencia de datos a terceros

Actividades
No están previstas cesiones, ni transferencias internacionales fuera del Espacio Económico Europeo
Datos Tratados
Las categorías de datos personales objeto de tratamiento son las siguientes: - Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.
Terceros involucrados
No aplica
Tecnologías Intervinientes
No aplica

6. ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

A. Inclusión del tratamiento en la lista de tratamientos exentos

Se puede determinar que el tratamiento de datos personales objeto de análisis no encaja en ninguno de los supuestos previstos como exentos de realización de la EIPD en la lista publicada por la AEPD dado que no aplica ninguna de las circunstancias previstas.

B. Análisis de la inclusión del tratamiento en los casos de tratamientos obligados

Desde la entidad responsable de tratamiento sé es consciente de que los sistemas de verificación elegidos para comprobar la identidad de sus alumnos, requieren un alto grado de protección en tanto son objeto de tratamiento, datos biométricos (pertenecientes a las categorías especiales de datos a que se refiere el artículo 9) y además se emplean nuevas tecnologías.

Asimismo, el tratamiento objeto de análisis tiene cabida en el tercer caso de los enumerados en el artículo 35.3 del RGPD, en su apartado b: *"tratamiento a gran escala de las* categorías

especiales de datos a que se refiere el artículo 9”.Adicionalmente, el tratamiento coincide con uno de los supuestos incluidos en el listado publicado por la Agencia Española de Protección de Datos en virtud del art. 35.4 RGPD, en los que se requiere la realización de una Evaluación de Impacto relativa a la Protección de Datos. Concretamente se refiere a *“Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física”*

Por eso y de cara a garantizar la privacidad de los interesados afectados por el tratamiento de datos personales, se ha decidido llevar a cabo la evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo.

C. Evaluación del nivel de riesgo

De acuerdo con el artículo 35.7.c del RGPD, se ha realizado una Evaluación de Impacto del tratamiento de Reconocimiento Facial y Dinámica de Tecleo para determinar e identificar los elementos de riesgo para los derechos y libertades de las personas.

Derivado del análisis realizado, la organización ha establecido como Nivel de Riesgo aceptable todo aquello que supere el nivel Medio, entre los 5 niveles sobre los que se realiza la evaluación, por lo tanto, todo aquello con un nivel Alto o Muy alto debe ser tratado por la organización.

En este sentido, se han obtenido unos riesgos no asumidos por la entidad siendo los siguientes:

- Tratamiento Reconocimiento facial y dinámica de tecleo:
    - Dificultad para la revocación del consentimiento o la manifestación de la oposición a un tratamiento con riesgo Alto.
- ADR
    - Inexistencia de contrato/acuerdo con los términos requeridos por RGDP con riesgo Alto.
    - Problemas de comunicación de los eventos de seguridad con riesgo Alto.

D. Análisis de la necesidad del tratamiento

Una vez efectuado anteriormente con éxito el análisis de licitud del tratamiento, procede ahora entrar a valorar la necesidad del tratamiento, para lo que se examinan las cuestiones indicadas a continuación:

- **Justificación del tratamiento:** la implantación del tratamiento anteriormente descrito en IMF responde a la necesidad de garantizar, con el menor margen de error posible, que las personas que están cursando los estudios se corresponden efectivamente con aquellas que realizan los exámenes y pruebas online.

En este sentido, en la memoria de planificación de las enseñanzas se fija que la Universidad debe verificar fehacientemente que el alumno es quien desarrolla las pruebas de evaluación, ya sea en un examen de carácter presencial o mediante video conferencia. Asimismo, las competencias específicas establecen que los alumnos deben utilizar las tecnologías de la información y las comunicaciones para la búsqueda y obtención de información jurídica, así como herramientas de trabajo y comunicación.

De las reuniones de toma de datos para configurar el tratamiento, así como de las reuniones de valoración de riesgos efectuadas con la organización, se desprende que los datos se van a utilizar exclusivamente para la finalidad declarada y para ninguna otra no informada o incompatible con la legitimidad de su uso, dando cumplimiento así al principio de limitación de la finalidad.

- **Expectativas del afectado:** atendiendo a que el RGPD marca que la ponderación debe hacerse teniendo en cuenta la expectativa razonable de los interesados en función de su relación con el responsable, podemos concluir que se da total cumplimiento a este punto, en tanto al afectado por el tratamiento, en este caso, a los alumnos, les cabe esperar que los datos relativos a sus rasgos faciales y dinámica del tecleo serán objeto de tratamiento. Ello porque, al inicio del tratamiento, el interesado es debidamente informado de este tratamiento, así como de todos los aspectos relacionados con el mismo, y son accesibles para los alumnos los datos de contacto del Delegado de Protección de Datos, con quien pueden consultar ante cualquier cuestión que les surja en relación con el tratamiento de datos personales que se pretende realizar.

- **Grado de invasión en la privacidad de los interesados:** en este caso debemos analizar si la intrusión en la esfera de la intimidad de las personas es proporcional a la finalidad requerida. Pues bien, partiendo de la premisa de que los datos personales descritos únicamente serán objeto de tratamiento exclusivamente durante el tiempo en que el alumno esté haciendo uso del Campus, parece que dicho tratamiento de datos no resulta desproporcionado atendiendo a

la finalidad perseguida por el responsable de tratamiento, toda vez que además el mismo ha prestado su consentimiento.

- **Minimización de datos personales:** tras la realización del análisis de los datos tratados en el presente tratamiento, se desprende el cumplimiento de la organización con el principio de minimización de datos, ya que no existen datos que no se utilicen por los empleados autorizados, ni se recopilan datos que no tengan utilidad para la finalidad del tratamiento ni para los interesados afectados. La finalidad que se pretende lograr a través del presente tratamiento requiere de todos los datos objeto de tratamiento, ya que de lo contrario no sería posible la identificación unívoca del interesado y en consecuencia, no se podría determinar sin margen de error, que el alumno que realiza el examen es efectivamente aquel que se encuentra matriculado en el curso. Ello porque los métodos alternativos como tarjetas identificativas, contraseñas o similares podrían ser utilizados por otros individuos, dando lugar con ello a posibles suplantaciones de identidad.

- **Minimización del plazo de conservación:** en cumplimiento del principio de minimización del plazo de conservación, cabe mencionar aquí que los datos personales únicamente se conservarán durante el plazo estrictamente necesario para cumplir con la finalidad que se pretende.

En esta línea, y en cumplimiento del principio de responsabilidad proactiva, existe el pleno compromiso de la entidad en dar cumplimiento a las políticas de conservación implementadas que garanticen que los datos personales obtenidos sean suprimidos efectivamente. En este sentido, se conservarán los datos personales únicamente por el plazo concreto en el que el alumnado está cursando el estudio de máster o grado. Pasado este plazo, los datos personales serán suprimidos.

- **Accesibilidad:** en relación con las cuestiones relacionadas con la accesibilidad, es preciso destacar que estos datos personales no serán revelados a terceros no autorizados, ni siquiera a un gran número de personas dentro de ambas entidades. Únicamente podrá tener acceso el personal designado para ello y que concretamente será el personal de Secretaría Académica de IMF International Business School S.L y el personal técnico de ADR formación, proveedor con quien se ha firmado el contrato de encargado de tratamiento.

- Medidas de seguridad: las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales

de la privacidad. Se aplican controles respecto de las tecnologías empleadas, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales de los usuarios gestionados durante el proceso.

Una vez analizados los aspectos más relevantes del tratamiento de datos personales cuyo análisis nos ocupa, es conveniente asegurar a continuación que el mismo supera con éxito el juicio de idoneidad y necesidad pertinente:

- **Juicio de idoneidad:** se puede concluir que la medida establecida cumple con el objetivo propuesto y que no es otro que el de garantizar que los alumnos que realizan los exámenes y pruebas online se corresponden con aquellos que se encuentran matriculados en el curso, verificando así su identidad de forma fehaciente e inequívoca.

- **Juicio de necesidad**: en este sentido, se puede afirmar que dicho tratamiento es necesario, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia, puesto que únicamente haciendo uso de datos biométricos es posible identificar unívocamente a las personas. Cualquier otro método que no utilice datos biométricos no cumplirá de forma fidedigna con dicho objetivo.

E. Beneficios para los interesados

En este apartado se pretenden identificar los beneficios directos para el conjunto de la sociedad, así como para los sujetos concretos sobre los que se tratan los datos personales.

El principal beneficio que obtiene el alumnado es poder realizar los exámenes cómodamente desde su casa, sin la necesidad de realizar traslados a la sede correspondiente que IMF tiene habilitadas para los exámenes presenciales, con el consiguiente ahorro de tiempo y dinero. Asimismo, la realización del examen en un entorno controlado reduce la presión a la que se ve sometido en situaciones imprevistas, lo que facilitará su concentración en la prueba.

Por otro lado, los exámenes online favorecen la calendarización de dichas pruebas, de tal modo que se puede ajustar con mayor precisión el momento de estudio y el de su evaluación, pudiendo ofrecer al alumnado la posibilidad de examinarse de la materia en el mismo mes que la cursa, favoreciendo así la evaluación continua. De igual modo, la realización de exámenes mes

a mes evita tener que presentarse el mismo día a diferentes exámenes, tal y como sucede actualmente en los exámenes presenciales.

Atendiendo a la movilidad geográfica, son muchos los alumnos que por diversas razones se ven obligados a cambiar de residencia a lo largo de los estudios, bien sea de ciudad o, incluso, de país. Esto genera problemas de desplazamiento al lugar de origen para poder realizar el examen o posponer los estudios hasta el regreso. Con la modalidad de exámenes online tiene la total garantía de que, esté en el lugar de mundo que esté, siempre podrá realizar los exámenes y completar sus estudios en el tiempo previsto.

F. Beneficios para la Entidad

Es preciso identificar en el presente apartado los beneficios que se derivan para la Entidad. En este sentido, es conveniente señalar que el principal beneficio que se deriva para la entidad con la implantación del tratamiento en cuestión es poder ampliar el público al que ofertar los servicios educativos. Eliminando la necesidad de acudir presencialmente a las sedes de la entidad, existe la posibilidad de contar con alumnos desde cualquier punto geográfico, tanto nacional, como internacional.

Cabe destacar también que este sistema permite a IMF planificar mejor las enseñanzas, siempre en aras de que el alumnado consiga la mayor calidad en la formación con los mejores recursos tecnológicos, tal y como se espera de la aplicación de la biometría para la realización de exámenes en modalidad online.

Asimismo, se desea destacar que la implantación del sistema de verificación a través de reconocimiento facial y dinámica del tecleo resulta innovador en un sector educativo que debe apostar por las virtudes que traen consigo los avances tecnológicos.

Adicionalmente, y derivado de lo anterior, se obtendría por parte de la entidad una notable mejora reputacional en tanto IMF sería pionera en la implantación de tan avanzada y ágil solución tecnológica.

G. Alternativas al Tratamiento y por qué no se han elegido.

El presente tratamiento se ha diseñado entendiendo el mismo como una mejora y extensión de un tratamiento ya existente en la entidad, que no era otro que el del seguimiento y evaluación

de los alumnos que cursan sus estudios en IMF como resultado de la relación contractual entre las partes.

Aunque ya se ha mencionado anteriormente, son múltiples las razones que justifican la modificación del tratamiento de cara a posibilitar la realización de los exámenes y pruebas de forma online, pero se desea a continuación incidir en las mismas:

- Mayor garantía de éxito derivado del sistema de evaluación continua.

- Reducción de costes derivados del desplazamiento para los alumnos.

- Reducción de esfuerzos para los alumnos.

- Innovación tecnológica.

- Máxima seguridad y garantías en la realización de exámenes.

- Mayor accesibilidad a los servicios ofrecidos por la entidad.

- Mejora reputacional de la entidad.

7. MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

A. Optimización del tratamiento

El tratamiento se da durante todo el ciclo en el que la matricula está en vigor, ya que cada vez que el alumno acceda a la plataforma para realizar la evaluación continua, deberá hacer uso de los datos objeto del tratamiento.

Las fases que están definidas en el tratamiento son las siguientes:

- Aceptación durante el proceso de matriculación

- Creación del perfil biométrico al acceder a la plataforma

- Acceso y monitorización del uso de los datos biométricos

- Acceso a exámenes.

- Finalización del proceso de matrícula y borrado del perfil biométrico

B. Medidas PbDD

IMF tiene implantados unos controles operacionales y técnicos de manera permanente para la gestión de los datos de los interesados asociados a los cursos que se imparten, con el fin de garantizar la privacidad de los mismos. Los controles se describen a continuación:

Minimización

- **Eliminación temprana de los datos no necesarios**: el sistema de Faceidentity está adaptado para eliminar los datos biométricos a petición del usuario o por revocamiento de la autorización del uso de dichos datos. Asimismo, por parte de IMF existe la posibilidad de adoptar los plazos que se deben configurar de acuerdo a la política de plazos de conservación y supresión anteriormente detallada.
- **Minimización de los datos recogidos y tratados en cada etapa del tratamiento**: los datos personales que se recogen son únicamente los estrictamente necesarios para la finalidad que se pretende. En este sentido, se cuenta con dos identificadores. Un primer identificador interno que pertenece a cada usuario, junto a los datos biométricos y un identificador externo en el que se incluye únicamente nombre y apellidos.
- **Limitación de la accesibilidad de bases de datos a través de la red**: existe limitación en tanto las bases de datos se encuentran cifradas y protegidas por usuario y contraseña.
- **Seudoanonimización de los datos almacenados**: junto con los datos biométricos, se minimiza al máximo los datos personales. El único campo es el identificador externo donde el responsable de tratamiento es el que establece que información se incluye y que en este caso se trata de nombre y apellidos.

Ocultación

- **Seudoanonimización de los datos almacenados:** tal y como se indica anteriormente, junto con los datos biométricos, se minimiza al máximo los datos personales. El único campo es el identificador externo donde el responsable de tratamiento es el que establece.
- **Control de la privacidad de los metadatos en las comunicaciones electrónicas:** todos los datos personales se encuentran cifrados y se transmiten cifrados por canal seguro a través de https.
- **Uso de credenciales:** para acceder al servicio se utiliza un doble factor de autenticación compuesto, en primer lugar por usuario y contraseña, así como por un segundo control con el uso de datos biométricos.
- **Cifrado de la información almacenada o en tránsito:** es preciso destacar que

actualmente la base de datos se encuentra cifrada y se ha marcado como plazo la fecha de 15 de mayo de 2020, en la que las medidas de cifrado se extenderán también a las imágenes. Se cifrará el Buckets S3 que contienen los ficheros y la información biométrica. Asimismo, es preciso resaltar que los datos personales viajan en canal seguro.

Agregación

- **Generalización de datos personales:** los datos personales que se almacenan son mínimos. Tal y como se indicaba anteriormente, únicamente se almacenará el identificador externo e interno en los términos descritos.
- **Reducción de la precisión/granularidad de recogida de los datos**: Se conserva la IP y el agente de usuario (navegador desde el que se accede), que es precisamente la información que permite las verificaciones en la base de datos

Información

- **Clausulas RGPD en condiciones generales del proveedor:** el contrato de colaboración con ADR Infor, recoge las condiciones generales del tratamiento de los datos según la normativa RGPD.
- **Aceptación de términos y condiciones (primera relación, acceso plataforma, realización examen):** Se establece un procedimiento de aceptación de términos y condiciones del uso de datos biométricos en tres fases o capas.

- En el proceso de matriculación.
- En el acceso a la plataforma tecnológica.
- A la realización del examen (recordatorio del acceso).

- **Política de privacidad:** Se recogen las condiciones de uso de los datos personales en las cláusulas informativas destinadas a recabar el consentimiento de los interesados. Se adjunta a través del **Anexo IV**, un ejemplo de cláusula informativa en el momento de preinscripción del alumno, así como de solicitud de consentimiento en el momento de acceder al Campus

Control

- **Contrato RGPD:** Acuerdo contractual con los alumnos que incluyen los requisitos necesarios para garantizar los derechos de los interesados, abarcando el derecho de información del

tratamiento, consentimiento a la hora de gestionar los datos, acuerdos de confidencialidad, así como el método para ejercer los derechos como interesado.

- **Formación usuarios:** formamos a los usuarios en políticas de Compliance y uso de los datos sensibles contemplados en la RGPD.
- **Auditorías:** como medida a futuro, se establecerán auditorías tanto jurídicas, como técnicas, que se realizarán a través de un empresa externa..

Cumplimiento

- **Medidas disciplinarias/sanción**: Se establecen procedimientos para el correcto uso de los datos y evitar intentos de fraude en el tratamiento de los datos biométricos.
- **Procedimiento para el tratamiento de la información**: está establecido un procedimiento para el tratamiento de la información y para el correcto funcionamiento de la identificación del alumno a partir del perfil de datos biométricos.

Medidas de Accountability

- **Procedimiento Alta/Baja/Modificación empleados y resto de usuarios**: existe un procedimiento de altas y bajas para aquellos usuarios que tienen acceso al tratamiento de los datos de carácter personal, con un anexo que explica el uso de los datos sensibles.
- **Usuarios nominales (no genéricos).** Todos los perfiles que tienen acceso a datos de carácter sensible usan usuarios nominales, para garantizar la trazabilidad del acceso a los datos biométricos.
- **Gestión de contraseñas (longitud, complejidad, caducidad)**. Tenemos una política de contraseñas cumpliendo los niveles de longitud y complejidad para garantizar que no sea fácil acceder suplantando la identidad de los usuarios, caducando la contraseña a los 90 días. Dicha contraseña no se puede repetir en un plazo inferior a un ciclo de 10 cambios.
- **Se cuenta con un DPD** que coordina y gestiona un departamento de protección de datos externo, compuesto por una consultora integral para el asesoramiento en materia de protección de datos y un abogado en ejercicio experto en protección de datos.

Medidas de Seguridad

- **Gestión de Privilegios (asignación correcta de accesos):** el acceso a los datos está controlado por una gestión de privilegios, garantizando que solo los usuarios que tengan autorización podrán acceder a los datos objeto del tratamiento.

- **Copias de seguridad:** como se ha explicado anteriormente, están establecidas políticas de backup de los datos y de los servidores donde se alojan los datos. Además se hacen pruebas de recuperación para garantizar que el proceso cubre las necesidad de la organización.
- **Implantación de antivirus:** como política de empresa, todos los equipos tienen instalado y actualizado al día el antivirus Microsoft Defender, gestionado desde los servidores de System Center.
- **Pruebas de compatibilidad de software**: Se establecen pruebas de compatibilidad para el uso de la tecnología antes de cualquier actualización que garantice el correcto funcionamiento de las distintas plataformas existentes.

8. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

Una vez realizado con éxito el juicio de proporcionalidad y necesidad del tratamiento objeto de análisis, así como habiendo asegurado que se encuentran implantados los controles y medidas de seguridad necesarios para garantizar que el tratamiento no supone una medida restrictiva para los derechos fundamentales de los interesados, se puede determinar que el tratamiento es ponderado y equilibrado, ya que, como se ha podido desarrollar a lo largo del presente informe, se derivan más beneficios y ventajas para los interesados que perjuicios.

Plan de acción

En base a los riesgos identificados en el apartado VII Análisis de la Obligación de realizar una EIPD: Evaluación del riesgo, se ha establecido el siguiente plan de acción para mitigar los riesgos obtenidos:

- Tratamiento Reconocimiento facial y dinámica de tecleo**:**
    - Dificultad la revocación del consentimiento o la manifestación de la oposición a un tratamiento para el que se aplica el siguiente control:

        - **Información al alumno**: Informar al alumno que si revoca el tratamiento de datos biométricos pierde su opción a evaluación continua, derivando a 2 evaluaciones anual como marca la norma académica.

- **ADR**
    - Inexistencia de contrato/acuerdo con los términos requeridos por RGDP para el que se aplica el siguiente control:
        - **Queda Documentado el Anexo Datos Biométricos (ADR)** con las medidas de seguridad y protección de los datos de los alumnos.
    - Problemas de comunicación de los eventos de seguridad para el que se aplica el siguiente control:
        - **Procedimiento Brechas de Seguridad**: Se dispone de un procedimiento de brechas de seguridad, con los tiempos de respuesta correctamente definidos.

Al margen de estas medidas para tratar los riesgos no asumidos, se aplican medidas desde el diseño tales como:

- Autenticación por doble factor.
- Logs de accesos al sistema.
- Borrado automático de datos.
- Política de backups.
- Plan de recuperación ante desastres.
- Antivirus CLAMAV.
- Firewall de Aplicaciones Web (WAF).
- Cifrado https: es necesario resaltar que actualmente la base de datos se encuentra cifrada y se ha marcado como plazo la fecha de 15 de mayo de 2020, en la que las medidas de cifrado se extenderán también a las imágenes. Se cifrará el Buckets S3 que contienen los ficheros y la información biométrica. Asimismo, es preciso resaltar que los datos personales viajan en canal seguro

9. CONCLUSIONES Y RECOMENDACIONES

Es preciso destacar aquí, que por parte de la entidad Instituto de Ciencias Empresariales de IMF S.L. (en adelante IMFICE), en el mes de septiembre de 2019 se realizó con éxito una prueba piloto del tratamiento descrito a lo largo del presente documento. La mencionada prueba piloto consistió en la realización de exámenes a través del sistema de verificación biométrico. Concretamente, se efectuó en el grado de ADE y Derecho que Instituto de Ciencias Empresariales de IMF. S.L. oferta y afectó a un total de 10 alumnos en el Grado de ADE y 60 en el Grado Derecho.

Se desea dejar constancia de que en todo caso, en virtud del principio de responsabilidad proactiva y de privacidad desde el diseño y por defecto, se dio cumplimiento a lo dispuesto en el RGPD, así como en la LOPDGDD. Entre otras se llevaron a cabo las siguientes acciones:

- Análisis exhaustivo sobre la licitud del tratamiento
- Configuración del registro de actividades
- Elaboración de las cláusulas informativas destinadas a recabar el consentimiento del interesado
- Realización de la EIPD
- Implantación de las medidas y controles de seguridad tendentes a asegurar la privacidad de los interesados

En virtud de lo anteriormente expuesto, cabe destacar que como resultado de la realización de la EIPD, se pudo determinar que no existía un riesgo alto para los derechos y libertades de los interesados en tanto se contaban con las medidas y controles suficientes y el alcance era claramente acotado.

En este sentido, se acompaña EIPD actualizada de IMFICE donde se ha realizado sobre un tratamiento ya existente con el nuevo modelo de informe facilitado por la AEPD (**Anexo V**).

Es ahora cuando, de acuerdo a lo descrito a lo largo del documento, y en aras de ampliar el tratamiento actualmente acotado a IMFICE, a otros estudios (másteres), se presenta la EIPD sobre el potencial tratamiento de datos efectuado por parte de IMF International Business School S.L. en calidad de empresa principal del grupo IMF.

En este sentido, como cambios significativos respecto a la inicial EIPD, que justifican la realización de esta nueva EIPD, es importante resaltar que se ha adaptado la EIPD al modelo

recientemente publicado por la AEPD, se incluyen medidas de seguridad más robustas, incidiendo sobre todo en hacer extensivo el uso de cifrado en un corto periodo de tiempo (15 de mayo de 2020) en los términos descritos anteriormente.

Es por ello, que se estima la necesidad de realizar una consulta previa a la Agencia de Protección de Datos antes del inicio del tratamiento, dado que se considera que de acuerdo a la EIPD presentada se muestra que el tratamiento entrañaría un alto riesgo si no se toman medidas para mitigarlo, en tanto se utilizan nuevas tecnologías, así como datos especialmente protegidos, como son los datos biométricos.

Asimismo, con las indicaciones que pueda facilitar la AEPD se valorará la confección de EIPD al resto de empresas del grupo para poder llevar a cabo el tratamiento de los datos como responsables del mismo.

Procede traer a colación aquí el hecho de que actualmente se está trabajando desde el Grupo IMF en la redacción de unas normas corporativas vinculantes en aras de garantizar el más estricto cumplimiento de la normativa vigente en materia de protección, así como los más altos estándares de privacidad respecto a los datos personales cuya protección nos encomiendan nuestros alumnos.

En esta misma línea, se hace necesario destacar que adicionalmente se está elaborando un código de conducta para todo el Grupo IMF, que permitirá una correcta autorregulación de las entidades que conforman el mismo.

En …….. a …….…. de …….……. de 2020

Firma en nombre de la entidad responsable del tratamiento

ANEXO I: DETALLE DE PREGUNTAS GENERALISTAS DESTINADAS A LA CONFIGURACIÓN DEL PERFIL BIOMÉTRICO.

Para la creación del modelo biométrico basado en patrones de tecleo se utilizan siete textos que el usuario debe escribir mediante el uso del teclado. Dado que los ritmos de tecleo son ligeramente diferentes cuando un usuario se limita a copiar un texto que cuando está escribiendo fruto de algo que ha pensado se somete al usuario a una serie de preguntas intrascendentes en las que deba razonar una respuesta.

Es importante destacar que las respuestas que teclea el usuario no se almacenan, solamente se miden los ritmos de tecleo.

Las preguntas a las que el usuario debe responder para crear el patrón de tecleo son estas:

- ¿Qué es y para qué sirve una taza?
- ¿Qué es y para qué sirve un bolígrafo?
- Describe el argumento de la última película que has visto.
- ¿Qué es un arco iris y qué colores tiene?
- Describe algunos elementos de una vivienda.
- Describe algunos elementos de un coche.
- Describe lo que puedes encontrar en un campo de fútbol.

Esquema funcional se los servicios biométricos

Funcionamiento

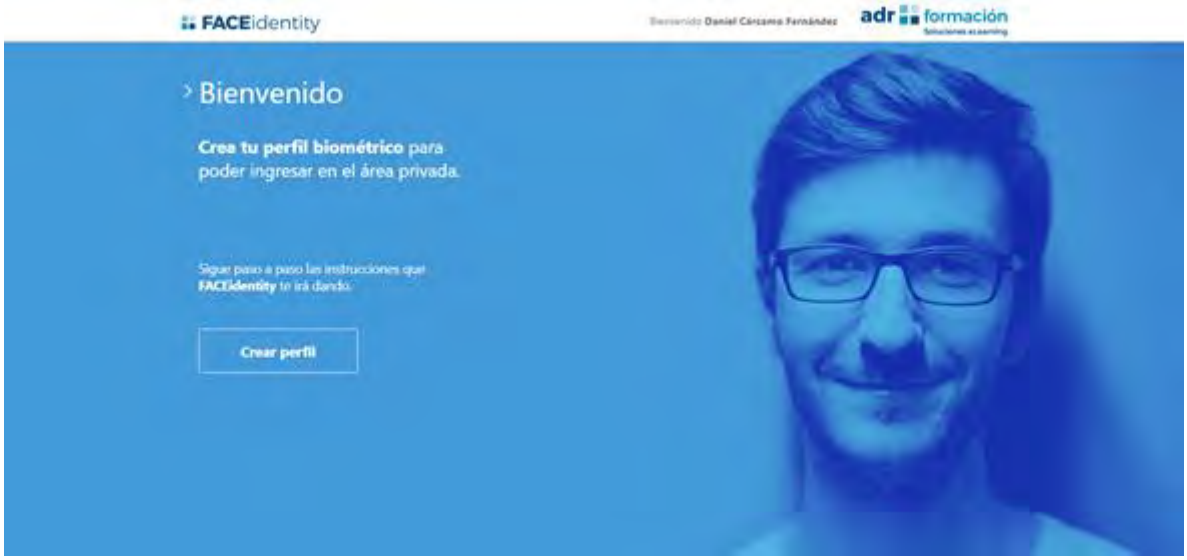
FACEidentity

FACEidentity es un sistema de reconocimiento facial que se puede utilizar en diferentes situaciones en las que sea necesaria la verificación de identidad del usuario, como por ejemplo acceso a área privada, exámenes online o webinars.

Disponemos de 2 formas de integración. Se puede utilizar para identificar a los usuarios, por ejemplo, en los accesos al campus. En esta integración, se toma una fotografía y se valida contra el perfil del usuario, permitiéndole acceder si el resultado es correcto.

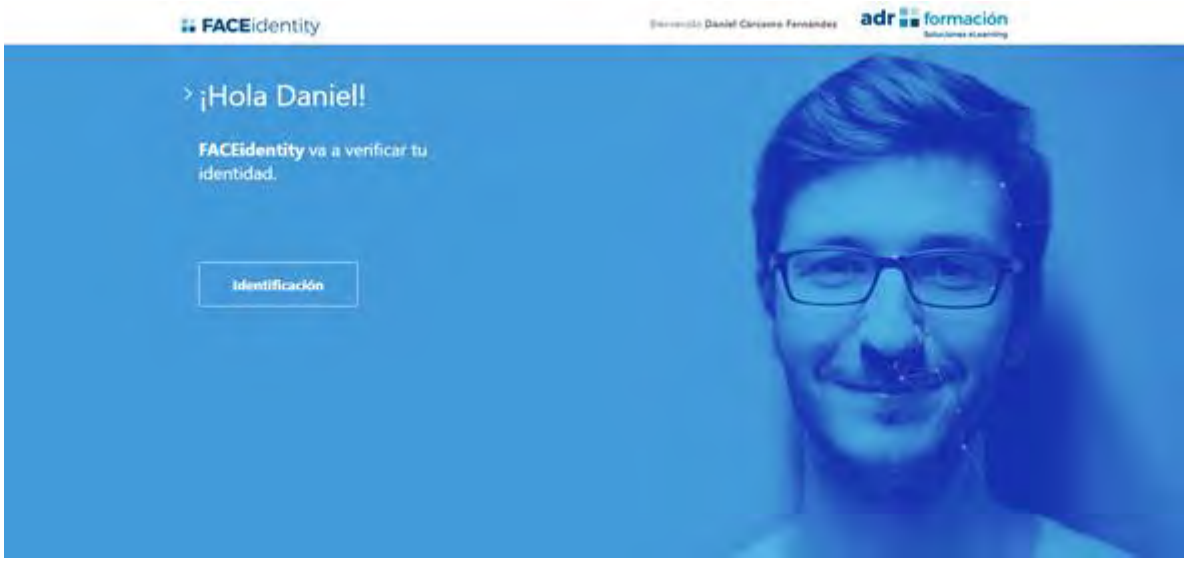
FACEidentity también se puede utilizar para monitorización continua, por ejemplo, para validar la autoría de un examen online. FACEidentity irá tomando fotos del usuario cada cierto periodo de tiempo y las validará contra su perfil.

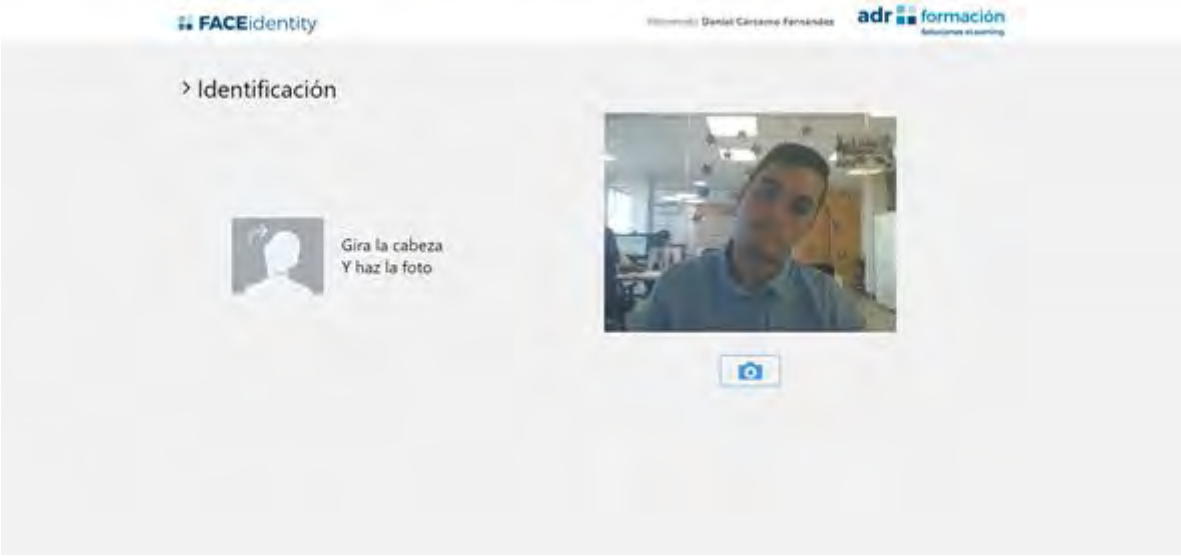
En el primer acceso a FACEidentity se realizan 3 fotografías con las que se crea el perfil biométrico del usuario. Estas fotografías deben cumplir con unos requisitos para la correcta creación del perfil, una correcta iluminación, que los ojos estén abiertos o que solo aparezca una persona en la foto. Este perfil puede ser validado, reseteado o eliminado por el administrador.



Una vez que el usuario tiene creado su perfil, en los siguientes accesos se realiza una fotografía, la cual se valida contra dicho perfil. Estas fotografías también deben de cumplir los requisitos oportunos. No importa los cambios de apariencia (pelo, barba, gafas), los parámetros biométricos recogidos por FACEidentity permiten identificar correctamente al usuario.

El proceso de reconocimiento consta de diferentes pruebas de vida que aseguran la presencia física del usuario frente a la cámara, como pueden ser girar la cabeza o sonreír.





Si en el proceso se encuentra una foto errónea, bien sea por que no cumple los requisitos o porque ha fallado la prueba de vida, el servicio pedirá al usuario que repita la fotografía solucionando el error generado. El cliente puede estipular unos límites de intentos de fotos.

El servicio devuelve el porcentaje de la similitud de la foto tomada con el perfil, dicho porcentaje lo hemos dividido en 3 umbrales.

-Positivo >=70%

-Incertidumbre <70% y >=50%

-Negativo <50%

Dependiendo del resultado obtenido, el cliente puede configurar el servicio para que realice una acción u otra.

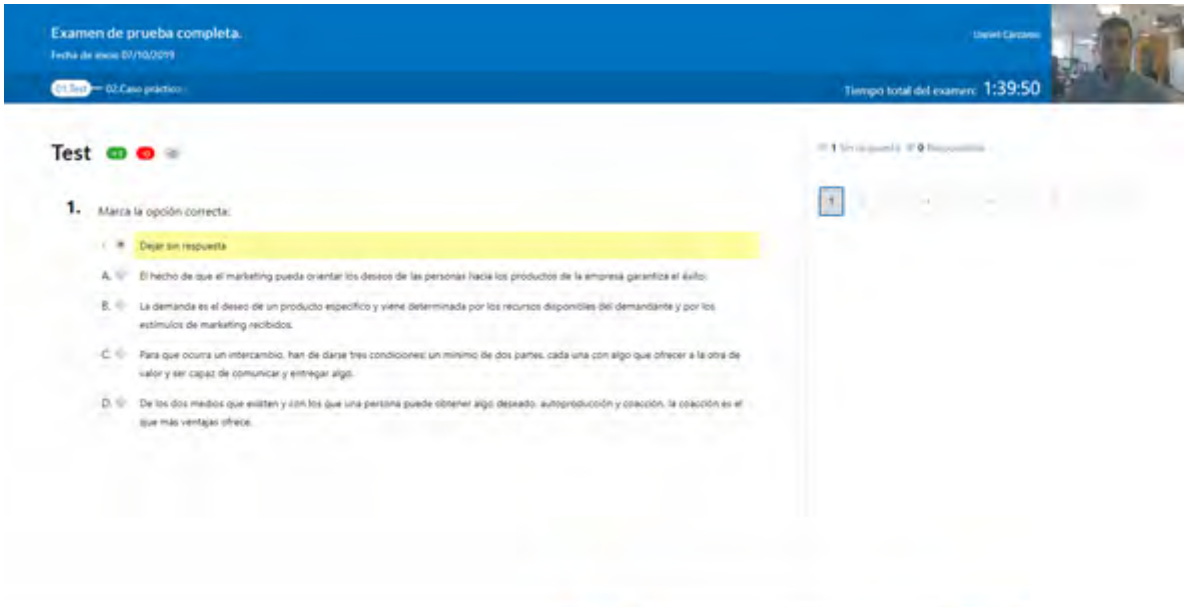
En la parte de monitorización, es necesario que el usuario ya disponga de un perfil biométrico creado anteriormente. El sistema irá tomando fotografías en un intervalo de tiempo configurado por el cliente. Cada fotografía se envía al servidor de FACEidentity y se valida contra su perfil. Al terminar la monitorización continua, el cliente podrá observar en el panel de administración los resultados de dicha sesión y tomar las medidas oportunas.

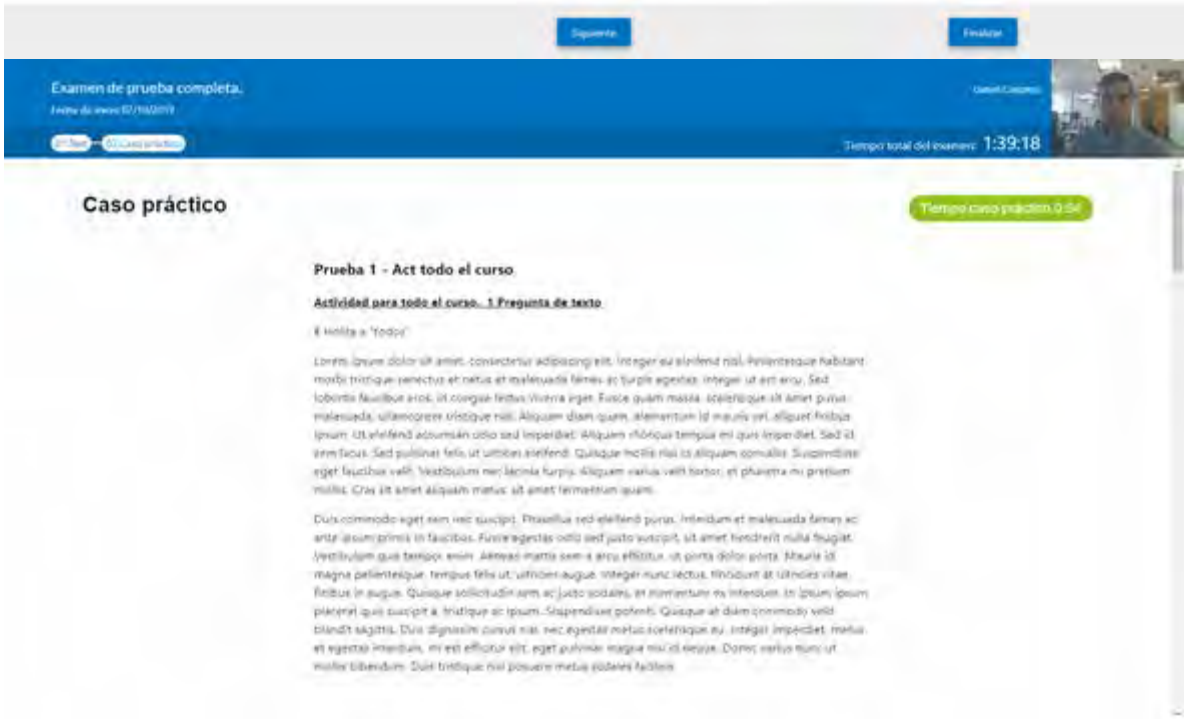
En la parte de monitorización continua, primero se comprueban los requisitos biométricos para saber que el usuario dispone de una webcam y la tiene habilitada.

adr formación
adr formación
> Validación de los requisitos para realizar el examen biométrico
Continuar

adr formación
adr formación
> Validación de los requisitos para realizar el examen biométrico
Intrucciones antes de comenzar el examen.
Recomendaciones
• Evitar una mala iluminación y el contraluz.
• Asegúrate de tener bien enfocada la webcam.
• Se tiene que ver la cara al completo en el recuadro de la imagen.
• No estar muy cerca o muy lejos de la cámara.
• Mantener la vista mirando la pantalla.
Se considera infracción
• Copiar en este examen.
• Consultar información en un libro o en cualquier dispositivo electrónico.
• Tapar la webcam.
• Recibir ayuda de otra persona.
• Abandonar el examen, es decir, en todo momento tiene que mostrarse tu imagen en el encuadre de la webcam.
• Mirar hacia abajo o hacia los laterales, especialmente en el apartado de tipo test. Debes mantener la vista mirando la pantalla.
El incumplimiento de las normas puede ser causa de invalidación del examen o de suspenso directo en el mismo.
Te recordamos que el sistema captura imágenes durante todo el examen.
Aceptar

Una vez validados correctamente los requisitos biométricos llegamos al examen





KEYidentity

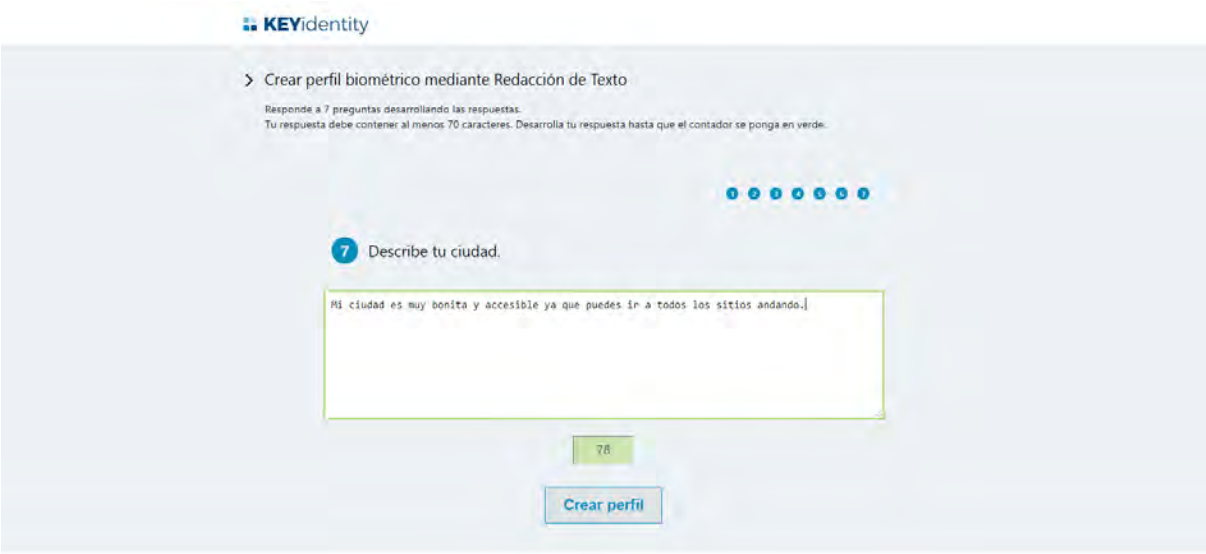
KEYidentity es un servicio de reconocimiento del patrón de tecleo mediante inteligencia artificial. Es un servicio privado, no se tiene en cuenta lo que el usuario escribe, sino cómo lo escribe. Además, es transparente para el usuario por lo que es menos invasivo que otros tipos de reconocimiento biométrico.

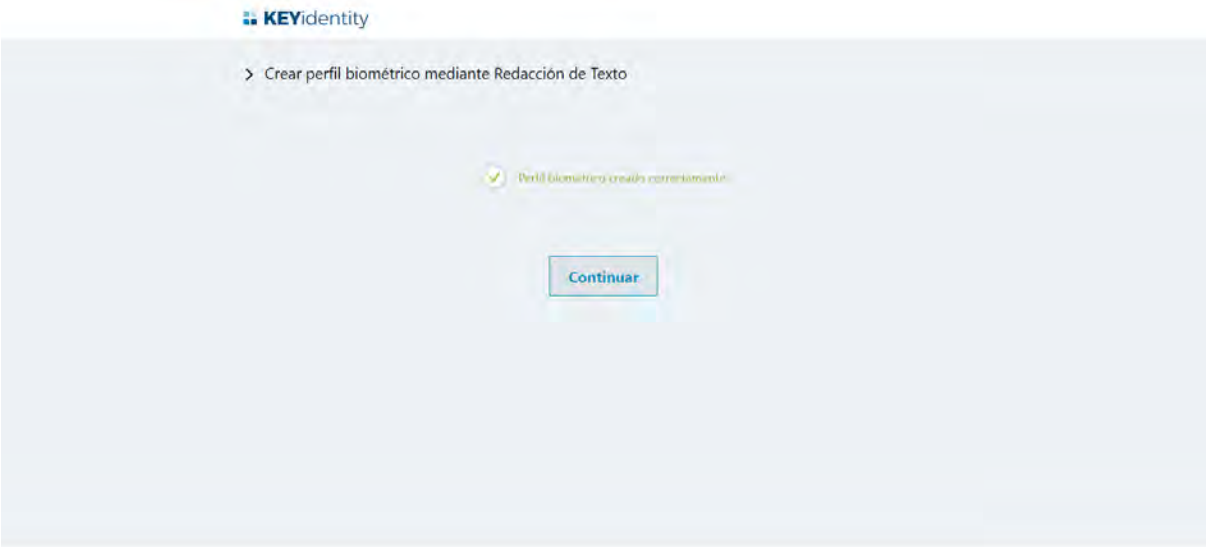
KEYidentity dispone de una pantalla de creación del perfil si así se desea. Si no se utiliza la pantalla de creación de perfil, el sistema tomará los 7 primeros registros del usuario para crear su perfil biométrico.

Hay dos formas de integrar KEYidentity. La integración completa, que captura los datos de todos los elementos donde se pueda escribir de la página. Y la integración personalizada, que permite al cliente seleccionar de qué campos desea recoger los datos de tecleo. En ambos casos se pueden capturar los datos de tecleo de editores avanzados de texto como CKEditor o Summernote.

KEYidentity es un servicio aplicable en diferentes situaciones en las que sea necesaria la verificación de que un usuario ha escrito un texto como exámenes, actividades, foros…

Existen 2 posibilidades para la creación del perfil. La recomendada es mediante la pantalla de creación de perfil, en la cual el usuario dispone de unas instrucciones y debe introducir 7 textos para que se cree el perfil biométrico.





La otra opción es sin la pantalla de registros, en esta opción, con los 7 primeros textos que introduce el usuario se crea su perfil.

Una vez concluida la fase de entrenamiento, en los formularios en los que se configure para recoger los datos de tecleo, el sistema captura los ritmos del usuario, los envía al servidor de KEYidentity y comprueba contra su perfil biométrico la identidad del mismo.

Configuración

El cliente en el servicio **FACEidentity** puede realizar las siguientes configuraciones para la parte de **identificación**:

Configuración	Descripción	Posibles valores
Fotos de registro	Guardar las 3 fotos de registro	-Si -No
Fotos de comprobación	Guardar las fotos de comprobación	-Todas -Solo las no positivas -Ninguna
Pruebas de vida	Realizar gestos para comprobar la presencia	-Si (4 gestos) -No
Fotos prueba de vida	Guardar las fotos de la prueba de vida (Si está activada)	-Si -No
Omitir creación perfil FACEidentity	Tener habilitado el botón de omitir FACEidentity (Si no se detecta la webcam en un usuario el botón aparecerá)	-Si -No
Omitir identificaciones FACEidentity	Tener habilitado el botón de omitir FACEidentity (Si no se detecta la webcam en un usuario el botón aparecerá)	-Si -No
Nº máximo de intentos	Permite saltar el reconocimiento si el usuario alcanza un nº de intentos de realizar la fotografía incorrecta	-Valor numérico (3) -No permitir saltarlo
Autenticaciones negativas	Dejar pasar al usuario que no se ha logrado identificar (obtiene un resultado negativo) o realizar otra fotografía.	-Dejar pasar -Tomar otra foto
Nº máximo de suplantaciones	Permite saltar el reconocimiento si el usuario alcanza un nº de intentos de superar el reconocimiento facial	-Valor numérico (3) -No permitir saltarlo
Configurar incertidumbre	Permite establecer el umbral de 50% a 70% como positivo o como negativo	-Positivo -Negativo
Protección de datos	Establecer si se desea que los usuarios tengan que aceptar una ley de protección de datos antes de registrar su perfil	-Mostrar -No mostrar
Video instrucciones	Video antes de la creación del perfil con las instrucciones	-Mostrar -No mostrar

Para la parte de **monitorización** continua se puede configurar:

Configuración	Descripción	Posibles valores
Fotos de monitorización	Guardar las fotos	-Todas -Solo las no positivas -Ninguna
Intervalo	Intervalo de tiempo en el cual se va a tomar una foto aleatoria en segundos	-Valor numérico (30)
Permitir pasar fallos	En la pantalla previa al examen donde se validan los requisitos biométricos, permitir acceder al examen aunque el alumno no sea quien dice ser o no	-Permitir pasar -Repetir la foto
Texto a mostrar	En la pantalla previa al examen donde se validan los requisitos biométricos, mostrar un texto informativo (útil para dar pautas al alumno antes de realizar un examen)	-Texto -No mostrar nada

El cliente en el servicio **KEYidentity** no puede realizar ninguna configuración para la monitorización continua. Para la parte de la **pantalla de registro** puede realizar la siguiente configuración:

Configuración	Descripción	Posibles valores
Permitir omitir	Permitir saltar el registro	-Si -No
Personalización de las preguntas	Permite personalizar las 7 preguntas que se realizan al usuario para crear su perfil.	-Por defecto -Personalizadas

Alertas

El servicio FACEidentity dispone de un sistema de alertas por correo electrónico. Este sistema de alertas, se puede configurar para enviar un correo electrónico en el caso de que se detecte una suplantación de identidad. Cuando el servicio detecte una suplantación, enviará un correo electrónico adjuntando un pdf similar al siguiente.

INFORME DE INCIDENCIA

Cliente:

adr formación Soluciones eLearning

Se ha producido una incidencia en uno de los perfiles registrados en el **Proyecto ADR Formación devel**

Fecha / Hora incidencia:
11-10-2019 / 14:55:08

Perfil incidentado:
ID usuario 105
Daniel Ibañez Del Campo

ESTADO DEL PERFIL: Verificado

Alerta:

14:55:08

Identificación incorrecta - Intento de suplantación

También se pueden configurar alertas para controlar el número de identificaciones que se han realizado en cada servicio. Si las identificaciones superan un determinado límite propuesto por el cliente, se enviaría un correo avisando al administrador de que se ha superado el límite. Estos correos son meramente informativos.

Política de seguridad de servicios biométricos.

Tecnología

Toda la tecnología utilizada en el proyecto está alojada en el cloud de Amazon Web Services.

El servicio en producción está alojado en AWS Irlanda y el plan de contingencia en AWS París.

Identificación de accesos al sistema

Autenticación por doble factor

Se ha establecido con carácter obligatorio la autenticación por doble factor para el acceso del cliente a los servicios de identificación biométrica. Cada cliente, aparte de disponer de unas claves únicas, tendrá que superar el reconocimiento facial para poder acceder al panel de administrador. Si no supera dicha autenticación, el equipo de administradores de ADR recibe un correo alertando del intento de suplantación para poder tomar las medidas oportunas.

Dentro de ADR Formación, únicamente tienen acceso a dicho panel el equipo de administradores y solamente es utilizado para comprobar su correcto funcionamiento.

Logs de accesos al sistema

Se guardan los logs de acceso al sistema durante un año. Estos logs se pueden analizar posteriormente si se ha detectado alguna irregularidad. En estos logs, se pueden filtrar los accesos de usuarios de clientes gracias a que cada uno de ellos accede a través de un dominio diferente.

Los usuarios acceden a través de los dominios: faceidentity.adrformacion.com y keyidentity.adrformacion.com
Los clientes en el acceso de administrador entran al dominio identify.adrformacion.com

Con estos logs, podemos realizar técnicas de análisis forense gracias a AWS Athena, un servicio de consultas interactivo que facilita el análisis de datos y permite verificar la legitimidad de los accesos.

Almacenamiento de datos

FACEidentity

Para procesar las imágenes utilizamos el servicio AWS Rekognition. Para cada rostro detectado, Amazon Rekognition extrae los rasgos faciales y almacena la información de rasgos en una base de datos. Además, almacena los metadatos de cada uno de los rostros detectados en la colección de rostros especificada. Amazon Rekognition no conserva los bytes de las imágenes reales.

Borrado automático de datos

Si el cliente lo desea para su posterior análisis, puede guardar las imágenes, y para este caso, se ha programado un esquema para cada cliente en el que se pueden configurar los periodos de almacenamiento máximo para los diferentes tipos de imagen en cada configuración del servicio (identificación o monitorización). Transcurrido ese periodo de días, las imágenes son eliminadas definitivamente.

ASIGNAR BORRADOFOTOS

Cliente	ADR Formación			
Identificación		Monitorización		
Positivas	15 días	Positivas	15	días
Incertidumbre	90 días	Incertidumbre	90	días
Negativas	90 días	Negativas	90	días
Gesto incorrecto	90 días	Foto no válida	90	días
Foto no válida	90 días			

KEYidentity

En el reconocimiento mediante patrones de tecleo, solamente guardamos los tiempos medios que tarda cada usuario en pulsar cada tecla. A KEYidentity en ningún caso llega el contenido que el usuario ha escrito.

Política de backups

Se realizan copias de seguridad de los diferentes elementos del sistema:

Base de datos
Los datos están almacenados en el el servicio AWS RDS del que se realizan copias diarias que se almacenan durante 35 días.

Servidor.
El servidor cuenta con 2 discos para los cuales se realizan las siguientes copias de seguridad:

- Diariamente se copian los discos y se mantienen las copias durante 7 días.
- Semanalmente se copian los discos y se mantienen las copias durante 8 semanas.
- Mensualmente se copian los discos y se mantienen las copias durante 12 meses.

Archivos de datos del sistema
Los archivos de imágenes del sistema se almacenan en un bucket s3 (identifyservice). En este bucket se ha habilitado el control de versiones para 365 días, de forma que se puede recuperar los archivos en el estado que estuvieran, antes de cualquier modificación o eliminación realizada dentro de esos 365 días.

Plan de recuperación ante desastres

Se define en la región de AWS París en otra cuenta de Amazon.

Base de datos
Se realiza una copia de la base de datos diaria que se almacena durante 7 días.

Servidor.
De los 2 discos del servidor se realiza una copia de seguridad diaria que se almacena durante 7 días

Archivos de datos del sistema
Los archivos de datos del sistema se replican a un bucket s3 (identifyparisservice) en esta cuenta.

Sistemas de seguridad

Disponemos de varias herramientas para la detección de intrusos y protección antimalware.

CLAMAV
Es un antivirus que nos permite detectas troyanos, virus, malware y otras amenazas maliciosas.

WAF
Es un firewall para aplicaciones web que nos ayuda a protegernos contra ataques web comunes que pueden afectar a la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. AWS WAF brinda control sobre cómo el tráfico llega a nuestras aplicaciones permitiéndonos crear reglas de seguridad que bloquean los patrones de ataque comunes, como la inyección de SQL o las secuencias de comandos entre sitios, y las reglas que filtran patrones de tráfico específicos que defina.

Cloudwatch con alarmas de umbrales definidas
Es un servicio de monitorización y observación que ofrece datos e información procesable para monitorizar nuestra aplicación. Gracias a las alarmas definidas, podemos saber si hay cambios de rendimiento que puedan afectar al sistema.

Transmisión de datos

Utilizamos el cifrado https entre cliente y servidor para que todas las transferencias de datos sean seguras. Al cifrar la conexión entre cliente y servidor evitamos ataques, como *man in the middle* o *eavesdropping* que nos podrían robar los datos. Para ello, tenemos configurado un certificado emitido por Amazon.

ANEXO II: ACUERDO DE CONFIDENCIALIDAD FIRMADO POR LOS EMPLEADOS

El abajo firmante, en el marco de la relación laboral que le une con IMF INTERNATIONAL BUSINESS SCHOOL S.L., puede tener acceso a recursos donde se contiene información relativa a datos de carácter personal de personas físicas, en su virtud se compromete a:

1. No revelar a persona alguna ajena a IMF INTERNATIONAL BUSINESS SCHOOL S.L., sin su consentimiento, cualquier información a información (entendiéndose por tal toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada) referente a la que haya tenido acceso en el desempeño de sus funciones en IMF INTERNATIONAL BUSINESS SCHOOL S.L., excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o de la entidad impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

2. Utilizar la información a que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en IMF INTERNATIONAL BUSINESS SCHOOL S.L., y no disponer de ella de ninguna otra forma o con otra finalidad. Mantener en el más estricto secreto toda la información que pueda llegar a su conocimiento como consecuencia de su profesión y del desempeño de sus funciones dentro de IMF INTERNATIONAL BUSINESS SCHOOL S.L., comprometiéndose a no divulgarla, publicarla, cederla, revelarla ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de IMF INTERNATIONAL BUSINESS SCHOOL S.L. que no estén autorizados a acceder a la citada información, cualquiera que sea el soporte en el que se encuentre la información.

3. Acceder a la información contenida tanto en los sistemas informáticos como en cualquier otro soporte, en papel, electrónico o telemático, sólo si tal acceso fuera necesario para la prestación de los servicios. No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de trabajador de IMF INTERNATIONAL BUSINESS SCHOOL S.L., y que no sea necesaria para el desempeño de sus funciones en la misma.

4. Cumplir, en el desarrollo de sus funciones en IMF INTERNATIONAL BUSINESS SCHOOL S.L., la normativa vigente, nacional y comunitaria, relativa a la protección de datos de carácter personal y, en particular, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de

estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos – RGPD) y disposiciones complementarias o cualquier otra norma que las sustituya en el futuro, estando obligado por ello al deber de secreto en virtud del artículo 5.1 f) de la citada normativa.

5. Devolver a IMF INTERNATIONAL BUSINESS SCHOOL S.L. todas las copias o documentos, independientemente del soporte en el que se encuentren, relativa a la información a la que haya tenido acceso como consecuencia de los servicios prestados sin necesidad de requerimiento.

6. Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con IMF INTERNATIONAL BUSINESS SCHOOL S.L.

7. El acceso a los recursos puestos a disposición del trabajador por parte de IMF INTERNATIONAL BUSINESS SCHOOL S.L., tales como teléfono móvil, PDA, portátil, Internet, teléfono, fax, correo electrónico, fotocopiadora, o escáner se considerará como un privilegio que está condicionado a la aceptación de este Compromiso. La anterior enumeración se hace sin carácter limitativo y se hará extensiva a cualquier otro recurso que la empresa ponga en disposición del trabajador, de forma que éste autoriza a que IMF INTERNATIONAL BUSINESS SCHOOL S.L., efectúe los controles necesarios para verificar el correcto desarrollo de sus obligaciones laborales por los medios técnicos oportunos, incluyendo la monitorización de los sistemas de información. El trabajador, por su parte, se compromete a efectuar un uso adecuado a sus obligaciones laborales y el tratamiento que, por el puesto a desarrollar, deba efectuarse, en la medida en que la calidad de los servicios prestados por IMF INTERNATIONAL BUSINESS SCHOOL S.L. depende en su mayor parte de la responsabilidad individual de los usuarios.

8.- Sin perjuicio de que se apliquen obligaciones similares a todos los recursos de la empresa, en relación con el correo electrónico, el trabajador es el único responsable de las actividades realizadas con el buzón de correo (o buzones) de los que le haya provisto IMF INTERNATIONAL BUSINESS SCHOOL S.L. El servicio de correo debe ser destinado únicamente a un uso laboral aunque excepcionalmente podría ser utilizado para fines personales siempre que no afecten al rendimiento del servicio en perjuicio de la empresa y las ocasiones sean puntuales. No se debe permitir el uso de la cuenta a personas no autorizadas y no se podrán instalar cuentas de correo de proveedores externos en los sistemas de información de IMF INTERNATIONAL BUSINESS SCHOOL S.L. En los envíos masivos de información, se utilizará el campo de copia oculta (CCo), especialmente si se trata de envíos comerciales o cualquier otra situación en la cual las direcciones de correo electrónicas de personas o empresas distintas pudieran quedar visiblemente expuestas el resto de destinatarios. En los casos en los que un correo electrónico resultara sospechoso de contener un virus, no se abrirá y se consultará con los responsables de los sistemas de información. En general, se prohíbe el uso del correo con intereses ajenos a los de IMF INTERNATIONAL BUSINESS SCHOOL S.L., así como participar en cadenas de e-mails, difundir contenidos ilegales (tales como piratería, pornografía, virus, fraudes, entre otros) o enviar mensajes que comprometan la reputación de IMF INTERNATIONAL BUSINESS SCHOOL S.L. a foros, blogs u otras listas de distribución.

9.- En relación con el uso de la red de Internet, el trabajador es el único responsable de las sesiones iniciadas en Internet desde su puesto de trabajo, siendo considerado su uso como estrictamente laboral, estando prohibido con fines distintos. En concreto no se podrán modificar las configuraciones de los navegadores del equipo ni la activación de servidores o puertos sin autorización de los responsables de los sistemas de información. No se podrán utilizar imágenes, sonido o videos para fines ajenos a la actividad laboral de la empresa, debido a que el tamaño de estos archivos satura los canales de comunicación y disminuye la velocidad de transmisión perjudicando al funcionamiento de la red en su conjunto. Además, se prohíbe expresamente el acceso, la descarga y el almacenamiento en cualquier soporte, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres, así como el uso de canales de chat cualquier que sea su proveedor o páginas webs de juegos en línea o dispositivos similares. IMF INTERNATIONAL BUSINESS SCHOOL S.L. colaborará con en cualquier investigación contra este tipo de actos o cualquier otra utilización ilegal con las Fuerzas y Cuerpos de Seguridad del Estado así como con la Administración de Justicia.

La obligación general señalada anteriormente será complementaria con los deberes de secreto profesional que les apliquen.

El abajo firmante entiende que en este sentido asume una obligación laboral específica, y que en caso de incumplirla, dicho incumplimiento podrá ser motivo de despido por justa causa, generándose además a favor de IMF INTERNATIONAL BUSINESS SCHOOL S.L. una acción judicial por cualquier daño o perjuicio que pudiera derivarse para el mismo y/o a terceras personas derivado del incumplimiento de los compromisos anteriores.

Y para que surta plenos efectos, firmo la presente declaración.

En a de de 201_

EMPLEADO CARGO

D.N.I. FIRMA

COPIA PARA ADR FORMACIÓN

IMF Business School

Nº 01/17

Contrato de CAMPUS BUSINESS SCHOOL para creación, gestión e impartición de formación online

COMPARECEN

De una parte, **D. José Luis Del Rincón Ruiz** con D.N.I. **16557974-K**, representante legal de **ADR Infor S.L.** con C.I.F. nº **B-26265835** y domicilio social en **Avda. Vara de Rey 41 bis. 8º Of. 6 de Logroño, 26002 La Rioja, España** (en adelante, "**ADR Formación**").

De otra parte, **D. Carlos Martínez Domínguez** con D.N.I. **22144543-M** representante legal de **IMF Business School, S.L.** con C.I.F. nº **B83074146** y domicilio social en **C/ Bernardino Obregón, 25** (en adelante, "**el cliente**").

Ambas partes, ADR Formación y el cliente, están interesados en formalizar el presente CONTRATO, reconociéndose capacidad legal suficiente para hacerlo y aceptando los términos y condiciones establecidos en las siguientes

CLÁUSULAS

1ª.- OBJETO DEL CONTRATO

El siguiente contrato tiene por objeto regular las condiciones en las que el cliente solicita y ADR Formación presta el servicio de **CAMPUS BUSINESS SCHOOL:** que incluye portal web personalizado, alquiler de plataforma de teleformación, cesión de contenidos, tutorización por parte de ADR Formación si así se requiere y explotación del sistema de autor por parte del cliente, con las características descritas en el presente contrato, así como la determinación de las condiciones y forma de remuneración del cliente a ADR Formación por el servicio prestado.

2ª.- DESCRIPCIÓN DEL SERVICIO

2.1 Alquiler y administración de la plataforma

El servicio de **Alquiler de Plataforma ó LCMS (Learning and Content Mangement System)** se ajustará a las siguientes características:

a) ADR Formación desarrollará un portal web personalizado acorde con la imagen corporativa del cliente desde donde se accederá a la plataforma de teleformación.

b) La plataforma estará alojada en el cloud de AMAZON (Irlanda), por lo que el mantenimiento del sistema, copias de seguridad y actualizaciones de las herramientas del LCMS son competencia exclusiva de ADR Formación.

c) La plataforma estará operativa de forma ininterrumpida. Si se produjera una interrupción de servicio motivado por fallo del proveedor de cloud, ADR Formación propondrá soluciones alternativas en un plazo no superior a 48 horas.

d) El cliente dispondrá de las herramientas necesarias para la gestión de la plataforma. Se crearán los perfiles necesarios con las herramientas que el cliente precise.

e) El cliente dispondrá de formación en el uso y manejo del sistema para los distintos perfiles.

f) El aula virtual será configurada por ADR Formación, siendo sus solapas personalizables para cada acción formativa por el propio cliente.

g) El cliente podrá activar el motor de voz que la plataforma incorpora sin coste adicional.

h) El cliente podrá utilizar el entorno de comunicaciones integrado (solapa Llamadas) sin coste adicional.

i) El cliente podrá utilizar servicios de comunicaciones de terceros integrables en la plataforma (Adobe connect, Gootomeeting, Webex) cuyos costes de licencia no están incluidos en este contrato.

j) ADR Formación supervisará y asegurará la capacidad técnica del sistema. Para resolver incidencias el cliente dispone de la herramienta de **HELP DESK** en la plataforma, donde se recogerán los tickets de soporte oportunos. Estos tickets serán atendidos en un plazo inferior a 48h laborales por el equipo técnico de ADR Formación.

k) El cliente será responsable de la matriculación de alumnos a través de las diferentes herramientas disponibles para ello.

l) El cliente será responsable del seguimiento, coordinación y supervisión de las acciones formativas.

2.2 Cesión de contenidos de ADR Formación:

Se entiende por cesión de contenidos el uso por parte del cliente del contenido que ADR Formación pone a su disposición a través del LCMS. Este servicio tiene como características principales:

a) El cliente podrá disponer de los contenidos que ADR Formación presente a través de la herramienta CATÁLOGO de la plataforma.

b) Estos contenidos serán tutorizados por personal del cliente. No está permitida la impartición de formación del catálogo de ADR Formación sin tutor.

c) El cliente será responsable de mantener actualizado su catálogo de formación incluyendo las novedades o descatalogando la formación obsoleta a través de las herramientas facilitadas. ADR Formación le informará mediante correo electrónico de las modificaciones en los títulos e igualmente las herramientas de la plataforma no permitirán matriculaciones en formación descatalogada, siendo el cliente el responsable último de la vigencia de los contenidos ofertados desde su portal.

d) Todos los contenidos del catálogo de ADR Formación están registrados y en ningún caso la cesión de contenidos conlleva derecho alguno sobre su propiedad intelectual por parte del cliente.

e) ADR Formación se encargará de mantener actualizados los contenidos disponibles así como de renovar y ampliar la oferta de títulos.

2.3 Servicio de tutorización

El servicio de **tutorización** prestado por ADR Formación se ajustará a las siguientes características:

a) ADR Formación podrá tutorizar contenidos de su propio catálogo en el portal del cliente.

b) La tutorización correrá a cargo de un experto en la materia, con conocimientos suficientes y experiencia en tutoría online.

c) Será el propio cliente quien determine si precisa tutor de ADR Formación o dispone de personal propio para asumir la tutoría, mediante la matriculación de un tutor (propio o de ADR Formación) a través de las herramientas de la plataforma cuando realice la primera venta de cada acción formativa.

2.4 Sistema de Autor

ADR Formación pondrá a disposición del cliente el **Sistema de Autor** para la creación y gestión de contenidos:

a) El Sistema de Autor es un conjunto de herramientas del LCMS que permite la creación y publicación de contenidos online por parte del cliente.

b) Los contenidos generados por el cliente serán propiedad del cliente y registrados a su nombre o del autor. ADR Formación no será propietaria de contenidos desarrollados por sus clientes.

c) ADR Formación ofrece al cliente de forma gratuita cursos online tutorizados para que sus trabajadores puedan desarrollar contenidos adecuados y explotar todas las posibilidades que la plataforma ofrece.

d) Los contenidos del cliente serán tutorizados por personal del cliente. ADR Formación no contempla la tutorización para contenidos ajenos a su catálogo.

e) Los contenidos generados por el cliente sí pueden ser impartidos sin tutorización si el cliente así lo considera.

f) El cliente dispondrá de un espacio de almacenamiento para la realización de cursos propios, establecido en la cláusula 4ª IMPORTE Y CONDICIONES DE PAGO del presente contrato.

g) Los contenidos desarrollados por el cliente serán exportables en formato SCORM.

h) El cliente podrá disponer de herramientas de exportación, control y gestión de licencias SCORM de su propio contenido.

3ª - COMPATIBILIDAD DE LA PLATAFORMA CON CONTENIDOS DE TERCEROS

La plataforma de ADR Formación es compatible con contenidos SCORM. Esto significa que es capaz de interpretar un contenido SCORM y mostrarlo, así como registrar los datos que el contenido SCORM reporte.

4ª.- IMPORTE Y CONDICIONES DE PAGO

4.1 Condiciones

Como contraprestación de estos servicios, el cliente se compromete a abonar las siguientes cantidades en tiempo y forma establecidos:

Portal web y LCMS	Importe
Plataforma, precio anual, que incluye:	63.100 € (5.258 €/mes)

- Hasta 45.000 altas anuales
- Hosting de alta disponibilidad
- Mantenimiento del LCMS
- Campus Personalizado
- Aula Virtual
- Motor de voz
- Comunicación en tiempo real integrada
- Sistema de Autor
- Herramientas para itinerarios/másters
- Herramienta de exportación/Importación SCORM y control de licencias exportadas

Exceso matrículas anuales:	
• Hasta 50.000 altas	1,18 €/alta
• Hasta 60.000 altas	1,14 €/alta

Capacidad almacenamiento datos:	Exceso GB:
• Hasta 250 GB incluidos	1,10 €/GB/mes

Formación en el uso del sistema	Importe
Curso de iniciación al desarrollo de contenidos	Sin coste
Curso de especialista en desarrollo de contenidos	Sin coste
Curso de tutor online	Sin coste
Curso de supervisor/administrador	Sin coste

Equipo Técnico*	Importe
Las horas de soporte técnico irán a cargo de las Bolsas de horas contratadas. En caso de agotarlas y no adquirir nuevas bolsas, se facturarán al precio vigente:	Con cargo a bolsas de horas adquiridas
Horas de soporte (tarifa vigente 2017)	50 €/hora (en fracciones de 30min)

* Las horas del equipo técnico serán facturadas con cargo a las bolsas de horas adquiridas o bien según la tarifa vigente. En este concepto se tendrán en cuenta todas aquellas horas que el equipo de ADR Formación invierta en el desarrollo de trabajos para el cliente (a modo de ejemplo: formación en el uso del sistema más allá de la formación incluida, soporte a autores, supervisores o tutores en el uso de la plataforma, desarrollos de herramientas a medida, diseño). En ningún caso se cobrarán los trabajos derivados de un mal funcionamiento de la plataforma, mejoras que ADR Formación decida implementar, elaboración de presupuestos o atención comercial. En este sentido ADR Formación será totalmente transparente para que el cliente conozca en cada momento el concepto por el que es facturado y puede solicitar previamente un presupuesto o estimación de horas a consumir.

Cursos catálogo ADR Formación (Cesión de Contenidos)	Importe* (Descuento sobre precio tarifa)	
Cesión de contenidos: (cursos ADR con tutor del cliente):	Los primeros 5.000€	70% dto
Se aplicará el tramo de descuento correspondiente en función de la facturación anual acumulada.	Desde 5.001 a 10.000€	75% dto
	Desde 10.001 a 30.000€	80% dto
Los tramos no son retroactivos.	A partir 30.001€	85% dto

*Importe por matrícula para volumen total de consumos anuales.

El precio tarifa será el precio de referencia publicado en la web www.adrformacion.com para los cursos (modalidad con tutor). El precio final (descuentos aplicados) será visible por el cliente desde sus herramientas de la plataforma. ADR Formación se reserva el derecho de modificar sus tarifas sin previo aviso.

La aplicación de los descuentos se realizará en base a las siguientes condiciones:

- Se asigna un descuento inicial del 70 % de descuento sobre el precio tarifa.
- Se computará mensualmente la facturación acumulada en el año natural.

- Cuando dicha facturación acumulada alcance o sobrepase los límites establecidos en los distintos tramos, desde el mes siguiente se aplicará el nuevo descuento indicado en el tramo correspondiente.
- Al iniciarse un nuevo año natural se aplicará como punto de partida, el descuento correspondiente tras acumular la facturación de todo el año natural precedente.

Certificados de Profesionalidad catálogo ADR Formación	Importe
Cesión de contenidos de Certificados de Profesionalidad	0,75 €/h

Cursos catálogo ADR Formación (Tutores ADR Formación)		Importe* (Descuento sobre precio tarifa)
Tutoría y dinamización de los expertos de ADR Formación	1os 10.000€	40% dto
Se aplicará el tramo de descuento correspondiente en función de la facturación anual acumulada.	Desde 10.000 a 30.000€	45% dto
	A partir 30.000€	50% dto
Los tramos no son retroactivos.		

La aplicación de los descuentos se realizará de la siguiente forma:

- Se asigna un descuento inicial del 40 % de descuento sobre el precio tarifa.
- Se irá computando mensualmente la facturación acumulada en el año natural.
- Cuando dicha facturación acumulada alcance o sobrepase los límites establecidos en los distintos tramos, desde el mes siguiente se aplicará el nuevo descuento indicado en el tramo correspondiente.
- Al iniciarse un nuevo año natural se aplicará el descuento correspondiente tras acumular la facturación de todo el año natural precedente

Consumo SMS	Importe/sms
En caso de activar el servicio, se facturarán los sms enviados. En ningún caso se facturan los sms enviados a los tutores de ADR Formación	0,15 €/sms

Servicios adicionales	Importe
Portal web estándar adicional	950 €
Skin de acceso a portal existente personalizada	300 €

4.2 Sistema de facturación automático

La facturación se realizará con una periodicidad mensual. Todos los servicios facturados están sujetos al Impuesto sobre el Valor Añadido al tipo vigente en cada momento, salvo el servicio de Tutorización que está exento de IVA en virtud del artículo 20.UNO.9º de la Ley 37/92 de IVA.

La plataforma de ADR Formación incorpora un **sistema de facturación** mediante el que el cliente podrá comprobar en tiempo real los datos provisionales de las facturas del mes en curso, así como acceder a los datos de las facturas de meses anteriores. El cliente **da su conformidad mediante la firma de este contrato para no recibir la factura en formato papel y muestra su compromiso a imprimirla desde la herramienta "Facturación" de la plataforma.**

Las facturas serán abonadas **mediante transferencia bancaria**. El cliente se compromete a descargar las facturas emitidas y realizar el abono mediante **transferencia bancaria a 30 días fecha factura, siendo los 5 y 20 los días de pago establecido.**

DATOS PARA EL ABONO DE LAS FACTURAS:

Titular de la cuenta: ADR INFOR, S.L.

Entidad bancaria: BANKIA

Nº Cuenta: ES33 2038 7490 1160 0001 6875

ADR Formación comunicará al cliente cualquier cambio en los datos facilitados para el pago con al menos una semana de antelación. El cliente se compromete a realizar los pagos en el tiempo y forma establecidos, sin demoras ni excepción.

5ª.- DURACIÓN DEL CONTRATO Y RESOLUCIÓN CONTRACTUAL

5.1 Duración del contrato

El presente contrato entra en vigor el día 01/01/2017 y tiene validez 31/12/2017, renovándose tácitamente por periodos anuales (año natural), si ninguna de las partes expresa su deseo de terminación con al menos un mes de antelación.

En la fecha de entrada en vigor del contrato se pone a disposición del cliente la plataforma e-learning.

5.2 RESOLUCIÓN CONTRACTUAL

Son causas de resolución del presente contrato las siguientes:

a) El transcurso del plazo de duración del contrato en los términos previstos en la Cláusula 5.1. anterior.

b) El mutuo acuerdo de las partes.

c) El incumplimiento por ADR Formación de las obligaciones asumidas en relación con la prestación de servicios objeto del presente contrato de acuerdo con lo dispuesto en la Cláusula 2ª anterior.

d) El incumplimiento por el cliente de las obligaciones de pago asumidas en virtud del presente contrato de acuerdo con lo establecido en la Cláusula 4ª.

e) El uso malicioso por el cliente de las herramientas puestas a su disposición en virtud del presente contrato, o la realización por el cliente de prácticas malintencionadas que pudieran repercutir en la seguridad del sistema.

f) La realización por el cliente de prácticas de competencia desleal con los clientes de ADR Formación.

Cada una de las partes responderá frente a la otra por los daños y perjuicios causados como consecuencia del incumplimiento de sus obligaciones asumidas en virtud del presente contrato.

En caso de resolución del contrato por las causas señaladas en los apartados a), b) y c) anteriores, ADR Formación se compromete a ejecutar el **Plan de Continuidad de Negocio** en la modalidad denominada "**transferencia ordenada**" que se especifica en el Anexo I del presente contrato.

6ª.- PROPIEDAD INTELECTUAL E INDUSTRIAL

El cliente reconoce los derechos de propiedad intelectual y, en su caso, industrial, de ADR Formación sobre el resultado de sus labores de análisis, programación, reparación, formación y adaptación del portal web de teleformación desarrollado: los entornos de formación, aula virtual, campus y herramientas que conforman el LCMS.

7ª.- CONFIDENCIALIDAD Y POLÍTICA DE PROTECCIÓN DE DATOS

Tanto ADR Formación como el cliente se comprometen a no divulgar la información confidencial referente a la otra parte de la que hayan tenido conocimiento por razón de la ejecución del presente contrato y a mantenerla en secreto, incluso después de la finalización del mismo.

En cumplimiento del artículo 12.2 de la Ley Orgánica 15/99 de Protección de Datos Personales (LOPD) ADR Formación tratará toda información propiedad del cliente de forma estrictamente confidencial, tomando las medidas necesarias para que su contenido no se divulgue a terceros, ni éstos puedan tener acceso a los mismos sin autorización expresa del cliente, garantizando expresamente el cumplimiento del deber de secreto (Art. 10 LOPD) en relación con los asuntos y datos del cliente, ADR Formación tratará los datos facilitados por el cliente de conformidad con las finalidades y los usos previstos en el presente contrato y se obliga a no utilizarlos para un fin distinto, salvo cuando así le sea indicado por el cliente.

ADR Formación se obliga igualmente a no comunicar los datos de carácter personal facilitados por el cliente ni siquiera para su conservación, a otras personas distintas de las que son parte en el presente Contrato, salvo que sea requerido a ello por una autoridad competente.

Una vez finalizada la relación entre ambas partes, ADR Formación devolverá o destruirá, a indicación del cliente, todos los datos de carácter personal al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del servicio establecido en este contrato.

ADR Formación declara tener implantadas las medidas de seguridad que son requeridas por la vigente legislación de protección de datos, en concreto las establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, donde se recogen las Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. Asimismo, en lo relativo a los datos facilitados para el cumplimiento de las actividades objeto del presente contrato ADR Formación aplicará las medidas correspondientes al nivel básico, las cuales se encuentran recogidas en un documento de seguridad debidamente actualizado.

8ª.- CARÁCTER MERCANTIL DE LA RELACIÓN CONTRACTUAL

El presente contrato tiene carácter mercantil, no existiendo vínculo laboral alguno entre el cliente y el personal de ADR Formación que pueda prestar sus servicios para el cliente en cumplimiento del presente contrato.

9ª.- LEGISLACIÓN APLICABLE Y TRIBUNALES COMPETENTES

Ambas partes se comprometen a resolver, de manera amistosa, cualquier desacuerdo que pueda surgir en la interpretación o ejecución de este contrato. En caso contrario será de aplicación la legislación española y ambas partes se someterán a los Juzgados y Tribunales de la Ciudad de Logroño con renuncia a su propio fuero, si éste fuese otro.

Ambas partes aceptan los términos y las condiciones expuestos en el presente contrato, y para que así conste firman a 01/01/2017

Fdo.: D. José Luis Del Rincón Ruiz
Cargo: Representante Legal

adr formación
Soluciones eLearning
ADR INFOR, S.L. CIF: B-26265835
Vara de Rey, nº41 Bis - 1º, Oficina 6
26002 Logroño, La Rioja
Tel.: 941 250 116 - adr@adrformacion.com

ADR INFOR, S.L.

Fdo.: Carlos Martínez Domínguez
Cargo: Representante Legal

IMF

IMF International Business School S.L.

Anexo I. Plan de continuidad de negocio

ADR Formación como proveedor de tecnología es consciente de la importancia que tiene el servicio que ofrece en los modelos de negocio de sus clientes. Con el objeto de minimizar los posibles inconvenientes que pudieran surgir del hecho de dejar de utilizar la tecnología de ADR Formación se redacta el siguiente plan de continuidad de negocio.

En atención a las circunstancias que concurran en el momento de resolución contractual por las causas señaladas en los apartados a), b) y c) de la Cláusula 5ª anterior, se aplicará el proceso denominado **"transferencia ordenada"**.

Transferencia ordenada

Por transferencia ordenada se entiende el proceso por el cual el cliente puede migrar su negocio de la mejor manera posible de la plataforma de teleformación de ADR Formación a otra plataforma de teleformación.

En caso de resolución contractual por las causas señaladas en los apartados a), b) y c) de la Cláusula 5ª anterior, el presente contrato se entenderá prorrogado en las condiciones económicas vigentes en el momento de resolución contractual por el periodo necesario para extinguir las acciones formativas activas, con un periodo máximo de 2 años a contar desde la fecha de resolución que deberá ser notificada al cliente.

El cliente no podrá iniciar nuevas acciones formativas durante el período de transferencia ordenada.

Durante el período de prórroga citado, ADR Formación continuará prestando los servicios pactados con el fin de facilitar la migración a realizar por el cliente.

En caso de que la migración vaya a implicar la prestación de servicios no contenidos en el contrato, deberán pactarse expresamente estos servicios.

Infraestructura propia

En caso de que ADR Formación no pueda continuar prestando sus servicios a IMF por causas de fuerza mayor o por cualquier otra circunstancia que haga imposible que el actual equipo gestor pierda la capacidad de explotar la plataforma, ADR Formación podrá segregar la plataforma actual del cliente, con todos los contenidos del cliente, alumnos y personalizaciones, generando una instancia de la misma en una infraestructura gemela e independiente en AMAZON.

El proceso de segregación se realizará en un plazo máximo de 15 días hábiles y tendrá un coste de 6.000 €.

A partir de la fecha de entrega de la infraestructura propia el cliente se hará cargo de los costes de hosting (AMAZON) así como de la gestión de la plataforma de teleformación.

El cliente adquiere una licencia de uso y modificación de la plataforma, por un plazo mínimo de 20 años, cuyo coste es de 189.300 €, en un pago único.

El cliente podrá actuar sobre la plataforma de teleformación adaptándola a sus necesidades y para su uso exclusivo, no pudiendo comercializar la plataforma a terceros.

COMPROMISO DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ENTRE RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

En Madrid, a 8 de enero de 2019

REUNIDOS

De una Parte,

IMF International Business School S.L. (en adelante, el "cliente" o "Responsable del Tratamiento"), con domicilio en C/ Bernardino Obregón, 25 Madrid y provista de CIF: B83074146 representada en este acto por D. Carlos Martínez Domínguez titular del D.N.I. 22144543M, actuando en su calidad de Representante.

Y de otra,

ADR Infor S.L. (en adelante, "Proveedor" o el "Encargado del Tratamiento"), con domicilio en Avda. Vara de Rey 41 bis.8º Of.6 de Logroño, 26002 La Rioja y provista de CIF: B86344108 representada en este acto por D. José Luis del Rincón Ruiz titular del D.N.I. 16557974K, actuando en su calidad de Representante.

A los efectos del presente documento, el Responsable del Tratamiento y el Encargado del Tratamiento podrán ser designados conjuntamente como las "Partes", e individual e indistintamente como la "Parte".

Ambas Partes, reconociéndose mutuamente capacidad legal suficiente para contratar y obligarse mediante este documento, y manifestando los comparecientes tener vigentes sus poderes y ser suficientes para obligar a sus representadas, y a tal efecto,

MANIFIESTAN

I. Que las Partes suscribieron en fecha de 1 de enero de 2017 un Contrato de CAMPUS BUSINESS SCHOOL para Creación, Gestión e Impartición de formación online (en adelante, el "Contrato") el cual sigue vigente. En virtud de este, el Responsable del Tratamiento encargó determinados servicios al Encargado del Tratamiento.

II. Que, las Partes están interesadas en realizar una novación modificativa no extintiva del Contrato, a los efectos de adaptar el mismo a las obligaciones regulatorias relativas a la protección de datos de carácter personal derivadas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

III. Que, expuesto cuanto antecede, las Partes, de mutuo acuerdo, libre y espontáneamente, convienen en suscribir la presente Adenda modificativa y no extintiva al Contrato (en adelante, la "Adenda"), y ello, de conformidad con los siguientes:

CLÁUSULAS

PRIMERA.- NOVACIÓN MODIFICATIVA NO EXTINTIVA DEL CONTRATO

Las Partes expresamente acuerdan sustituir en su totalidad la Cláusula 7ª "Confidencialidad y Política de protección de datos" del Contrato, e incorporar el anexo correspondiente, quedando éstos redactados del tenor literal que sigue:

1.1. Objeto

Mediante las presentes cláusulas se habilita a la entidad encargada del tratamiento, para tratar por cuenta del responsable del tratamiento, los datos de carácter personal necesarios para prestar los servicios objeto del contrato, así como para la integración de sistemas de identificación biométrica y desarrollo de módulo de exámenes.

1.2. Duración

El presente acuerdo tiene la misma duración que el Contrato de Servicios profesionales al que acompaña.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

1.3. Titularidad de los datos

El tratamiento de datos automatizados o no de carácter personal será responsabilidad del CLIENTE, quien mantendrá dicha titularidad en todo momento, con las modificaciones que sufran como consecuencia de sus actualizaciones, altas, bajas y modificaciones.

Así, en todo momento EL CLIENTE conservará el derecho exclusivo de propiedad y uso de los datos y todos sus procesos de actualización.

1.4. Tratamiento de los datos.

4.1 EL PROVEEDOR, en el tratamiento de datos de carácter personal del CLIENTE, podrá tratarlos en las propias instalaciones de éste o bien fuera de ellas, y lo hará de conformidad con las finalidades y los usos previstos en el presente Contrato, de forma que accederá únicamente a aquellos datos que EL CLIENTE le proporcione y procederá a su tratamiento de acuerdo con las instrucciones proporcionadas por el mismo, no constituyendo, en ningún caso, dicho acceso una comunicación de datos.

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento, pone a disposición del encargado del tratamiento, la información que se describe a continuación:

a) **Tipos de datos personales objeto de tratamiento:**

- Datos Identificativos: Nombre y apellidos, imagen/voz.
- Datos biométricos relativos al reconocimiento facial y dinámica del tecleo.

b) Colectivos o categorías de interesados:

- ☐ Clientes y usuarios (alumnos)
- ☐ Empleados

SEGUNDA.- OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, únicamente para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La seudonimización y el cifrado de datos personales.
b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 15 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección datos@imf-formacion.com.La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la

solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información. Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de correo electrónico, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2.- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
3.- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
4.- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad siguientes:

1.- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2.- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
3.- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4.- Seudonimizar y cifrar los datos personales, en su caso.

No obstante lo anterior, el Proveedor garantiza que cuenta con los controles de seguridad especificados en la política de seguridad de servicios biométricos, detallada en el Esquema Funcional de los Servicios Biométricos, y que se adjunta como Anexo I al presente contrato.

TERCERA.- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

1. El Responsable deberá entregar al Encargado los datos a los que hace referencia la cláusula primera del presente contrato, que contienen la información necesaria para llevar a cabo las tareas encomendadas en el contrato suscrito. Si los datos anteriores sufriesen alguna variación, deberá comunicárselo al Encargado, para que aquél pueda actualizarlos.

2. Asimismo deberá aplicar las medidas técnicas y organizativas para garantizar y demostrar que el tratamiento de datos es conforme a la normativa de protección de datos.

3. Atender los ejercicios de derechos establecidos en la normativa vigente de protección de datos de carácter personal aunque dicho ejercicio se dirija ante el Encargado de tratamiento.

4. Igualmente, deberá velar, durante todo el tratamiento, por el cumplimiento de la normativa en materia de protección de datos por parte del Encargado por el cumplimiento del RGPD y la ley 3/2018 LOPDGDD

CUARTA.- RESPONSABILIDAD

1. En el caso de que EL PROVEEDOR en su calidad de encargado de tratamiento, destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

2.Ninguna de las partes asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud del presente Contrato si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor o caso fortuito admitido como tal por la Jurisprudencia, en particular: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico o cualquier otra medida excepcional adoptada por las autoridades administrativas o gubernamentales.

QUINTA.- CONFIDENCIALIDAD

1. EL PROVEEDOR garantiza que mantendrá la más estricta confidencialidad y expreso cumplimiento del deber de secreto profesional, en relación con los asuntos de EL CLIENTE durante la vigencia de este Contrato y después de su terminación.

2. EL PROVEEDOR durante y con posterioridad a la vigencia de este Contrato tratará toda información propiedad de EL CLIENTE de forma estrictamente confidencial, tomando las medidas necesarias para que su contenido no se divulgue a terceros, bien directamente, bien a través de terceras personas o empresas, ni estos puedan tener acceso a los mismos sin autorización expresa de EL CLIENTE.

3. A los efectos del presente Contrato, tendrá la consideración de información confidencial toda aquella susceptible de ser revelada por palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en un futuro, ya sea

intercambiada como consecuencia de esta relación contractual, conocida antes de la misma o que una parte señale o designe como confidencial a la otra.

4. Las obligaciones de confidencialidad establecidas en el presente contrato estarán en vigor mientras dure la relación entre las partes objeto del presente contrato, así como una vez extinguida la relación contractual por cualquier causa entre EL CLIENTE y EL PROVEEDOR.

Fdo. José Luis del Rincón Ruiz

Fdo. Carlos Martínez Domínguez

En muestra de aceptación y conformidad con todos y cada una de las cláusulas estipuladas, obligándose al cumplimiento de todo lo acordado, lo firman por duplicado en cada una de sus hojas en el lugar y fecha del encabezamiento de la presente adenda.

IMF Business School

TITULOS PROPIOS

Enseñanzas que no conducen a la obtención de un título con valor oficial

Modalidad Online

IMF INTERNATIONAL BUSINESS SCHOOL, S.L., B83074146. C/ Bernardino Obregón 25, 28012 Madrid, España

Datos del alumno

Apellidos: _____ Nombre: _____

Dirección: _____ Cód Postal: _____

Población: _____ Provincia: _____ País: _____

NIF: _____ Teléfono: + ____ / _____ Móvil: _____ F. Nacimiento: _____

Email: (Rellenar en mayusculas) _____ Nick de Twitter: _____

Estudios

☐ Licenciatura / Ingeniería Superior ☐ Diplomatura / Ingeniería Técnica ☐ Grado ☐ Otras titulaciones

Especificar: _____

Situación Laboral

☐ Emp. Pública ☐ Emp. Privada ☐ Autónomo ☐ Desempleado Nº de la Seguridad Social _____

Datos de la empresa (Por favor rellenar si estás en activo)

Razón Social: _____

Dirección: _____ C.I.F.: _____

Localidad: _____ C.P.: _____ Provincia: _____ Teléfono: + ____ / _____

Plantilla media: _____ Email: (Rellenar en mayusculas): _____

Cargo y/o Departamento: _____ Sector de la actividad: _____

Persona de contacto: _____ Cargo de la persona de contacto: _____

Nombre del Curso

Nombre del curso: _____

Modalidad Online Servicio Plus: ☐ Sí ☐ No

Dirección de envío del material de estudio: (Servicio Plus) ☐ Domicilio particular ☐ Domicilio empresa ☐ Otro

Entrega: ☐ Mañana ☐ Tarde

Rellenar si la dirección es distinta a la arriba indicada

Nombre y Apellidos o Razón Social _____

Dirección _____

Población _____ C.P.: _____ Provincia _____

Precio y Forma de pago

Facturar a: ☐ Datos personales ☐ Empresa Precio total del curso _____ €

☐ Precio pago contado ☐ Precio pago fraccionado Primer pago de _____ € y ____ mensualidades de _____ €

Forma de Primer Pago o Pago Total:

☐ Efectivo ☐ Ingreso en Cuenta

☐ Transferencia Bancaria ☐ Tarjeta

Desde España:
La Caixa: ES85 2100 5641 0502 0000 9142 - CAIXESBBXXX
Bankia: ES58 2038 4132 9860 0006 6669 - CAHMESMM
Banco Sabadell: ES93 0081 5246 8600 0122 6528 - BSABESBB
Desde el extranjero:
Banco Sabadell: ES93 0081 5246 8600 0122 6528 - BSABESBB

Domiciliación bancaria:

Mediante la firma de esta orden de domiciliación, el alumno autoriza a IMF a enviar instrucciones a la entidad del alumno, para adeudar su cuenta, y a la entidad para efectuar con adeudos en su cuenta siguiendo las instrucciones de IMF.

Nº de recibos _____

Importe: _____ €

IBAN ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

BIC ☐☐☐☐☐☐☐☐☐☐☐

Titular de la cuenta _____

Firma del titular de la cuenta

El alumno acepta el presente contrato que constituye, junto con las condiciones generales especificadas en el anexo, el contrato de inscripción del cual el alumno recibe un ejemplar firmado.

Firma y sello de IMF

En _____, a ____ de _____ de _____

Firma del Alumno

IMF INTERNATIONAL BUSINESS SCHOOL S.L. (en adelante IMF) es un centro privado de estudios de postgrado que imparte formación online, presencial y semipresencial.

Una vez informado el alumno de todas las cuestiones de su interés, IMF y el ALUMNO acuerdan la formalización del presente contrato de enseñanza, obligándose a su cumplimiento ambas partes, conforme a las siguientes cláusulas:

- **Metodología de formación:**

- La formación que se concierta es online a través de una plataforma e-learning en la que el alumno dispondrá del material de estudio, realizará ejercicios y recibirá la tutorización adecuada al programa formativo que contrata.

- En los programas con la opción de contratación del servicio plus, el alumno contará con la posibilidad de estudio del contenido teórico en versión papel. Este material formativo será enviado, una vez confirmado el pago inicial correspondiente a la formalización de la inscripción en la mayor brevedad posible, siendo el plazo normal de envío de veinte días naturales. En el hipotético caso de que se produjera cualquier retraso en la entrega del material, IMF se pondrá en contacto con el alumno para informarle de la nueva fecha de envío.

- El material de estudio que se facilita al alumno inscrito, corresponde a la versión actualizada y vigente del curso a impartir, no teniendo el alumno derecho alguno a versiones posteriores del contenido.

- **Alumnos de otros países:**

- El alumno es el único responsable de todas las gestiones necesarias para trasladarse al lugar de impartición. IMF no se responsabiliza de ningún trámite burocrático encaminado al traslado, obtención de visados, requisitos legales etc. siendo el alumno quien lo debe gestionar y tramitar por su propia cuenta. Al ser responsabilidad directa del alumno, IMF informa de que en ningún caso, serán motivo de baja del programa en el que el alumno se matrícula, ni de devolución de los importes efectivamente abonados.

- **Régimen Interno:**

- Con la firma de este documento el Alumno reconoce que ha recibido, ha leído y entendido el reglamento interno de la organización, pudiendo ser apercibido, sancionado y/o expulsado todo aquel alumno que no cumpla con dicho reglamento, en función de la gravedad del incumplimiento.

- **Expedición de Títulos:**

- La emisión de los títulos estará sujeta a la superación de la evaluación programada para la formación, al cumplimiento íntegro del valor del curso (total o fraccionado) y al pago de la tasa de emisión de título que asciende a 100 €, concepto y cantidad no incluida en el importe total del máster.

- **Condiciones económicas:**

- En la presente hoja de inscripción se recogen las cantidades correspondiente al programa contratado y que el alumno acepta: importe del curso y forma de pago.
- En los casos de pago fraccionado no interviene ninguna entidad de financiación externa y distinta a IMF.
- En el caso de pagos fraccionados o aplazados, las cuotas se abonarán en mensualidades corrientes sucesivas.
- El impago de cualquiera de las cantidades aplazadas dará lugar a la resolución de este contrato y por ende de la matrícula, pudiendo IMF reclamar el resto de cantidades pendientes de pago, reservándose el derecho de restringir el acceso a la plataforma de E-learning de aquel que no cumplan correctamente con el pago fraccionado de la matrícula, bloqueándose automáticamente el acceso desde el momento en el que consten, al menos, dos mensualidades impagadas.
- En el caso de que el alumno procediera al abono de las mensualidades debidas, antes del transcurso del plazo de dos meses a contar desde el último impago, IMF se compromete a reactivar el acceso a la Plataforma Online para que éste pueda seguir disponiendo de los materiales de estudio, ejercicios y tutorización habituales.
- Duración del contrato: la duración de la formación contratada será de máximo dos años desde la fecha de matriculación.
- En el supuesto de que el alumno no supere las oportunidades de evaluación extraordinarias o bien agote el plazo previsto sin haberse presentado a estas pruebas, causará baja automáticamente en IMF, considerándose el presente contrato extinguido.
- Una vez producida la baja, el alumno cuenta con un plazo de 1 mes para renovar su matrícula en las asignaturas correspondientes, siendo establecidos los costes de rematriculación por parte de IMF.

- **Resolución del contrato:**

- Derecho de desistimiento: el alumno dispone de un plazo de quince días naturales, contados desde la formalización de la matrícula, para desistir del contrato, con derecho al reintegro de las cantidades abonadas, mediante comunicación escrita a IMF. Para el caso en que el alumno haya contratado el servicio Plus, el alumno asumirá el coste directo de la devolución de los materiales, siempre y cuando éstos se encuentren en perfecto estado. En caso contrario, se le descontará del importe a devolver la parte correspondiente al valor de los daños producidos en el material.
- En el hipotético caso que por circunstancias fehacientes, de fuerza mayor por hechos extraordinarios, imprevisibles o inevitables, IMF no pudiese prestar definitivamente el servicio de formación que se contrata, se obliga a comunicarlo al alumno en un plazo máximo de treinta días, teniendo derecho el alumno al reintegro de las cantidades abonadas a estos efectos.
- Si el alumno abandonase el programa contratado, éste no tendrá derecho a la devolución de los importes ya abonados. IMF reclamará el cumplimiento del contrato. En todo caso, ante posibles causas de fuerza mayor de vida y fehacientemente acreditada, IMF se reserva el estudio de la situación del expediente de baja académica.

- **Prácticas:**

☐ He leído y acepto las condiciones del anexo 1 a esta matrícula Condiciones de la Promoción "Prácticas Garantizadas en todo el territorio nacional" para alumnos matriculados en Máster profesionales en IMF Business School a partir del 1 de Septiembre de 2013.

- **Protección de datos:**

- **Responsable:** IMF INTERNATIONAL BUSINESS SCHOOL S.L.
- **Dirección:** C/ BERNARDINO OBREGÓN Nº 25, 28012 MADRID
- **Teléfono:** +34913645157
- **Correo electrónico:** datos@imf.com

En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se le informa de que IMF INTERNATIONAL BUSINESS SCHOOL S.L. tratará sus datos para con la finalidad de gestionar la solicitud realizada por el titular de los datos en relación con los servicios proporcionados por la entidad. Para la correcta gestión de dichos servicios, y en los casos necesarios (gestión de ayudas, justificación de subvenciones, etc), sus datos serán comunicados a los organismos oficiales necesarios (Fundae, Fondo Social Europeo, etc). Además, IMF INTERNATIONAL BUSINESS SCHOOL S.L. tratará sus datos de alumno o antiguo alumno con finalidades comerciales y de publicidad, por cualquier medio, incluido el electrónico, para lo cual se le solicita su autorización:

☐ Marque la casilla si desea que sus datos sean tratados para envío de información comercial personalizada (cursos, eventos, seminarios, nuevos programas, etc.).

Asimismo, desde IMF INTERNATIONAL BUSINESS SCHOOL, S.L., y en relación al uso del Campus Virtual de la entidad, le informamos que se encuentra implantado un sistema de verificación consistente en reconocimiento facial y dinámica del tecleo, que permite garantizar inequívocamente su identidad mediante el tratamiento de datos biométricos con el objetivo de poder realizar los exámenes en modalidad online. En este sentido, únicamente se tratarán sus datos biométricos si usted otorga de forma libre su consentimiento, que le será solicitado en el primer acceso al campus virtual. En caso de que no otorgue su consentimiento al tratamiento de datos descrito, podrá realizar los exámenes de forma presencial en la sede de Madrid en las fechas programadas en el calendario académico.

Conforme a lo establecido en la normativa de protección de datos, Usted tiene derecho a obtener confirmación sobre si en IMF INTERNATIONAL BUSINESS SCHOOL S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Asimismo, podrá oponerse al tratamiento de sus datos, solicitar la limitación al tratamiento y la portabilidad de sus datos. Si considera que sus datos personales no han sido tratados conforme a la normativa, puede contactar con datos@imf.com. Igualmente, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido la satisfacción en el ejercicio de sus derechos, a través de la sede electrónica en www.aepd.es. Puede consultar la información adicional al tratamiento de sus datos en www.imf-formacion.com/privacidad.

- **Hoja de reclamaciones:**

- IMF las pone a disposición de sus alumnos.

El Alumno firmante reconoce estar debidamente informado sobre el programa que contrata, así como de las materias formativas, del sistema de impartición, modalidad, horarios de tutorías y metodología, y CONFORME con ello, suscribe la presente matrícula de inscripción, adquiriendo el firme compromiso del pago de la totalidad de la cantidad comprometida en este contrato.

El Alumno, siendo perfectamente conocedor del alcance y efectos académicos del título expedido por IMF, exime a esta Entidad de toda responsabilidad de cualquier denegación respecto de posibles homologaciones o convalidaciones del título obtenido, que se imparte amparo de los artículos 2 y 34 de la Ley Orgánica 6/2001, del 21 de diciembre, de Universidades, modificada por Ley Orgánica 7/2007, de 12 de abril. Estos estudios dan derecho a la expedición de diplomas u títulos propios que no tienen carácter oficial.

☐ He leído las condiciones.

En _____, a _____ de _____ de 20 _____ Firma del Alumno

CLÁUSULA PARA RECABAR EL CONSENTIMIENTO DE LOS ALUMNOS PARA RECONOCIMIENTO FACIAL Y PATRÓN DE TECLEO

- Responsable: IMF INTERNATIONAL BUSINESS SCHOOL, S.L.
  - Dirección: calle Bernardino Obregón 25, 28012 Madrid
  - Teléfono: 91 364 51 57
  - Correo electrónico: datos@imf.com
  - Delegado de Protección de Datos: Pablo Perancho Ruiz

En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se le informa de que IMF INTERNATIONAL BUSINESS SCHOOL, S.L.es la entidad responsable del tratamiento de sus datos personales biométricos relativos a la identificación de sus rasgos faciales, permitiendo su reconocimiento facial; así como de la dinámica del tecleo que permite el reconocimiento de su patrón de tecleo.

En cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en concreto en base a su artículo 83 se pretende por parte del Responsable de Tratamiento el establecimiento de un sistema educativo que garantice la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales. En consecuencia y en aras de los nuevos derechos digitales, se establece en los estudios, la implantación de un sistema de exámenes que garanticen unívocamente la identidad del alumno mediante la combinación del sistema de reconocimiento facial así como de dinámica de tecleo, garantizando de este modo la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

La finalidad del tratamiento es utilizar las mencionadas técnicas de reconocimiento facial para poder autentificarle como alumno y usuario del Campus, y poder verificar así su identidad a la hora de realización de pruebas online (exámenes) asegurando de este modo el debido cumplimiento de las obligaciones que le vinculan a usted como alumno de IMF INTERNATIONAL BUSINESS SCHOOL, S.L.

El procedimiento requiere que los alumnos se tomen tres fotografías en algún momento previo al examen, y que servirán como base de verificación; una vez llegado el momento de realizar la prueba, el ordenador tomará un determinado número de fotografías tanto en el momento de autentificarse en el sistema como en momentos aleatorios, durante el examen, comparando las diferentes capturas con las que se tomaron como base. Asimismo, se irá registrando su patrón de teclado a lo largo de todo el proceso definido, tanto durante el momento de alta en el Campus, durante la utilización del mismo, como en el momento de realización de la prueba online.

El tratamiento se legitima mediante el consentimiento expreso que se le solicita y usted otorga libremente.

Asimismo, se le informa de que el tratamiento de los datos personales de los que usted es titular únicamente se efectuará con las finalidades señaladas y con ninguna otra no declarada.

Los datos personales proporcionados se conservarán durante los plazos legalmente exigidos conforme a la legislación vigente.

No están previstas transferencias internacionales de sus datos personales fuera del Espacio Económico Europeo.

Cualquier persona tiene derecho a obtener confirmación sobre si en IMF INTERNATIONAL BUSINESS SCHOOL, S.L. estamos tratando datos personales que les conciernan, y en tal caso, derecho de acceso a sus datos personales, a los fines del tratamiento, y a las categorías de datos personales de que se trate.

Asimismo, tendrá derecho a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, los datos ya no sean necesarios para los fines que fueron recogidos; se haya retirado el consentimiento en el que se basa

el tratamiento o se oponga al tratamiento; los datos personales se hayan tratado de manera ilícita; o deban suprimirse para el cumplimiento de una obligación legal establecida en el derecho de la Unión o de los Estados miembros.
Podrá solicitar la limitación del tratamiento de sus datos cuando, impugne la exactitud de los datos personales durante el plazo que permita al responsable verificar la exactitud de los mismos; el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. En tales casos, únicamente conservaremos los datos para el ejercicio o la defensa de reclamaciones.

En determinadas circunstancias y por motivos relacionados con su situación particular, usted podrá oponerse al tratamiento de sus datos. IMF INTERNATIONAL BUSINESS SCHOOL, S.L. dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Tendrá derecho a recibir los datos personales que le incumban, y que haya facilitado, en un formato estructurado, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando, el tratamiento este basado en el consentimiento; o le tratamiento se efectúe por medios automatizados.

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, deberán comunicarlo por correo electrónico a la dirección datos@imf.com

Si considera que sus datos personales no han sido tratados conforme a la normativa, puede contactar con datos@imf.com. Asimismo, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido la satisfacción en el ejercicio de sus derechos, a través de la sede electrónica en www.aepd.es.

Los datos personales que tratamos en IMF INTERNATIONAL BUSINESS SCHOOL, S.L. proceden del propio interesado.

Puede consultar la información adicional al tratamiento de sus datos en https://imf-formacion.com/privacidad

Por último, se informa al interesado de que la consecuencia de no otorgar el consentimiento que se le solicita será la imposibilidad de realizar el examen en su modalidad online. En tanto no es posible verificar su identidad fehacientemente, en caso de no prestar su consentimiento al tratamiento de datos descrito, necesariamente deberá realizar el examen de forma presencial en Madrid para lo cual se programarán las fechas correspondientes.

¿Consiente expresamente el tratamiento de sus datos relativos al reconocimiento facial y patrón del tecleo con los fines anteriormente descritos?

☐ SI

☐ NO

Podrá revocar su consentimiento en cualquier momento en la dirección datos@imf.com

ANEXO V

INFORME DE EVALUACIÓN DE IMPACTO

EN LA PROTECCIÓN DE DATOS

IMF Instituto de Ciencias Empresariales

CONTENIDO

1. RESUMEN EJECUTIVO

2. DESCRIPCIÓN DEL TRATAMIENTO

3. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

4. METODOLOGÍA DE LA EIPD

5. ANÁLISIS DEL TRATAMIENTO

6. ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

7. MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

8. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

9. CONCLUSIONES Y RECOMENDACIONES

ANEXO I: DETALLE DE PREGUNTAS GENERALISTAS DESTINADAS A LA CONFIGURACIÓN DEL PERFIL BIOMÉTRICO.

ANEXO II: ACUERDO DE CONFIDENCIALIDAD FIRMADO POR LOS EMPLEADOS

ANEXO III: CONTRATO DE SERVICIO Y DE ENCARGADO DE TRATAMIENTO FIRMADO CON LA ENTIDAD ADR

ANEXO IV: CLÁUSULAS INFORMATIVAS DESTINADAS A INFORMAR A LOS ALUMNOS, ASÍ COMO A RECABAR SU CONSENTIMIENTO.

1. RESUMEN EJECUTIVO

El tratamiento de datos que en Instituto de Ciencias Empresariales IMF. S.L. se ha implantado consiste en el establecimiento de un procedimiento de verificación de identidad de los alumnos combinando las técnicas de reconocimiento facial y de reconocimiento de patrón de tecleo para poder verificar así, con todas las garantías exigidas, la identidad de las personas que están cursando sus estudios.

Los datos personales objeto de tratamiento se corresponden con las categorías especiales previstos en el artículo 9 del RGPD y más concretamente con datos biométricos.

Desde Instituto de Ciencias Empresariales IMF. S.L. sé es consciente de que los sistemas de verificación elegidos para comprobar la identidad de sus alumnos, requieren un alto grado de protección, en tanto son objeto de tratamiento, datos biométricos (pertenecientes a las categorías especiales de datos a que se refiere el artículo 9 RGPD) y además se emplean nuevas tecnologías.

Asimismo, el tratamiento objeto de análisis tiene cabida en el tercer caso de los enumerados en el artículo 35.3 del RGPD, en su apartado b: *"tratamiento a gran escala de las* categorías especiales de datos a que se refiere el artículo 9".Adicionalmente, el tratamiento coincide con uno de los supuestos incluidos en el listado publicado por la Agencia Española de Protección de Datos en virtud del art. 35.4 RGPD, en los que se requiere la realización de una Evaluación de Impacto relativa a la Protección de Datos. Concretamente se refiere a *"Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física"*

Por eso y de cara a garantizar la privacidad de los interesados afectados por el tratamiento de datos personales, se ha decidido actualizar la presente Evaluación de Impacto relativa a la Protección de Datos (en adelante EIPD), con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Asimismo, se adapta la EIPD al nuevo informe facilitado por la Agencia Española de Protección de Datos y además se decide incrementar las medidas de seguridad (mediante cifrado).

La EIPD ha sido desarrollada de manera conjunta por un equipo multidisciplinar con conocimientos en el ámbito jurídico y técnico, permitiendo abordar la evaluación de los riesgos desde diferentes ámbitos, permitiendo con ello establecer los riesgos a los que está expuesto el tratamiento objeto del presente informe.

En este sentido, se ha llevado a cabo un análisis de riesgos empleando para ello una metodología contrastada en el mercado, ya que combina las recomendaciones de la Agencia de Protección de Datos, así como metodologías de evaluación de riesgos propuesta por la norma ISO 31000.

En cuanto al contexto de la EIPD, se desea destacar que Instituto de Ciencias Empresariales IMF, S.L es un centro privado autorizado por la Administración Pública para la implantación de estudios superiores oficiales y se organiza de acuerdo a la Norma 01/2014, reguladora del Régimen Interior del Centro.

Adicionalmente, para la gestión de tratamiento se va a utilizar FACEidentity que es un sistema de reconocimiento facial que se puede utilizar en diferentes situaciones en las que sea necesaria la verificación de identidad del usuario.

Son numerosos los beneficios que se obtendrán con la implantación y se desarrollarán a lo largo del informe, pero cabe mencionar los siguientes:

- Mayor garantía de éxito derivado del sistema de evaluación continua.
- Reducción de costes derivados del desplazamiento para los alumnos.
- Reducción de esfuerzos para los alumnos.
- Innovación tecnológica.
- Máxima seguridad y garantías en la realización de exámenes.
- Mayor accesibilidad a los servicios ofrecidos por la entidad.
- Mejora reputacional de la entidad.

2. DESCRIPCIÓN DEL TRATAMIENTO

A. Fecha de realización de la EIPD

HISTORIAL DE CAMBIOS				
AUTORES	VERSIÓN	FECHA	HORA	OBSERVACIONES
Instituto de Ciencias Empresariales IMF. S.L. Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	1.0	12/02/2020	12:00h	Documentación Actualizada
Instituto de Ciencias Empresariales IMF. S.L. Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	2.0	24/02/2020	15:30h	Revisión fichero

Instituto de Ciencias Empresariales IMF. S.L. Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	3.0	23/03/2020	10:00h	Revisión y adaptación a plantilla EIPD - AEPD
Instituto de Ciencias Empresariales IMF. S.L. Dirección Asesoramiento prestado por el DPD, D. Pablo Perancho y su departamento de Protección de Datos.	4.0	27/03/2020	16:00h	Revisión definitiva

B. Nombre y Descripción del Tratamiento

El tratamiento de datos personales cuyo análisis nos ocupa recibe la denominación de Reconocimiento facial y dinámica del tecleo.

En primer lugar, resulta indispensable proceder a identificar claramente el tratamiento de datos personales que se pretende efectuar y asimismo, se debe analizar a qué finalidad responde el mismo, así como los medios a través de los cuáles se llevará a cabo:

En este sentido, cabe resaltar aquí que el tratamiento de datos que en Instituto de Ciencias Empresariales IMF, S.L. se esta gestionando consiste en el establecimiento de un procedimiento de verificación de identidad de los alumnos y que combina las técnicas de reconocimiento facial y de reconocimiento de patrón de tecleo para poder verificar así, con todas las garantías exigidas, la identidad de las personas que están cursando sus estudios, y que mayoritariamente son mayores de edad. Y donde se esta valorando abarcar más estudios.

Por un lado, el sistema de reconocimiento facial hace posible la identificación de una persona mediante las características biométricas de su rostro. Se trata de una tipología de identificación biométrica que hace uso de los rasgos fisiológicos para verificar la identidad de los usuarios. El

sistema que se utiliza emplea un conjunto de datos biométricos que logran la identificación de las personas a través de la medición de puntos estratégicos en la forma y estructura únicas de sus rostros.

Por su parte, el reconocimiento por patrón de tecleo, se trata de un sistema de reconocimiento biométrico consistente en medir la fuerza con la que el usuario teclea, el tiempo de pulsación y el plazo que transcurre entre dos pulsaciones de teclado.

Las implicaciones que se derivan de esta implementación son las siguientes:

1. Registro del perfil biométrico: la primera vez que accede el alumno a la plataforma, se le solicitará la toma de tres fotografías en distintas posturas para su registro, además de la escritura de un breve texto para la identificación de su patrón de tecleo.

2. Identificación continua en el Campus: para la obtención de un correcto patrón de teclado, al tratarse de una formación online y debido a la necesidad de completar un número determinado de trabajos en la plataforma, el sistema continuo registra el patrón de teclado.

3. Identificación intensiva en el examen online: se trata del principal objetivo de la implementación del citado sistema y consiste en garantizar de la forma más fehaciente posible que la persona que se dispone a realizar el examen online es aquella que está cursando los estudios y ninguna otra. Al proceder a su acceso al examen online, el usuario debe identificarse mediante una fotografía, y en caso de que el sistema no lo reconozca, no podrá realizar el mismo. Una vez que el usuario haya accedido con éxito al examen, se irán tomando fotografías de forma aleatoria durante la realización de este para su identificación, además de que se registrará su patrón de teclado. Esta información es contrastada por el sistema con los datos del perfil biométrico y con el patrón de teclado que se ha ido definiendo a lo largo del curso.

La evaluación de impacto ha sido actualizada al nuevo formato facilitado por la Agencia Española de Protección de datos. Asimismo, se ha decidido incluir como mejora de seguridad un cifrado de la base de datos y de las fotografías.

Se facilita a continuación el contenido del registro de actividades de tratamiento con el que se pretende dar cumplimiento a la obligación establecida en el artículo 30 RGPD:

Nombre del tratamiento	Reconocimiento facial y dinámica del tecleo
Responsables de Tratamiento	Instituto de Ciencias Empresariales de IMF. S.L.
Dirección del Responsable	C/ Costanilla de San Pedro 2, 28005 Madrid
Delegado de Protección de Datos	Pablo Perancho Ruíz dpd@imf.com
Descripción finalidad del tratamiento	Utilización de las técnicas de reconocimiento facial y dinámica del tecleo con el objetivo de autentificar a los alumnos en la plataforma del Campus y poder verificar así la identidad de los mismos a la hora de realización de pruebas online (exámenes).
Categoría de Interesados	Alumnos y supervisores.
Descripción tipo de datos	Datos biométricos: Datos relativos al reconocimiento facial y dinámica del teclado
Descripción Encargados de Tratamiento	ADR Infor S.L. (administración de la plataforma) DPD: Alberto Manuel García Martín datos@adrformacion.com
Cesión	No
En el caso de cesiones, indique destinatario de los datos y finalidad	No aplica
Transferencias internacionales	No hay transferencias internacionales
Destinatario de los datos, país y finalidad de la TI	No aplica
Documentación de garantías adecuadas en la TI	No aplica
Origen de Datos	Del propio interesado, su representante legal.

Plazo de conservación	Plazo Supresión: Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades derivadas del tratamiento. Posteriormente, la supresión se realiza conforme a la normativa de documentación y archivos. Incluir esto y eliminar campo de abajo.
Cantidad de datos tratados	De 25 a 1.500 interesados
Accesibilidad a los datos	En inicio únicamente tendrán acceso dos Técnicas de Formación encargadas del seguimiento del alumnado y la responsable de la Secretaría Académica, así como los administradores de la plataforma de ADR Infor S.L.
Información a los interesados	A través de cláusulas informativas conforme al artículo 13 RGPD, destinadas a recabar el consentimiento de los mismos.
Causa legitimadora del tratamiento	RGPD: 6.1.a) El interesado dio su consentimiento para el tratamiento de sus datos personales para los fines específicos.
Medidas de seguridad	Desarrolladas a lo largo del presente informe

Política de plazos de conservación/Plazos de supresión

Información personal	**Plazo de conservación**	**Justificación**
Perfil biométrico	Duración del curso académico, así como un año adicional.	Posible existencia de reclamaciones y/o gestiones que el alumnado deba realizar dentro de la plataforma
Identificación continua en el Campus	Plazo de un mes	Posible necesidad de depurar algún error existente
Identificación durante el examen	Duración del curso académico	Posibles invalidaciones de exámenes. Una vez cerradas las

		Actas del curso, ya no hay posibilidad de modificaciones.
Identificación a través de Key Identity	Se conservará mientras el alumno se encuentre matriculado en los estudios que cursa.	Los registros resultantes de Key Identity son ininteligibles.

C. Categorías de datos

Cabe plantearse aquí qué datos personales son objeto de tratamiento y quiénes son los interesados afectados por dicho tratamiento, así como las operaciones que se realizarán sobre los mismos, destacando en cualquier caso, que siempre será previo otorgamiento del consentimiento expreso por parte del interesado. La recogida de datos se realiza a través de dos herramientas implementadas dentro del campus virtual y cuyo funcionamiento se detalla a continuación:

FACEidentity es un sistema de reconocimiento facial que permite verificar la identidad del usuario. Cuando el alumno accede por primera vez al campus el sistema le solicita que realice 3 fotografías con las que se crea el perfil biométrico del usuario. Estas fotografías deben cumplir con unos requisitos para la correcta creación del perfil: una correcta iluminación, que los ojos estén abiertos o que solo aparezca una persona en la foto. Una vez que el usuario tiene creado su perfil, en los siguientes accesos se realiza una fotografía, la cual se valida contra dicho perfil. Estas fotografías también deben de cumplir los requisitos oportunos. No importa los cambios de apariencia (pelo, barba, gafas), los parámetros biométricos recogidos por FACEidentity permiten identificar correctamente al usuario. El proceso de reconocimiento consta de diferentes pruebas de vida que aseguran la presencia física del usuario frente a la cámara, como pueden ser girar la cabeza o sonreír. Si en el proceso se encuentra una foto errónea, bien sea porque no cumple los requisitos o porque ha fallado la prueba de vida, el servicio pedirá al usuario que repita la fotografía, solucionando el error generado.

KEYidentity es un servicio de reconocimiento del patrón de tecleo mediante inteligencia artificial. No se tiene en cuenta lo que el usuario escribe, sino cómo lo escribe. Para la creación del perfil biométrico, el alumno accede a una pantalla donde se le realizan unas preguntas generalistas y debe responder escribiendo un texto. Durante el desarrollo de las actividades en las que el alumno tiene que escribir (elaboración de trabajos, participación en foros, etc) el

sistema captura los ritmos del usuario, los envía al servidor de KEYidentity y comprueba, contra su perfil biométrico, la identidad del mismo. Se aporta a través del **Anexo I,** la relación de preguntas generalistas a las que se hace mención.

Para la realización de los exámenes el alumno accederá a la plataforma siguiendo el proceso descrito anteriormente. Una vez dentro, tendrá acceso a examen en las fechas y requisitos establecidos para ello. Al iniciar el examen, comienza un proceso de monitoreo que consiste en que el sistema irá tomando fotografías en un intervalo de tiempo determinado. Cada fotografía se envía al servidor de FACEidentity y se valida contra su perfil. Asimismo, todo lo que escriba en la resolución de examen se envía al servidor de KEYidentity y comprueba, contra su perfil biométrico, la identidad del mismo. Al terminar la monitorización continua, el supervisor de la plataforma podrá observar en el panel de administración los resultados de dicha sesión.

En este sentido, las categorías de interesados de los que se tratarán los datos personales necesarios para dar cumplimiento al tratamiento indicado anteriormente serán únicamente los alumnos y supervisores del Campus de Instituto de Ciencias Empresariales de IMF. S.L., quiénes deberán verificar su identidad a la hora de realizar las pruebas y exámenes online que los cursos en los que están realizando sus estudios, exigen. Cabe precisar que la condición de supervisor del Campus se limita a tres personas: dos Técnicas de Formación encargadas del seguimiento del alumnado y la responsable de la Secretaría Académica. Se aporta a través del **Anexo II,** el acuerdo de confidencialidad firmado por los empleados de la entidad.

Asimismo, procede destacar que los datos personales objeto de tratamiento se corresponden con las categorías especiales de datos personales previstos en el artículo 9 del RGPD y más concretamente con datos biométricos, en tanto se trata, tanto de los rasgos faciales de los interesados, como de su dinámica del tecleo y ambos a través de medios técnicos específicos, permiten la identificación o la autenticación unívocas de las personas físicas.

En este sentido, si se hace hincapié en que la finalidad que se pretende lograr a través del presente tratamiento requiere de todos los datos objeto de tratamiento, ya que de lo contrario no sería posible la identificación unívoca del interesado y en consecuencia, no se podría determinar sin margen de error, que el alumno que realiza el examen es efectivamente aquel que se encuentra matriculado en el curso. Ello porque los métodos alternativos como tarjetas identificativas, contraseñas o similares podrían ser utilizados por otros individuos, dando lugar con ello a posibles suplantaciones de identidad.

D. Identificación del Responsable-RGPD

En el presente tratamiento intervienen las siguientes figuras:

El responsable de tratamiento respecto al tratamiento objeto de análisis es Instituto de Ciencias Empresariales de IMF. S.L.

Los datos de contacto del Delegado de Protección de Datos son dpd@imf.com (auxiliado por un departamento de protección de datos).

E. Contexto interno del tratamiento en la organización

Instituto de Ciencias Empresariales IMF es un centro de educación superior del sistema universitario español adaptado al Espacio Europeo de Educación Superior (EEES), es decir, es un centro privado autorizado por la Administración Pública para la implantación de estudios superiores oficiales.

Estructura orgánica de instituto de Ciencias Empresariales IMF

Instituto de Ciencias Empresariales IMF se organiza de acuerdo con la Norma 01/2014, reguladora del Régimen Interior del Centro, que establece la preceptiva existencia del Claustro como máximo órgano de representación de la comunidad universitaria, la Junta de Centro como órgano académico colegiado superior, y el Consejo Asesor como el órgano consultivo del Centro. Así mismo establece como órganos académicos unipersonales el Decanato, el Vicedecanato, la Secretaría y las Direcciones de los estudios implantados. En total el acceso al tratamiento se realiza por un número reducido de usuarios del centro. En este sentido, las responsabilidades de cada órgano son las siguientes:

- **Claustro:** son miembros natos del Claustro las personas titulares de todos los cargos académicos del Centro y el profesorado que *detente venia docendi* en alguno de los estudios implantados, y son miembros electos del Claustro, hasta un máximo de 50 miembros: los representantes del personal, tutor del alumnado, y del personal de administración y servicios, que serán elegidos de acuerdo con el reglamento de funcionamiento del Claustro.

  El Claustro es convocado por el Decanato del Centro y se reúne ordinariamente en Madrid el tercer viernes del mes de julio.

  Son competencias del Claustro:

  - Velar por el cumplimiento de las normas del Centro.
  - Ser informado de las líneas generales de actuación del Centro en la docencia, la investigación, en la administración y en la gestión.
  - Formular propuestas de mejora en la calidad de las actividades del Centro.
  - Ser oído en el nombramiento de la persona titular del Decanato.

- **Junta de Centro:** la Junta del Centro es el órgano académico colegiado superior del Centro y lo constituyen las personas titulares del Decanato, que la preside, del Vicedecanato, de la Secretaría, que asume las funciones de secretaría del órgano

colegiado, así como todas las personas responsables de la Dirección de los estudios oficiales implantados en el Centro.

Las competencias de la Junta del Centro son:

- Proponer la aprobación y/o reforma de las normas del Centro.
- Proponer la implantación de nuevos títulos, así como la aprobación y la modificación de los respectivos planes de estudios.
- Proponer la creación y la supresión de servicios universitarios, y definir su composición y organización.
- Proponer la configuración y las modificaciones de la plantilla del personal académico, así como su sistema de selección y de promoción.
- Proponer criterios para la concesión de permisos, excedencias y años sabáticos al profesorado.
- Aprobar la memoria de cada curso académico
- Aprobar el calendario académico.
- Resolver los conflictos de competencias que se planteen entre estudios o servicios universitarios.
- Cualquier otra competencia que le sea atribuida por este Reglamento y otras disposiciones que le puedan ser de aplicación.

- **Consejo Asesor**: el Consejo Asesor del Centro es un órgano académico colegiado de naturaleza consultiva.

  Sus miembros son nombrados por la Junta General, a propuesta de los colectivos e instituciones que participan en los procesos de consulta externos sobre los estudios oficiales y en sus comisiones de seguimiento.

  El Decanato nombra entre los consejeros a su Presidente y Secretario, los cuales ejercen dichas funciones de acuerdo con el reglamento adoptado para el funcionamiento del órgano.

- **Decanato**: el Decanato es el órgano académico unipersonal superior del Centro y la persona titular ha de ser un académico con el grado de doctor y dedicación completa al Centro. Su nombramiento y cese corresponde al Patronato de la Universidad, a

propuesta de la Junta General, una vez oído el Claustro del Centro. El mandato ordinario del cargo será de cuatro años, no estableciéndose límites en su renovación.

Las competencias del Decanato son las:

- Dirigir y supervisar la docencia, la investigación y el resto de las actividades académicas del Centro.
- Proponer a la Administración el nombramiento de las personas titulares de los Vicedecanatos y la Secretaría del Centro.
- Reconocer los estudios del alumnado que así lo solicite, oídos los responsables de los programas y materias afectadas y de conformidad con las normas aplicables.
- Velar por el cumplimiento de las normas universitarias en el Centro, así como el buen funcionamiento de los servicios y el mantenimiento de la convivencia académica.
- Fomentar la investigación y las actividades culturales y de extensión universitaria.

- **Vicedecanato**: el Vicedecanato es un órgano académico unipersonal destinado a ejercer las funciones del Decanato en el caso de ausencia, enfermedad o defunción de la persona titular, así como a ejercer las funciones delegadas específicas que el Decanato considere oportunas.

  La persona titular del Vicedecanato ha de ser un académico con el grado de doctor y su nombramiento y cese corresponde al Decanato. El mandato ordinario del cargo es de cuatro años, no estableciéndose límites en su renovación.

- **Secretaria**: la Secretaría Académica es un órgano académico unipersonal encargado de asistir al Decanato en las tareas de gobierno ordinario del Centro, de levantar y custodiar las actas de las sesiones de la Junta de Centro, así como de certificar los expedientes académicos del alumnado y dirigir el servicio de Secretaría Académica del Centro.

  La persona titular de la Secretaría ha de ser un académico con el grado de doctor y dedicación completa al centro. Su nombramiento y cese corresponde al Decanato. El

mandato ordinario del cargo será de cuatro años, no estableciéndose límites en su renovación.

- **Direcciones**: las Direcciones de Estudios son los órganos académicos unipersonales responsables de la coordinación general de los estudios oficiales implantados en el Centro, y sus personas titulares han de ser académicos con el grado de doctor. Su nombramiento y cese corresponde al Decanato y su mandato es indefinido.

  Las Direcciones de Estudios ejercen las funciones siguientes:

  - Participar en la Comisión de Seguimiento.
  - Informar a la Secretaría de las solicitudes del alumnado de su Estudio sobre reconocimiento de créditos, así como las referidas al proceso de admisión.

Entre las normas que le afectan al Instituto de Ciencias Empresariales IMF están las siguientes:

- **Norma 01/2014**, de 25 de abril, reguladora del Régimen Interior del Centro
- **Norma 02/2014**, de 25 de abril, reguladora del proceso de implantación de nuevos estudios en el Centro
- **Norma 03/2014**, de 25 de abril, reguladora del proceso de admisión del alumnado a los estudios del Centro
- **Norma 04/2014**, de 25 de abril, reguladora del proceso de reconocimiento y transferencia de ECTS del Centro
- **Norma 05/2014**, de 25 de abril, reguladora del Sistema Interno de Garantía de Calidad
- **Norma 06/2016**, de 2 de enero, reguladora de los Sistemas de Evaluación
- **Norma 07/2016**, de 2 de enero, reguladora del proceso de elaboración y evaluación de los Trabajos Fin de Estudios
- **Norma 08/2016**, de 2 de enero, reguladora de las Actividades Formativas

La sede oficial del Instituto de Ciencias Empresariales IMF se sitúa en el Palacio de Anglona, situado en el número 2 de la Costanilla de San Pedro de la Villa de Madrid, en la céntrica e histórica zona de la ciudad conocida popularmente como el “Madrid de los Austrias”.

La sede dispone de una superficie aproximada de quinientos metros cuadrados, se ubican los Laboratorios de Docencia y de Investigación y la unidad de gestión de Recursos Tecnológicos, servicios todos ellos preceptivos por Real Decreto 420/2015, de 29 de mayo, de creación,

reconocimiento, autorización y acreditación de universidades y centros universitarios. En la misma sede se ubica también la unidad de Gestión Académica y Docente.

El Centro ofrece los recursos para el aprendizaje y la investigación a través de la biblioteca virtual ODILO, una plataforma digital puntera de aprendizaje colaborativo, que permite poner a disposición del alumnado y el profesorado una gran biblioteca digital de contenido empresarial con miles de libros, revistas, artículos, informes y vídeos, así como herramientas para que saquen el máximo provecho a los contenidos e interactúen con otros universitarios en un espacio de formación abierto.

Por último, para la gestión de tratamiento se va a utilizar FACEidentity que es un sistema de reconocimiento facial que se puede utilizar en diferentes situaciones en las que sea necesaria la verificación de identidad del usuario, como por ejemplo acceso a área privada, exámenes online o webinars.

Se utiliza para identificar a los usuarios, por ejemplo, en los accesos al campus. En esta integración, se toma una fotografía y se valida contra el perfil del usuario, permitiéndole acceder si el resultado es correcto. También se utiliza para monitorización continua, por ejemplo, para validar la autoría de un examen online ya que el sistema irá tomando fotos del usuario cada cierto periodo de tiempo y las validará contra su perfil.

En caso de que se desee conocer información adicional sobre la entidad, se puede consultar a través del siguiente enlace: https://www.imfice.es/

En último lugar, cabe mencionar aquí las posibles relaciones del tratamiento cuyo análisis nos ocupa con otros tratamientos de datos de la propia organización y en concreto con los siguientes tratamientos personales identificados en el registro de actividades:

El tratamiento denominado “Alumnos” tiene como finalidad la grabación de matrículas, impartición, seguimiento y evaluación de los cursos de los alumnos que participan en ellos y se ha identificado como interesados a los alumnos de la entidad.

Asimismo, se encuentra relación con el tratamiento denominado “Gestión financiera”, cuya finalidad es llevar a cabo correctamente toda la gestión de los clientes y alumnos de la entidad desde el punto de vista comercial, contable, fiscal y administrativa. Se identifica como interesados, entre otros, a los alumnos de la entidad.

F. Contexto externo de la organización y el tratamiento.

El objetivo principal de Instituto de Ciencias Empresariales IMF es dar un servicio de calidad a los alumnos que demandan formación superior, focalizando de forma ágil sus problemas y prestando una atención y servicio excelentes, así como la búsqueda constante de ocasiones para mejorar los productos y servicios y crear nuevas oportunidades de formación

La organización cree que la experiencia del alumnado y las relaciones éticas van de la mano, prestando la máxima importancia a la seguridad y protección de los datos.

La estrategia de Instituto de Ciencias Empresariales IMF está orientada a garantizar las necesidades y expectativas de los alumnos adoptando para ello un enfoque diferenciador, dinámico, eficiente y responsable. En este sentido se pretende:

- Mejorar la relación con los alumnos, simplificando la interacción mediante herramientas colaborativas que permiten ir adquiriendo un mejor conocimiento de los alumnos.
- Diversificar mediante la optimización de nuestros activos explorando nuevas oportunidades de mejora, con el fin de anticipar las necesidades esenciales de nuestros alumnos y, simultáneamente, seguir trabajando en nuestro anhelo de mejora continua.

Instituto de Ciencias Empresariales IMF lo constituyen centros de formación universitaria sólidos y estables, que ha podido ampliar sus servicios de una forma continuada y sostenida aún en tiempos de crisis económica, debido a su interés por la mejora e innovación y su afán de servicio a la comunidad.

3. LICITUD DEL TRATAMIENTO Y CUMPLIMIENTO NORMATIVO

Tal y como establece el RGPD, el tratamiento de datos personales debe ser lícito y, por tanto, se ha de asegurar que se cuenta con una causa legítima correctamente aplicada para el mismo, de modo que los datos personales se traten de acuerdo con las condiciones recogidas en el RGPD.

En este sentido, el artículo 6 del RGPD, recoge los supuestos en los que se considera que el tratamiento de datos personales es lícito y entre los mismos, se encuentra el consentimiento.

Siguiendo el literal del art 9 RGPD que versa sobre las categorías especiales de datos personales, entre los que se encuentran los datos biométricos, se puede observar que se establece, como regla general, la prohibición del tratamiento de datos biométricos con la finalidad de identificar de manera unívoca a una persona física.

No obstante, el RGDP en el apartado 2. a) del artículo 9 continúa indicando que "lo dispuesto anteriormente no será de aplicación cuando concurran una serie de circunstancias". Entre las circunstancias previstas y que podrían constituir una excepción a la prohibición, se prevé expresamente la identificación del consentimiento como base legitimadora del tratamiento de datos biométricos.

Se podría invocar el consentimiento como causa legitimadora del tratamiento que se quiere llevar a cabo, pero es conveniente asegurar que se dan todas las condiciones para que el consentimiento sea válido, y por tanto libre, específico, informado e inequívoco..

En esta línea, el artículo 7 RGPD establece las siguientes condiciones:

"1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales"

> Para dar cumplimiento a este primer punto, el responsable de tratamiento, Instituto de Ciencias Empresariales IMF, en cumplimiento del principio de responsabilidad proactiva, ha procedido a elaborar las cláusulas destinadas a recabar el consentimiento explícito e informado de los interesados en un formato que permita a posteriori poder demostrar el cumplimiento de esta obligación en caso de ser necesario y ello antes del inicio del tratamiento. Para ello, se habilitarán casillas destinadas a ser marcadas por aquellos interesados que decidan otorgar su consentimiento de forma libre, explícita e informada.

"2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento"

> En función de lo dispuesto en el segundo de los requisitos, es condición indispensable para que el consentimiento sea válido, que la solicitud se presente de forma separada respecto del resto de información en su caso y que el usuario pueda acceder y entender esta información de forma clara y fácil. En este sentido, se garantiza que la cláusula destinada a recabar dicho consentimiento se presentará de forma separada respecto al resto de información que se proporcione al interesado.

"3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a

su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo"

Con el objetivo de dar cumplimiento a este punto, Instituto de Ciencias Empresariales IMF, en el caso de que los alumnos no deseen prestar su consentimiento al tratamiento en cuestión o lo retiren posteriormente, fijará anualmente dos fechas que permitirán la realización de los exámenes de forma presencial como alternativa y con las mismas garantías, a celebrar en Madrid, España.

"4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato"

En este sentido, se puede afirmar sin lugar a duda que el interesado puede hacer una elección real y no existe ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta ello porque, en caso de que el interesado no desee prestar su consentimiento al tratamiento indicado, podrá realizar el examen de forma presencial y con los mismos derechos y deberes que asisten a aquellos alumnos que se decantan por la opción online. Se garantiza que la prestación del servicio no depende de modo alguno del consentimiento en cuestión. Asimismo, también se da cumplimiento al art. 6 de la LOPDGDD.

4. METODOLOGÍA DE LA EIPD

a) Implicados en la ejecución de la EIPD

La EIPD ha sido desarrollada de manera conjunta por un equipo multidisciplinar con conocimientos en el ámbito jurídico y técnico, permitiendo abordar la evaluación de los riesgos

desde diferentes ámbitos, permitiendo con ello establecer los riesgos a los que está expuesto el tratamiento objeto del presente informe actualizado.

Los recursos que han participado son los siguientes:

- DPD: el Delegado de Protección de Datos tiene atribuidas las siguientes funciones:
    - Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
    - Supervisar el cumplimiento de la normativa.
    - Asesorar respecto de la evaluación de impacto relativa a la protección de datos.
    - Cooperar con la autoridad de control.
    - Actuar como punto de contacto para cuestiones relativas al tratamiento.
    - Difundir y comunicar las prácticas de protección de datos personales implementadas a los usuarios del interior de la organización, formando y concienciando a todo el personal sobre las mismas.
    - Efectuar el análisis de riesgos de cada tratamiento y aplicar las medidas de seguridad necesarias, y en su caso, aplicación de las oportunas políticas de protección de datos.
    - Supervisar las auditorías correspondientes.
- Responsable del Tratamiento: el responsable de tratamiento, con un perfil jurídico tiene que velar por:
    - Asegurar que las prácticas de protección de datos personales en la compañía cumplan con la Ley y otras normas aplicables.
    - Difundir y comunicar las prácticas de protección de datos personales implementadas a los usuarios del interior de la organización, formando y concienciando a todo el personal sobre las mismas.
    - Asegurar el cumplimiento de los principios de protección de datos.
    - Cumplir con la obtención del consentimiento inequívoco.
    - Garantizar los derechos del tratamiento de los menores de edad.
    - Cumplir con el nuevo deber de información de forma integral.

- Establecer y gestionar procedimientos para la recepción, tramitación, seguimiento y atención de las solicitudes para el ejercicio de los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.
- Establecer y gestionar procedimientos para la recepción, tramitación, seguimiento y atención de los nuevos derechos de los afectados.
- Llevanza del registro de actividades del tratamiento.
- Regularizar las relaciones con los encargados de tratamiento conforme al RGPD.
- Efectuar las evaluaciones de impacto de los tratamientos de datos personales.
- Elegir únicamente encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD.
- Consultar y facilitar la información necesaria, a la autoridad de control sobre los tratamientos que entrañarían un alto riesgo, como resultado de la evaluación, si el responsable no toma medidas para mitigarlo.

- Encargado de tratamiento **(Anexo III)**:
  - Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional;
  - Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
  - Aplicar todas las medidas y controles de seguridad necesarias;
  - Asistir al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para

que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;

- Ayudar al responsable a garantizar el cumplimiento de las obligaciones;
- A elección del responsable, suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales.
- Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

El tratamiento implica el uso de tecnologías novedosas a la hora de evaluar al alumnado de manera remota a través de FACEidentity, el cual identifica a un usuario mediante las características faciales extraídas de una imagen captada por su webcam. FACEidentity se basa en uno de los más avanzados sistemas de Inteligencia Artificial para reconocimiento facial que existen en la actualidad, AWS Rekognition.

De un modo sencillo se registra el perfil biométrico del usuario mediante 3 fotografías. Una vez creado el perfil, durante el proceso de identificación el servicio solicita diferentes acciones que aseguran la presencia física del usuario frente a la cámara.

Con FACEidentity se puede s asegurar que la persona que está delante del dispositivo es quien dice ser sin importar sus posibles cambios de apariencia.

Para la gestión de dicha tecnología se cuenta con el DPD de INSTITUTO DE CIENCIAS EMPRESARIALES IMF que a su vez es el Responsable de Seguridad, que cuenta con un perfil tecnológico capaz de controlar y gestionar con el proveedor de servicios cualquier evento funcional de la plataforma, así como el impacto a la privacidad de los interesados y que asimismo, se encuentra respaldado por un departamento de protección de datos bajo su coordinación, contando con el asesoramiento de una consultora integral para el asesoramiento en materia de protección de datos y un abogado en ejercicio experto en protección de datos.

b) Guías, herramientas, metodologías, normas y dictámenes utilizados en la evaluación

El tratamiento de Reconocimiento Facial y dinámica de tecleo implica la gestión de datos biométricos mediante una tecnología de evaluación novedosa en el mercado.

Debido a ello se ha llevado a cabo un análisis de riesgos contrastada en el mercado ya que combina las recomendaciones de la Agencia de Protección de Datos y metodologías de evaluación de riesgos propuesta por la norma ISO 31000.

La metodología de Análisis de Riesgos se he realizado de manera analítica con los responsables del tratamiento en el cual se han tenido en cuenta las siguientes dimensiones:

- Finalidad del tratamiento: donde se tiene en cuenta el tipo de finalidad a la que están destinados los tratamientos, en especial aquellos que pueda suponer riesgos para los derechos o libertades de los interesados, categorías especiales de datos o datos relativos a condenas o delitos penales.
- Cantidad de datos tratados: se evalúa la cantidad de datos de los interesados que se gestionan, ya que a mayor volumen de tratamientos mayor es el riesgo para los interesados.
- Plazo de conservación: se define un plazo de conservación de los datos que se debe limitar únicamente a lo estrictamente necesario y cuanto mayor sea el periodo de almacenamiento, mayor será el riesgo de producirse alguna vulneración de los derechos.
- Accesibilidad: se valora el número de personas que tienen acceso al tratamiento, ya sean empleados o encargados del tratamiento.
- Tipos de datos tratados: se diferencian los tipos de datos tratados, teniendo en cuenta la existencia de datos especialmente protegidos o aquellos que puedan darnos datos de personalidad, comportamientos, etc.
- Transferencias internacionales: se evalúa la existencia o no de transferencias internacionales teniendo en cuenta el hecho objetivo, no si existen medidas para que se realicen de forma legal.

Derivado de dicho análisis se establece la necesidad de realizar una evaluación de impacto del tratamiento objeto del presente informe. Para ello se ha analizado en profundidad las

implicaciones de dicho tratamiento para INSTITUTO DE CIENCIAS EMPRESARIALES IMF, En este sentido partiendo del Tratamiento se han definido los recursos necesarios para gestionarlo.

Es por ello que se han identificado aquello recursos hardware, software, instalaciones, encargados de tratamiento necesarios, estableciendo para cada uno de ellos un listado de riesgos que pueden afectar a los interesados. Estos riesgos han sido evaluados mediante los siguientes criterios:

- Probabilidad: probabilidad de que un riesgo se materialice en función de la experiencia existente en situaciones similares y de los controles preventivos existentes.
- Impacto: determina el daño o la degradación que produciría en los procesos de la organización la materialización de la amenaza.

La metodología empleada en el análisis de riesgos debe perseguir un objetivo claro: obtener un valor que nos indique el riesgo asociado a los tratamientos y los activos que lo soportan y que nos permita tomar decisiones priorizadas. Estas decisiones tienen que tomarse por comparación con un umbral de riesgo definido.

El cálculo del riesgo de una amenaza se realiza mediante la siguiente tabla teniendo en cuenta la probabilidad y el impacto obtenidos:

PROBABILIDAD					
Muy Alta	Medio	Medio	Alto	Muy alto	Muy alto
Alta	Medio	Medio	Alto	Alto	Muy alto
Media	Bajo	Bajo	Medio	Alto	Alto
Baja	Muy Bajo	Bajo	Bajo	Medio	Medio
Muy Baja	Muy bajo	Muy bajo	Bajo	Bajo	Medio
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
	IMPACTO				

Una vez realizado el análisis de riesgos, la Dirección debe aprobar los resultados obtenidos.

Para aquellos tratamientos que no se asuman sus riesgos asociados, se establece un plan de tratamiento que incluye la definición de medidas de seguridad a implementar, plazos, responsables y descripción de las actividades a realizar.

Una vez ejecutado el plan de tratamiento se debe reevaluar la situación para verificar que se han mitigado las amenazas tratadas e identificar el riesgo residual existente que debe ser aprobado por Dirección.

5. ANÁLISIS DEL TRATAMIENTO

Se indica a continuación el ciclo de vida relacionado con el tratamiento objeto de análisis

CAPTURA DE LOS DATOS

Actividades
La recogida de datos se realiza a través de dos herramientas integradas dentro del campus virtual y cuyo funcionamiento se detalla a continuación: FACEidentity es un sistema de reconocimiento facial que permite verificar la identidad del usuario y monitorizarlo cuando realiza los exámenes. <u>Creación del perfil biométrico en FaceIdentity.</u> Cuando el alumno accede por primera vez al campus el sistema le solicita que realice 3 fotografías con las que se crea el perfil biométrico del usuario. Estas fotografías deben cumplir con unos requisitos para la correcta creación del perfil: una correcta iluminación, que los ojos estén abiertos o que solo aparezca una persona en la foto. Una vez que el usuario tiene creado su perfil, en los siguientes accesos se realiza una fotografía, la cual se valida contra dicho perfil. <u>Identificación con FaceIdentity.</u> El proceso de identificación se usa para validar la identidad del usuario cada vez que hace login en el campus. Es usado por tanto como doble factor de autenticación.

El proceso de reconocimiento consta de diferentes pruebas de vida que aseguran la presencia física del usuario frente a la cámara, como pueden ser girar la cabeza o sonreír. Si en el proceso se encuentra una foto errónea, bien sea porque no cumple los requisitos o porque ha fallado la prueba de vida, el servicio pedirá al usuario que repita la fotografía corrigiendo el error generado. En este proceso el Faceidentity captura una fotografía de la webcam del usuario que se registra. Esta fotografía se envía a AWS Rekognition, es analizada y comparada con el perfil biométrico ya creado y devuelve un porcentaje de similitud con el modelo. En función de este resultado FaceIdentity devuelve al campus si la identificación ha sido positiva, negativa o incertiumbre.

Monitorización con FaceIdentity.

Este proceso solamente se realiza durante la realización del examen.

FaceIdentity muestra la imagen de la webcam del usuario a través de un iframe que va capturando fotografías del alumno cada cierto tiempo mientras este realiza el examen. Estas fotografías capturadas son enviadas al servicio FaceIdentity que las almacena y a su vez procesa con AWS Rekognition. En este procesado se verifica la identidad del usuario para cada una de las imágenes, así como otros detalles adicionales: que solamente aparece una persona en la pantalla, la dirección en la que mira, que el rostro se muestre completo.

Los datos capturados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

KEYidentity es un servicio de reconocimiento del patrón de tecleo mediante inteligencia artificial. No se tiene en cuenta lo que el usuario escribe, sino cómo lo escribe.

Creación del perfil biométrico.

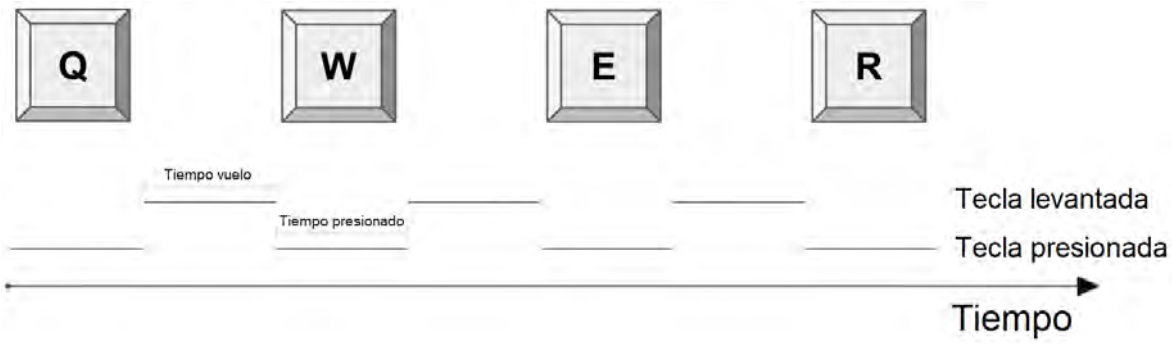
Para la creación del perfil biométrico, el alumno accede a una pantalla donde se le realizan unas preguntas generales a las que tiene que responder escribiendo un texto. A partir de estas muestras en las que se registra una matriz de datos con los tiempos de pulsación y vuelo de cada tecla el sistema genera un modelo biométrico de los ritmos de escritura del usuario.

Monitorización de la identidad con keyidentity.

Durante el desarrollo de las actividades en las que el alumno tiene que escribir (elaboración de trabajos, participación en foros, etc) el sistema captura los ritmos del usuario, los envía al servicio

de KEYidentity y comprueba contra su perfil biométrico la identidad del mismo. El resultado de las identificaciones es almacenado en la base de datos del servicio.

KEYidentity usa tecnología JavaScript para la captura de tiempos de vuelo y pulsación de cada tecla. El servicio Keyidentity almacena estas matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario



Datos Tratados

FaceIdentity

Los datos capturados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

Para el servicio FACEidentity, se utilizan las tablas USUARIOS y LOGS. En la tabla USUARIOS se guardan:

- El id biométrico
- El id externo del usuario
- El id del cliente
- El número de fotos que ha utilizado el usuario para entrenarse (0 no está entrenado, 3 si está entrenado)
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)

Si el usuario está verificado (el cliente ha validado el perfil biométrico desde la consola de supervisor)

En la tabla LOGS, se almacenan los siguientes datos:

El id de la identificación
El id biométrico del usuario
La fecha en la que se ha realizado la comprobación
El porcentaje de similitud con cada una de las fotos del entrenamiento
El resultado obtenido (positivo, negativo o incertidumbre)
La prueba de vida a la que se ha sometido el usuario (gesto en la fotografía)
Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
El id enlazado, id de la anterior comprobación si sigue en la misma sesión
Si la foto está almacenada o no.
El user agent.
El posicionamiento de la cara respecto a la cámara, para saber si el usuario está mirando a la pantalla o no.
El tipo de registro (identificación o monitorización)

Keyidentity

Para el servicio keyidentity los datos que se capturan son las matrices de tiempos de cada usuario, el useragent, ip del usuario.

Para el servicio KEYidentity, se utilizan las tablas KEYSTROKE_USUARIOS_TEXTO y KEYSTROKE_LOGS_TEXTO.

En la tabla KEYSTROKE_USUARIOS_TEXTO se guardan:

El id biométrico
El id del cliente
El id externo del usuario
Si el usuario está entrenado o no
El número de registros que lleva el usuario
El porcentaje actual de identificaciones correctas y el porcentaje de intentos ilícitos detectados en una prueba interna que se realiza para comprobar su robustez.

Si el usuario se ha marcado como sospechoso y un comentario de porque se ha marcado así.

El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)

Si el usuario tiene que contar para la facturación.

En la tabla KEYSTROKE_LOGS_TEXTO, se almacenan los siguientes datos:

El id de la identificación

El id biométrico del usuario

Los datos de los tiempos de tecleo de la identificación

El tipo de registro (entrenamiento o identificación)

El porcentaje de similitud con el modelo entrenado

La fecha en la que se ha realizado la comprobación

Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros

La IP, el navegador, el SO y la ciudad (basada en su IP) del usuario para saber de dónde vienen los datos

El número de caracteres que tiene el registro

Si la pantalla es táctil o no.

El user agent.

Las categorías de datos personales objeto de tratamiento son las siguientes:

- Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica de tecleo.

Origen de los Datos

Los datos personales únicamente son proporcionados por el propio interesado una vez que ha sido informado de todos los aspectos relativos al tratamiento de datos personales.

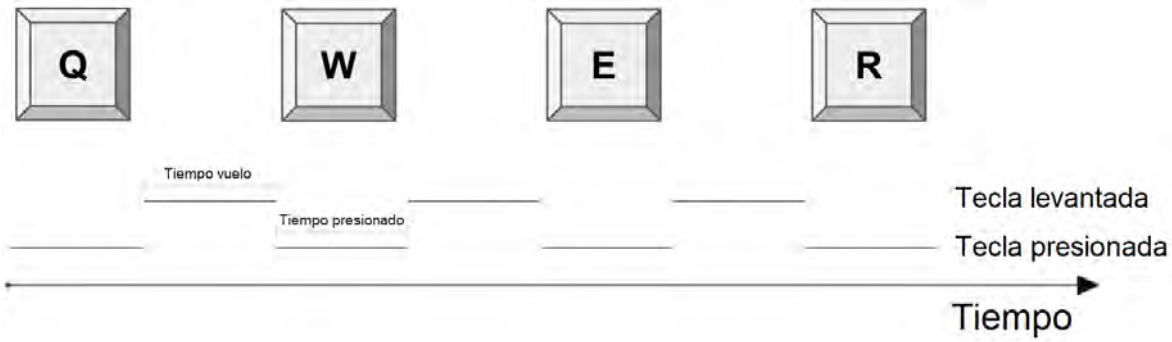
Tecnologías Intervinientes

FACEidentity y KEYidentity son desarrollos propios de nuestro partner tecnológico ADR Infor, S.L. alojados en la nube AWS. Los datos están alojados en Irlanda con centro de respaldo en París.

Para la captura de las fotografías se utiliza un iframe que envía los datos al servicio FaceIdentity.

Para la captura de los ritmos de tecleo se utiliza una función Javascript que captura los ritmos de tecleo en los editores de texto donde el alumno responde a las preguntas escribiendo con el teclado. Una vez se ha llenado el buffer de datos con la captura de tiempos esta es enviada al servicio KeyIdentity para su registro e identificación.

KEYidentity usa tecnología JavaScript para la captura de tiempos de vuelo y pulsación de cada tecla.



CLASIFICACIÓN Y ALMACENAMIENTO

Actividades

FaceIndetity

El servicio FaceIdentity almacena fotografías capturadas asociadas a un Id de usuario. Los datos biométricos no son gestionados por el servicio sino que son generados a partir de la fotografía por el api de AWS Rekognition. El api AWS Rekognition es la que genera el modelo biométrico, lo almacena en una colección interna y lo compara con el del usuario devolviendo a Faceidentity el porcentaje de similitud entre modelos. FaceIdentity por tanto no gestiona ni almacena estos datos biométricos.

Keyidentity

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Con estos datos se construye un modelo biométrico

formado por tres archivos asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Cuando el servicio recibe nuevas matrices de tiempos estas son procesadas y comparadas con el modelo almacenado en el bucket S3. Como resultado de este proceso Rekognition genera un nuevo registro en la base de datos guardando el porcentaje de similitud con el modelo y la matriz de tiempos procesada.

Datos Tratados

El servicio FaceIdentity almacena fotografías capturadas asociadas a un Id de usuario. Los datos biométricos no son gestionados por el servicio sino que son generados a partir de la fotografía por el api de AWS Rekognition. El api AWS Rekognition es la que genera el modelo biométrico y lo compara con el del usuario devolviendo a Faceidentity el porcentaje de similitud entre modelos. FaceIdentity por tanto no gestiona ni almacena estos datos biométricos.

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Con estos datos se construye un modelo biométrico formado por tres archivos asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Como resultado de este proceso Rekognition genera un nuevo registro en la base de datos guardando el porcentaje de similitud con el modelo y la matriz de tiempos procesada.

Ubicación de los datos

<u>FACEidentity</u>

En el punto anterior se explica que FaceIdentity almacena fotografías, pero no gestiona ni trata datos biométricos, ya que estos son únicamente generados y gestionados por el servicio AWS Rekognition. Los datos que almacena FaceIdentity son las fotografías que se almacenan en S3 y los resultados de las identificaciones de dichas imágenes que se almacenan en AWS RDS.

Información sobre AWS Rekognition. Con las tres fotografías iniciales el servicio construye un modelo biométrico a partir del análisis de los rasgos faciales de estas fotografías. AWS Rekognition almacena internamente estos datos biométricos en una colección. Cada vez que se llama a Rekognition se le envía una fotografía y este servicio extrae los metadatos y los compara con las del modelo original devolviendo a FaceIdentity el porcentaje de similitud. Amazon Rekognition no conserva los bytes de las imágenes reales.

KeyIdentity.

El servicio Keyidentity almacena matrices de datos con los tiempos de pulsación y vuelo de las diferentes teclas asociadas a cada usuario. Estos datos son almacenados en registros de una base de datos en AWS RDS (Relational Database Service).

Con estos datos se construye un modelo biométrico formado por tres archivos que está asociado a cada usuario. Estos modelos son almacenados en un bucket S3 de AWS.

Tecnologías Intervinientes

FACEidentity

FaceIdentity es por tanto un servicio que hace de interfaz entre el campus virtual, (capturando y almacenando las imágenes) y el servicio AWS Rekognition que realiza el análisis de las mismas.

Para el almacenamiento de los datos se utiliza AWS RDS como base de datos.

Para el almacenamiento de las imágenes se utiliza un bucket S3.

KeyIdentity

Para la construcción de los modelos biométricos se utiliza Deep Learning que es un modelo computacional basado en redes neuronales. Para la implementación de este desarrollo se han utilizado las librerías Keras y Tensor Flow.

Para el almacenamiento interno de las matrices de datos capturados se utiliza como base de datos AWS RDS.

Para el almacenamiento de los modelos se utiliza un bucket S3 de AWS.

Todos los datos están alojados en una cuenta de AWS Irlanda.

Actividades
FACEIdentity El servicio FaceIdentity tiene dos modos de funcionamiento: Identificación y monitorización. En la identificación FaceIdentity recibe una fotografía con el IdUsario al que se quiere identificar. La fotografía se procesa al api de Rekognition y es comparada con el modelo creado obteniendo el porcentaje de similitud. Este porcentaje es registrado en la base de datos RDS y a su vez se devuelve al campus como resultado una identificación positiva, negativa o incertidumbre. En la monitorización el sistema va recibiendo cada pocos segundos, imágenes a identificar, que son procesadas internamente por el api de Rekognition y los resultados registrados en la base de datos. En este caso no se devuelve al campus ninguna información en tiempo real. Es el campus quién solicita información sobre los resultados de esta secuencia de imágenes procesadas durante un examen. En este caso la información devuelta es el número de imágenes que no han superado la identificación en relación al total de imágenes capturadas en el examen. Si este valor está por encima de un umbral el resultado del examen se marca a REVISAR para que el supervisor pueda acceder al panel de supervisor de FaceIdentity y comprobar que ha sucedido tras una visualización manual de las fotografías capturadas. En caso contrario se considera que el comportamiento durante el examen ha sido el esperado y el examen queda autovalidado. En cualquier caso el supervisor puede acceder a la consola de Faceidentity y revisar las imágenes capturadas de cualquier examen. Consola de Supervisor Como hemos mencionado previamente el servicio FaceIdentity tiene una consola de Supervisión que muestra un listado con todos los usuarios registrados en el servicio y varios botones de acción con las siguientes funciones: Verificar.

Permite verificar el modelo biométrico. Para ello el supervisor debe comprobar que las 3 fotografías con las que se ha construido el modelo corresponden a la persona que se desea identificar.

Detalle.

Permite mostrar todos los registros de identificación de un usuario, mostrando la fecha y hora, el resultado de la identificación, y la fotografía si estuviera disponible (dado que se van eliminando según el periodo max de almacenamiento).

Resetear.

Permite eliminar el modelo biométrico del usuario de forma que en el próximo acceso le solicitará la creación de un nuevo modelo.

Eliminar.

Elimina completamente todos los datos registrados de un usuario.

Además, el servicio cuenta con una serie de parámetros de configuración para ajustarse a los requisitos de cada cliente.

Configuración

Para la parte de uso, se puede configurar los siguientes parámetros:

Configuración	Descripción	Posibles valores
Fotos de monitorización	Guardar las fotos.	-Todas -Solo las no positivas -Ninguna
Intervalo	Intervalo de tiempo en el cual se va a tomar una foto aleatoria en segundos.	-Valor numérico (30)
Permitir pasar fallos	En la pantalla previa al examen donde se validan los requisitos biométricos, permitir acceder al	-Permitir pasar -Repetir la foto

	examen, aunque el alumno no sea quien dice ser o no.	
Texto a mostrar	En la pantalla previa al examen donde se validan los requisitos biométricos, mostrar un texto informativo (útil para dar pautas al alumno antes de realizar un examen).	-Texto -No mostrar nada

Alertas

El servicio FACEidentity dispone de un sistema de alertas por correo electrónico. Este sistema de alertas se puede configurar para enviar un correo electrónico en el caso de que se detecte una suplantación de identidad.

También se pueden configurar alertas para controlar el número de identificaciones que se han realizado en cada servicio. Si las identificaciones superan un determinado límite se enviaría un correo avisando al supervisor de la plataforma de que se ha superado el límite. Estos correos son meramente informativos.

KeyIdentity

El servicio de KeyIdentity tiene solamente un modo de funcionamiento: monitorización.

Este servicio va recibiendo las muestras de tiempos capturadas a medida que el usuario va escribiendo y el buffer está completo (unos 70 caracteres como mínimo). Cada una de estas muestras recibidas es comparada con el modelo biométrico del usuario y tanto la muestra como el porcentaje de similitud obtenido es almacenado en un nuevo registro de la base de datos.

Consola de Supervisor

Como hemos mencionado previamente el servicio KeyIdentity tiene una consola de Supervisión que muestra un listado con todos los usuarios registrados en el servicio y varios botones de acción con las siguientes funciones:

Detalle.

Permite mostrar todos los registros de identificación de un usuario, mostrando la fecha y hora, el resultado de la identificación.

Eliminar.

Elimina completamente todos los datos registrados de un usuario.

DATOS TRATADOS

Las categorías de datos personales objeto de tratamiento son las siguientes:

- Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.

FaceIdentity

Los datos tratados por el servicio FaceIdentity son las fotografías tomadas de la webcam del usuario, el identificador asociado a cada persona, y el useragent como datos más relevantes.

Para el servicio FACEidentity, se utilizan las tablas USUARIOS y LOGS. En las tabla USUARIOS se guardan:

- El id biométrico
- El id externo del usuario
- El id del cliente
- El número de fotos que ha utilizado el usuario para entrenarse (0 no está entrenado, 3 si está entrenado)
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)
- Si el usuario está verificado (el cliente ha validado el perfil biométrico desde la consola de supervisor)

En la tabla LOGS, se almacenan los siguientes datos:

- El id de la identificación
- El id biométrico del usuario
- La fecha en la que se ha realizado la comprobación

- El porcentaje de similitud con cada una de las fotos del entrenamiento
- El resultado obtenido (positivo, negativo o incertidumbre)
- La prueba de vida a la que se ha sometido el usuario (gesto en la fotografía)
- Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
- El id enlazado, id de la anterior comprobación si sigue en la misma sesión
- Si la foto está almacenada o no.
- El user agent.
- El posicionamiento de la cara respecto a la cámara, para saber si el usuario está mirando a la pantalla o no.
- El tipo de registro (identificación o monitorización)

Keyidentity

Para el servicio keyidentity los datos que se tratan son las matrices de tiempos de cada usuario, el useragent, ip del usuario.

Para el servicio KEYidentity, se utilizan las tablas KEYSTROKE_USUARIOS_TEXTO y KEYSTROKE_LOGS_TEXTO.

En la tabla KEYSTROKE_USUARIOS_TEXTO se guardan:

- El id biométrico
- El id del cliente
- El id externo del usuario
- Si el usuario está entrenado o no
- El número de registros que lleva el usuario
- El porcentaje actual de identificaciones correctas y el porcentaje de intentos ilícitos detectados en una prueba interna que se realiza para comprobar su robustez.
- Si el usuario se ha marcado como sospechoso y un comentario de porque se ha marcado así.
- El identificador que el cliente quiera proveer para ver más fácilmente a sus usuarios en el panel (el cliente se hace responsable de compartir estos datos personales)
- Si el usuario tiene que contar para la facturación.

En la tabla KEYSTROKE_LOGS_TEXTO, se almacenan los siguientes datos:

- El id de la identificación
- El id biométrico del usuario
- Los datos de los tiempos de tecleo de la identificación
- El tipo de registro (entrenamiento o identificación)
- El porcentaje de similitud con el modelo entrenado
- La fecha en la que se ha realizado la comprobación
- Las etiquetas externas que le facilitan al cliente el posterior filtrado de los registros
- La IP, el navegador, el SO y la ciudad (basada en su IP) del usuario para saber de dónde vienen los datos
- El número de caracteres que tiene el registro
- Si la pantalla es táctil o no.
- El user agent.

QUIÉN TRATA LOS DATOS

El tratamiento se efectúa por la propia entidad responsable de tratamiento.

Asimismo, interviene ADR Infor S.L. proveedor que actúa en calidad de encargado de tratamiento.

TECNOLOGÍAS INTERVINIENTES

Política de seguridad de servicios biométricos.

Tecnología

Toda la tecnología utilizada en el proyecto está alojada en el cloud de Amazon Web Services.

El servicio en producción está alojado en AWS Irlanda y el plan de contingencia en AWS París.

Identificación de accesos al sistema

Autenticación por doble factor

Se ha establecido con carácter obligatorio la autenticación por doble factor para el acceso a la consola de supervisor de la plataforma a los servicios de identificación biométrica. Cada supervisor de la plataforma, aparte de disponer de unas claves únicas, tendrá que superar el reconocimiento

facial para poder acceder al panel de administrador. Si no supera dicha autenticación, el equipo de administradores de ADR recibe un correo alertando del intento de suplantación para poder tomar las medidas oportunas.

Dentro de ADR Formación, únicamente tienen acceso a dicho panel el equipo de administradores y solamente es utilizado para comprobar su correcto funcionamiento y dar soporte al cliente (IMFICE).

Logs de accesos al sistema.

Se guardan los logs de acceso al sistema durante un año. Estos logs se pueden analizar posteriormente si se ha detectado alguna irregularidad. En estos logs, se pueden filtrar los accesos de usuarios de la entidad gracias a que cada uno de ellos accede a través de un dominio diferente.

Los usuarios acceden a través de los dominios: faceidentity.adrformacion.com y keyidentity.adrformacion.com

El acceso a la consola de supervisor de la plataforma, en el acceso de administrador entran al dominio identify.adrformacion.com

Con estos logs, podemos realizar técnicas de análisis forense gracias a AWS Athena, un servicio de consultas interactivo que facilita el análisis de datos y permite verificar la legitimidad de los accesos.

Sistemas de seguridad

ADR Infor dispone de varias herramientas para la detección de intrusos y protección antimalware:

CLAMAV Es un antivirus que permite detectas troyanos, virus, malware y otras amenazas maliciosas.

WAF Es un firewall para aplicaciones web que nos ayuda a protegernos contra ataques web comunes que pueden afectar a la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. AWS WAF brinda control sobre cómo el tráfico llega a nuestras aplicaciones permitiéndonos crear reglas de seguridad que bloquean los patrones de ataque comunes, como la inyección de SQL o las secuencias de comandos entre sitios, y las reglas que filtran patrones de tráfico específicos que defina.

Cloudwatch con alarmas de umbrales definidas Es un servicio de monitorización y observación que ofrece datos e información procesable para monitorizar nuestra aplicación. Gracias a las alarmas definidas, podemos saber si hay cambios en los patrones de normalidad de uso del servicio.

DESTRUCCIÓN DE LOS DATOS

Actividades

Borrado automático de datos

FaceIdentity

Periodo de almacenamiento de fotografías.

Se ha programado un esquema para que INSTITUTO DE CIENCIAS EMPRESARIALES IMF pueda configurar los periodos de almacenamiento máximo para los diferentes tipos de imagen en cada configuración del servicio (identificación o monitorización). Transcurrido ese periodo de días, las imágenes son eliminadas de FaceIdentity.

ASIGNAR BORRADOFOTOS	
Cliente	ADR Formación
Identificación	
Positivas	15 días
Incertidumbre	90 días
Negativas	90 días
Gesto incorrecto	90 días
Foto no válida	90 días

Monitorización	
Positivas	15 días
Incertidumbre	90 días
Negativas	90 días
Foto no válida	90 días

Para la eliminación del modelo biométrico almacenado en AWS Rekognition IMFICE dispone de una consola para eliminar de forma manual todos los datos registrados del usuario.

KeyIdentity Periodo de almacenamiento. Se ha programado un esquema para que INSTITUTO DE CIENCIAS EMPRESARIALES IMF pueda configurar los periodos de almacenamiento máximo para las muestras de datos almacenadas en RDS. Transcurrido ese periodo los datos serán eliminados de manera automática. Para la eliminación del modelo biométrico almacenado en Keyidentity INSTITUTO DE CIENCIAS EMPRESARIALES IMF dispone de una consola que elimina todos los datos registrados del usuario.
Datos Tratados
Las categorías de datos personales objeto de tratamiento son las siguientes: - Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.
¿**Quién destruye los datos?**
Políticas automáticas definidas en el apartado anterior.
Tecnologías Intervinientes
Borrado automático de datos Si el responsable de tratamiento lo desea, puede guardar las imágenes para su posterior análisis, y para este caso, se ha programado un esquema para cada cliente en el que se pueden configurar los periodos de almacenamiento máximo para los diferentes tipos de imagen en cada configuración del servicio (identificación o monitorización). Transcurrido ese periodo de días, las imágenes son eliminadas definitivamente. Del mismo modo sucede con las matrices de tiempos registradas en el servicio KeyIdentity.

Cesión o transferencia de datos a terceros

Actividades
No están previstas cesiones, ni transferencias internacionales fuera del Espacio Económico Europeo
Datos Tratados
Las categorías de datos personales objeto de tratamiento son las siguientes: - Datos de categorías especiales: concretamente datos biométricos relativos al reconocimiento facial y dinámica del teclado.
Terceros involucrados
No aplica
Tecnologías Intervinientes
No aplica

6. ANÁLISIS DE LA OBLIGACIÓN DE REALIZAR UNA EIPD: EVALUACIÓN DEL RIESGO

a) Inclusión del tratamiento en la lista de tratamientos exentos

Se puede determinar que el tratamiento de datos personales objeto de análisis no encaja en ninguno de los supuestos previstos como exentos de realización de la EIPD en la lista publicada por la AEPD dado que no aplica ninguna de las circunstancias previstas.

b) Análisis de la inclusión del tratamiento en los casos de tratamientos obligados

Desde la entidad responsable de tratamiento sé es consciente de que los sistemas de verificación elegidos para comprobar la identidad de sus alumnos, requieren un alto grado de protección en tanto son objeto de tratamiento, datos biométricos (pertenecientes a las categorías especiales de datos a que se refiere el artículo 9) y además se emplean nuevas tecnologías.

Asimismo, el tratamiento objeto de análisis tiene cabida en el tercer caso de los enumerados en el artículo 35.3 del RGPD, en su apartado b: *"tratamiento a gran escala de las* categorías

especiales de datos a que se refiere el artículo 9”.Adicionalmente, el tratamiento coincide con uno de los supuestos incluidos en el listado publicado por la Agencia Española de Protección de Datos en virtud del art. 35.4 RGPD, en los que se requiere la realización de una Evaluación de Impacto relativa a la Protección de Datos. Concretamente se refiere a *“Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física”*

Por eso y de cara a garantizar la privacidad de los interesados afectados por el tratamiento de datos personales, se ha decidido llevar a cabo la actualización de evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo.

c) Evaluación del nivel de riesgo

De acuerdo con el artículo 35.7.c del RGPD, se ha realizado una Evaluación de Impacto del tratamiento de Reconocimiento Facial y Dinámica de Tecleo para determinar e identificar los elementos de riesgo para los derechos y libertades de las personas.

Derivado del análisis realizado, la organización ha establecido como Nivel de Riesgo aceptable todo aquello que supere el nivel Medio, entre los 5 niveles sobre los que se realiza la evaluación, por lo tanto, todo aquello con un nivel Alto o Muy alto debe ser tratado por la organización.

En este sentido, se han obtenido unos riesgos no asumidos por la entidad siendo los siguientes:

- Tratamiento Reconocimiento facial y dinámica de tecleo:
    - Dificultad para la revocación del consentimiento o la manifestación de la oposición a un tratamiento con riesgo Alto.
- ADR
    - Inexistencia de contrato/acuerdo con los términos requeridos por RGDP con riesgo Alto.
    - Problemas de comunicación de los eventos de seguridad con riesgo Alto.

d) Análisis de la necesidad del tratamiento

Una vez efectuado anteriormente con éxito el análisis de licitud del tratamiento, procede ahora entrar a valorar la necesidad del tratamiento, para lo que se examinan las cuestiones indicadas a continuación:

- **Justificación del tratamiento:** la implantación del tratamiento anteriormente descrito en Instituto de Ciencias Empresariales de IMF. S.L responde a la necesidad de garantizar, con el menor margen de error posible, que las personas que están cursando los estudios se corresponden efectivamente con aquellas que realizan los exámenes y pruebas online.

En este sentido, en la memoria de planificación de las enseñanzas se fija que la Universidad debe verificar fehacientemente que el alumno es quien desarrolla las pruebas de evaluación, ya sea en un examen de carácter presencial o mediante video conferencia. Asimismo, las competencias específicas establecen que los alumnos deben utilizar las tecnologías de la información y las comunicaciones para la búsqueda y obtención de información jurídica, así como herramientas de trabajo y comunicación.

De las reuniones de toma de datos para configurar el tratamiento, así como de las reuniones de valoración de riesgos efectuadas con la organización, se desprende que los datos se van a utilizar exclusivamente para la finalidad declarada y para ninguna otra no informada o incompatible con la legitimidad de su uso, dando cumplimiento así al principio de limitación de la finalidad.

- **Expectativas del afectado:** atendiendo a que el RGPD marca que la ponderación debe hacerse teniendo en cuenta la expectativa razonable de los interesados en función de su relación con el responsable, podemos concluir que se da total cumplimiento a este punto, en tanto al afectado por el tratamiento, en este caso, a los alumnos, les cabe esperar que los datos relativos a sus rasgos faciales y dinámica del tecleo serán objeto de tratamiento. Ello porque, al inicio del tratamiento, el interesado es debidamente informado de este tratamiento, así como de todos los aspectos relacionados con el mismo, y son accesibles para los alumnos los datos de contacto del Delegado de Protección de Datos, con quien pueden consultar ante cualquier cuestión que les surja en relación con el tratamiento de datos personales que se pretende realizar.

- **Grado de invasión en la privacidad de los interesados:** en este caso debemos analizar si la intrusión en la esfera de la intimidad de las personas es proporcional a la finalidad requerida. Pues bien, partiendo de la premisa de que los datos personales descritos únicamente serán objeto de tratamiento exclusivamente durante el tiempo en que el alumno esté haciendo uso del Campus, parece que dicho tratamiento de datos no resulta desproporcionado atendiendo a

la finalidad perseguida por el responsable de tratamiento, toda vez que además el mismo ha prestado su consentimiento.

- **Minimización de datos personales:** tras la realización del análisis de los datos tratados en el presente tratamiento, se desprende el cumplimiento de la organización con el principio de minimización de datos, ya que no existen datos que no se utilicen por los empleados autorizados, ni se recopilan datos que no tengan utilidad para la finalidad del tratamiento ni para los interesados afectados. La finalidad que se pretende lograr a través del presente tratamiento requiere de todos los datos objeto de tratamiento, ya que de lo contrario no sería posible la identificación unívoca del interesado y en consecuencia, no se podría determinar sin margen de error, que el alumno que realiza el examen es efectivamente aquel que se encuentra matriculado en el curso. Ello porque los métodos alternativos como tarjetas identificativas, contraseñas o similares podrían ser utilizados por otros individuos, dando lugar con ello a posibles suplantaciones de identidad.

- **Minimización del plazo de conservación:** en cumplimiento del principio de minimización del plazo de conservación, cabe mencionar aquí que los datos personales únicamente se conservarán durante el plazo estrictamente necesario para cumplir con la finalidad que se pretende.

En esta línea, y en cumplimiento del principio de responsabilidad proactiva, existe el pleno compromiso de la entidad en dar cumplimiento a las políticas de conservación implementadas que garanticen que los datos personales obtenidos sean suprimidos efectivamente. En este sentido, se conservarán los datos personales únicamente por el plazo concreto en el que el alumnado está cursando el estudio de máster o grado. Pasado este plazo, los datos personales serán suprimidos.

- **Accesibilidad:** en relación con las cuestiones relacionadas con la accesibilidad, es preciso destacar que estos datos personales no serán revelados a terceros no autorizados, ni siquiera a un gran número de personas dentro de ambas entidades. Únicamente podrá tener acceso el personal designado para ello y que concretamente será el personal de Secretaría Académica de Instituto de Ciencias Empresariales de IMF. S.L y el personal técnico de ADR formación, proveedor con quien se ha firmado el contrato de encargado de tratamiento.

- Medidas de seguridad: las tecnologías empleadas para el tratamiento son adecuadas para la finalidad establecida desde el punto de vista del cumplimiento de los principios fundamentales de la privacidad. Se aplican controles respecto de las tecnologías empleadas, para garantizar la

confidencialidad, integridad y disponibilidad de los datos personales de los usuarios gestionados durante el proceso.

Una vez analizados los aspectos más relevantes del tratamiento de datos personales cuyo análisis nos ocupa, es conveniente asegurar a continuación que el mismo supera con éxito el juicio de idoneidad y necesidad pertinente:

- **Juicio de idoneidad:** se puede concluir que la medida establecida cumple con el objetivo propuesto y que no es otro que el de garantizar que los alumnos que realizan los exámenes y pruebas online se corresponden con aquellos que se encuentran matriculados en el curso, verificando así su identidad de forma fehaciente e inequívoca.

- **Juicio de necesidad**: en este sentido, se puede afirmar que dicho tratamiento es necesario, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia, puesto que únicamente haciendo uso de datos biométricos es posible identificar unívocamente a las personas. Cualquier otro método que no utilice datos biométricos no cumplirá de forma fidedigna con dicho objetivo.

e) Beneficios para los interesados

En este apartado se pretenden identificar los beneficios directos para el conjunto de la sociedad, así como para los sujetos concretos sobre los que se tratan los datos personales.

El principal beneficio que obtiene el alumnado es poder realizar los exámenes cómodamente desde su casa, sin la necesidad de realizar traslados a la sede correspondiente que Instituto de Ciencias Empresariales de IMF. S.L tiene habilitadas para los exámenes presenciales, con el consiguiente ahorro de tiempo y dinero. Asimismo, la realización del examen en un entorno controlado reduce la presión a la que se ve sometido en situaciones imprevistas, lo que facilitará su concentración en la prueba.

Por otro lado, los exámenes online favorecen la calendarización de dichas pruebas, de tal modo que se puede ajustar con mayor precisión el momento de estudio y el de su evaluación, pudiendo ofrecer al alumnado la posibilidad de examinarse de la materia en el mismo mes que la cursa, favoreciendo así la evaluación continua. De igual modo, la realización de exámenes mes

a mes evita tener que presentarse el mismo día a diferentes exámenes, tal y como sucede actualmente en los exámenes presenciales.

Atendiendo a la movilidad geográfica, son muchos los alumnos que por diversas razones se ven obligados a cambiar de residencia a lo largo de los estudios, bien sea de ciudad o, incluso, de país. Esto genera problemas de desplazamiento al lugar de origen para poder realizar el examen o posponer los estudios hasta el regreso. Con la modalidad de exámenes online tiene la total garantía de que, esté en el lugar de mundo que esté, siempre podrá realizar los exámenes y completar sus estudios en el tiempo previsto.

f) Beneficios para la Entidad

Es preciso identificar en el presente apartado los beneficios que se derivan para la Entidad. En este sentido, es conveniente señalar que el principal beneficio que se deriva para la entidad con la implantación del tratamiento en cuestión es poder ampliar el público al que ofertar los servicios educativos. Eliminando la necesidad de acudir presencialmente a las sedes de la entidad, existe la posibilidad de contar con alumnos desde cualquier punto geográfico, tanto nacional, como internacional.

Cabe destacar también que este sistema permite a Instituto de Ciencias Empresariales de IMF S.L planificar mejor las enseñanzas, siempre en aras de que el alumnado consiga la mayor calidad en la formación con los mejores recursos tecnológicos, tal y como se espera de la aplicación de la biometría para la realización de exámenes en modalidad online.

Asimismo, se desea destacar que la implantación del sistema de verificación a través de reconocimiento facial y dinámica del tecleo resulta innovador en un sector educativo que debe apostar por las virtudes que traen consigo los avances tecnológicos.

Adicionalmente, y derivado de lo anterior, se obtendría por parte de la entidad una notable mejora reputacional en tanto Instituto de Ciencias Empresariales de IMF. S.L es pionera en la implantación de tan avanzada y ágil solución tecnológica.

g) Alternativas al Tratamiento y por qué no se han elegido.

El presente tratamiento se ha diseñado entendiendo el mismo como una mejora y extensión de un tratamiento ya existente en la entidad, que no era otro que el del seguimiento y evaluación

de los alumnos que cursan sus estudios en Instituto de Ciencias Empresariales de IMF. S.L como resultado de la relación contractual entre las partes.

Aunque ya se ha mencionado anteriormente, son múltiples las razones que justifican la modificación del tratamiento de cara a posibilitar la realización de los exámenes y pruebas de forma online, pero se desea a continuación incidir en las mismas:

- Mayor garantía de éxito derivado del sistema de evaluación continua.

- Reducción de costes derivados del desplazamiento para los alumnos.

- Reducción de esfuerzos para los alumnos.

- Innovación tecnológica.

- Máxima seguridad y garantías en la realización de exámenes.

- Mayor accesibilidad a los servicios ofrecidos por la entidad.

- Mejora reputacional de la entidad.

7. MEDIDAS PARA LA REDUCCIÓN DEL RIESGO

a) Optimización del tratamiento

El tratamiento se da durante todo el ciclo en el que la matricula está en vigor, ya que cada vez que el alumno acceda a la plataforma para realizar la evaluación continua, deberá hacer uso de los datos objeto del tratamiento.

Las fases que están definidas en el tratamiento son las siguientes:

- Aceptación durante el proceso de matriculación

- Creación del perfil biométrico al acceder a la plataforma

- Acceso y monitorización del uso de los datos biométricos

- Acceso a exámenes.

- Finalización del proceso de matrícula y borrado del perfil biométrico

b) Medidas PbDD

El Instituto de Ciencias Empresariales IMF tiene implantados unos controles operacionales y técnicos de manera permanente para la gestión de los datos de los interesados asociados a los cursos que se imparten, con el fin de garantizar la privacidad de los mismos. Los controles se describen a continuación:

Minimización

- **Eliminación temprana de los datos no necesarios**: el sistema de Faceidentity está adaptado para eliminar los datos biométricos a petición del usuario o por revocamiento de la autorización del uso de dichos datos. Asimismo, por parte de IMF existe la posibilidad de adoptar los plazos que se deben configurar de acuerdo a la política de plazos de conservación y supresión anteriormente detallada.
- **Minimización de los datos recogidos y tratados en cada etapa del tratamiento**: los datos personales que se recogen son únicamente los estrictamente necesarios para la finalidad que se pretende. En este sentido, se cuenta con dos identificadores. Un primer identificador interno que pertenece a cada usuario, junto a los datos biométricos y un identificador externo en el que se incluye únicamente nombre y apellidos.
- **Limitación de la accesibilidad de bases de datos a través de la red**: existe limitación en tanto las bases de datos se encuentran cifradas y protegidas por usuario y contraseña.
- **Seudoanonimización de los datos almacenados**: junto con los datos biométricos, se minimiza al máximo los datos personales. El único campo es el identificador externo donde el responsable de tratamiento es el que establece que información se incluye y que en este caso se trata de nombre y apellidos.

Ocultación

- **Seudoanonimización de los datos almacenados:** tal y como se indica anteriormente, junto con los datos biométricos, se minimiza al máximo los datos personales. El único campo es el identificador externo donde el responsable de tratamiento es el que establece.
- **Control de la privacidad de los metadatos en las comunicaciones electrónicas:** todos los datos personales se encuentran cifrados y se transmiten cifrados por canal seguro a través de https.
- **Uso de credenciales:** para acceder al servicio se utiliza un doble factor de autenticación compuesto, en primer lugar por usuario y contraseña, así como por un segundo control

con el uso de datos biométricos.

- **Cifrado de la información almacenada o en tránsito:** es preciso destacar que actualmente la base de datos se encuentra cifrada y se ha marcado como plazo la fecha de 15 de mayo de 2020, en la que las medidas de cifrado se extenderán también a las imágenes. Se cifrará el Buckets S3 que contienen los ficheros y la información biométrica. Asimismo, es preciso resaltar que los datos personales viajan en canal seguro.

Agregación

- **Generalización de datos personales:** los datos personales que se almacenan son mínimos. Tal y como se indicaba anteriormente, únicamente se almacenará el identificador externo e interno en los términos descritos.
- **Reducción de la precisión/granularidad de recogida de los datos**: Se conserva la IP y el agente de usuario (navegador desde el que se accede), que es precisamente la información que permite las verificaciones en la base de datos

Información

- Clausulas RGPD en condiciones generales del proveedor: el contrato de colaboración con ADR Infor S.L., recoge las condiciones generales del tratamiento de los datos según la normativa RGPD.

Aceptación de términos y condiciones (primera relación, acceso plataforma, realización examen): Se establece un procedimiento de aceptación de términos y condiciones del uso de datos biométricos en tres fases.

- En el proceso de matriculación
- En el acceso a la plataforma tecnológica
- A la realización del examen (recordatorio del acceso)

Política de privacidad: Se recogen las condiciones de uso de los datos personales en las cláusulas informativas destinadas a recabar el consentimiento de los interesados. Se adjunta a través del **Anexo IV**, un ejemplo de cláusula informativa en el momento de preinscripción del alumno, así como de solicitud de consentimiento en el momento de acceder al Campus política de privacidad propia de INSTITUTO DE CIENCIAS EMPRESARIALES IMF

Control

- Contrato RGPD: Acuerdo contractual con los alumnos que incluyen los requisitos necesarios para garantizar los derechos de los interesados, abarcando el derecho de información del tratamiento, consentimiento a la hora de gestionar los datos, acuerdos de confidencialidad, así como el método para ejercer los derechos como interesado.

- Formación usuarios: formamos a los usuarios en políticas de Compliance y uso de los datos sensibles contemplados en la RGPD.

- Auditorías internas: Establecemos auditorías internas y externas con el fin de garantizar la viabilidad de las medidas establecidas para el cumplimiento de los requisitos de RGPD .

Cumplimiento

Medidas disciplinarias/sanción: Se establecen procedimientos para el correcto uso de los datos y evitar intentos de fraude en el tratamiento de los datos biométricos .

Procedimiento para el tratamiento de la información: está establecido un procedimiento para el tratamiento de la información y para el correcto funcionamiento de la identificación del alumno a partir del perfil de datos biométricos.

Medidas de Accountability

- Procedimiento Alta/Baja/Modificación empleados y resto de usuarios: existe un procedimiento de altas y bajas para aquellos usuarios que tienen acceso al tratamiento de los datos de carácter personal, con un anexo que explica el uso de los datos sensibles.

- Usuarios nominales (no genéricos). Todos los perfiles que tienen acceso a datos de carácter sensible usan usuarios nominales, para garantizar la trazabilidad del acceso a los datos biométricos.

- Gestión de contraseñas (longitud, complejidad, caducidad). Tenemos una política de contraseñas cumpliendo los niveles de longitud y complejidad para garantizar que no sea fácil acceder suplantando la identidad de los usuarios, caducando la contraseña a los 90 días. Dicha contraseña no se puede repetir en un plazo inferior a un ciclo de 10 cambios.

- **Se cuenta con un DPD** que coordina y gestiona un departamento de protección de datos externo, compuesto por una consultora integral para el asesoramiento en materia de protección de datos y un abogado en ejercicio experto en protección de datos.

Medidas de Seguridad

- Gestión de Privilegios (asignación correcta de accesos): el acceso a los datos está controlado por una gestión de privilegios, garantizando que solo los usuarios que tengan autorización podrán acceder a los datos objeto del tratamiento.

- Copias de seguridad: como se ha explicado anteriormente, están establecidas políticas de backup de los datos y de los servidores donde se alojan los datos. Además se hacen pruebas de recuperación para garantizar que el proceso cubre las necesidad de la organización.

- Implantación de antivirus: como política de empresa, todos los equipos tienen instalado y actualizado al día el antivirus Microsoft Defender, gestionado desde los servidores de System Center.

- **Cifrado de la información almacenada o en tránsito**: es preciso destacar que actualmente la base de datos se encuentra cifrada y se ha marcado como plazo la fecha de 15 de mayo de 2020, en la que las medidas de cifrado se extenderán también a las imágenes. Se cifrará el Buckets S3 que contienen los ficheros y la información biométrica. Asimismo, es preciso resaltar que los datos personales viajan en canal seguro.

- **Pruebas de compatibilidad de software:** Se establecen pruebas de compatibilidad para el uso de la tecnología antes de cualquier actualización que garantice el correcto funcionamiento de las distintas plataformas existentes.

8. ANÁLISIS DEL BALANCE ENTRE RIESGO-BENEFICIO

Una vez realizado con éxito el juicio de proporcionalidad y necesidad del tratamiento objeto de análisis, así como habiendo asegurado que se encuentran implantados los controles y medidas de seguridad necesarios para garantizar que el tratamiento no supone una medida restrictiva para los derechos fundamentales de los interesados, se puede determinar que el tratamiento es ponderado y equilibrado, ya que, como se ha podido desarrollar a lo largo del presente informe, se derivan más beneficios y ventajas para los interesados que perjuicios.

Plan de acción

En base a los riesgos identificados en el apartado VII Análisis de la Obligación de realizar una EIPD: Evaluación del riesgo, se ha establecido el siguiente plan de acción para mitigar los riesgos obtenidos:

- Tratamiento Reconocimiento facial y dinámica de tecleo:
    - Dificultad la revocación del consentimiento o la manifestación de la oposición a un tratamiento para el que se aplica el siguiente control:
        - Información al alumno: Informar al alumno que si revoca el tratamiento de datos biométricos pierde su opción a evaluación continua, derivando a 2 evaluaciones anual como marca la norma académica. Responsable Pablo Perancho, Plazo de ejecución Marzo 2020.
- ADR
    - Inexistencia de contrato/acuerdo con los términos requeridos por RGDP para el que se aplica el siguiente control:
        - Documentar Anexo Datos Biométricos (ADR) con las medidas de seguridad y protección de los datos de los alumnos. Responsable Pablo Perancho, Plazo de ejecución Marzo 2020.
    - Problemas de comunicación de los eventos de seguridad para el que se aplica el siguiente control:
        - Procedimiento Brechas de Seguridad: Disponer de un procedimiento de brechas de seguridad, con los tiempos de respuesta correctamente definidos. Este procedimiento debe ser comunicado y entendido por el

proveedor del servicio. Responsable Pablo Perancho, Plazo de ejecución Marzo 2020.

Al margen de estas medidas para tratar los riesgos no asumidos, se aplican medidas desde el diseño tales como:

- Autenticación por doble factor.
- Logs de accesos al sistema.
- Borrado automático de datos.
- Política de backups.
- Plan de recuperación ante desastres.
- Antivirus CLAMAV.
- Firewall de Aplicaciones Web (WAF).
- Cifrado https.

9. CONCLUSIONES Y RECOMENDACIONES

Es preciso destacar aquí, que por parte de la entidad Instituto de Ciencias Empresariales de IMF S.L. (en adelante IMFICE), en el mes de septiembre de 2019 se realizó con éxito una prueba piloto del tratamiento descrito a lo largo del presente documento. La mencionada prueba piloto consistió en la realización de exámenes a través del sistema de verificación biométrico. Concretamente, se efectuó en el grado de ADE y Derecho que Instituto de Ciencias Empresariales de IMF. S.L. oferta y afectó a un total de 10 alumnos en el Grado de ADE y 60 en el Grado Derecho.

Se desea dejar constancia de que en todo caso, en virtud del principio de responsabilidad proactiva y de privacidad desde el diseño y por defecto, se dio cumplimiento a lo dispuesto en el RGPD, así como en la LOPDGDD. Entre otras se llevaron a cabo las siguientes acciones:

- Análisis exhaustivo sobre la licitud del tratamiento
- Configuración del registro de actividades
- Elaboración de las cláusulas informativas destinadas a recabar el consentimiento del interesado
- Realización de la EIPD
- Implantación de las medidas y controles de seguridad tendentes a asegurar la privacidad de los interesados

Y actualmente se ha establecido un nuevo plan de acción sobre el tratamiento al fijar un plazo para el cifrado de las imágenes.

En virtud de lo anteriormente expuesto, cabe destacar que como resultado de la realización de la presente EIPD, se ha podido determinar que no existe un riesgo alto para los derechos y libertades de los interesados en tanto se contaban con las medidas y controles suficientes y el alcance es claramente acotado. Se valora positivamente poder abrir a otros estudios del Instituto de Ciencias Empresariales de IMF. S.L. un procedimiento de verificación de identidad de los alumnos combinando las técnicas de reconocimiento facial y de reconocimiento de patrón de tecleo.

En ……. a …… de ……. de 2020

Firma en nombre de la entidad responsable del tratamiento

ANEXO I: DETALLE DE PREGUNTAS GENERALISTAS DESTINADAS A LA CONFIGURACIÓN DEL PERFIL BIOMÉTRICO.

Para la creación del modelo biométrico basado en patrones de tecleo se utilizan siete textos que el usuario debe escribir mediante el uso del teclado. Dado que los ritmos de tecleo son ligeramente diferentes cuando un usuario se limita a copiar un texto que cuando está escribiendo fruto de algo que ha pensado se somete al usuario a una serie de preguntas intrascendentes en las que deba razonar una respuesta.

Es importante destacar que las respuestas que teclea el usuario no se almacenan, solamente se miden los ritmos de tecleo.

Las preguntas a las que el usuario debe responder para crear el patrón de tecleo son estas:

- ¿Qué es y para qué sirve una taza?
- ¿Qué es y para qué sirve un bolígrafo?
- Describe el argumento de la última película que has visto.
- ¿Qué es un arco iris y qué colores tiene?
- Describe algunos elementos de una vivienda.
- Describe algunos elementos de un coche.
- Describe lo que puedes encontrar en un campo de fútbol.

COMPROMISO DE CONFIDENCIALIDAD PARA LOS TRABAJADORES

El abajo firmante, en el marco de la relación laboral que le une con INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., puede tener acceso a recursos donde se contiene información relativa a datos de carácter personal de personas físicas, en su virtud se compromete a:

1. No revelar a persona alguna ajena a INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., sin su consentimiento, cualquier información a información (entendiéndose por tal toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada) referente a la que haya tenido acceso en el desempeño de sus funciones en INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o de la entidad impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

2. Utilizar la información a que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., y no disponer de ella de ninguna otra forma o con otra finalidad. Mantener en el más estricto secreto toda la información que pueda llegar a su conocimiento como consecuencia de su profesión y del desempeño de sus funciones dentro de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., comprometiéndose a no divulgarla, publicarla, cederla, revelarla ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. que no estén autorizados a acceder a la citada información, cualquiera que sea el soporte en el que se encuentre la información.

3. Acceder a la información contenida tanto en los sistemas informáticos como en cualquier otro soporte, en papel, electrónico o telemático, sólo si tal acceso fuera necesario para la prestación de los servicios. No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de trabajador de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., y que no sea necesaria para el desempeño de sus funciones en la misma.

4. Cumplir, en el desarrollo de sus funciones en INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., la normativa vigente, nacional y comunitaria, relativa a la protección de datos de carácter personal y, en particular, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos – RGPD) y disposiciones complementarias o cualquier otra norma que las sustituya en el futuro, estando obligado por ello al deber de secreto en virtud del artículo 5.1 f) de la citada normativa.

5. Devolver a INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. todas las copias o documentos, independientemente del soporte en el que se encuentren, relativa a la información a la que haya tenido acceso como consecuencia de los servicios prestados sin necesidad de requerimiento.

6. Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L.

7. El acceso a los recursos puestos a disposición del trabajador por parte de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., tales como teléfono móvil, PDA, portátil, Internet, teléfono, fax, correo electrónico, fotocopiadora, o escáner se considerará como un privilegio que está condicionado a la aceptación de este Compromiso. La anterior enumeración se hace sin carácter limitativo y se hará extensiva a cualquier otro recurso que la empresa ponga en disposición del trabajador, de forma que éste autoriza a que INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., efectúe los controles necesarios para verificar el correcto desarrollo de sus obligaciones laborales por los medios técnicos oportunos, incluyendo la monitorización de los sistemas de información. El trabajador, por su parte, se compromete a efectuar un uso

adecuado a sus obligaciones laborales y el tratamiento que, por el puesto a desarrollar, deba efectuarse, en la medida en que la calidad de los servicios prestados por INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. depende en su mayor parte de la responsabilidad individual de los usuarios.

8. Sin perjuicio de que se apliquen obligaciones similares a todos los recursos de la empresa, en relación con el correo electrónico, el trabajador es el único responsable de las actividades realizadas con el buzón de correo (o buzones) de los que le haya provisto INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. El servicio de correo debe ser destinado únicamente a un uso laboral aunque excepcionalmente podría ser utilizado para fines personales siempre que no afecten al rendimiento del servicio en perjuicio de la empresa y las ocasiones sean puntuales. No se debe permitir el uso de la cuenta a personas no autorizadas y no se podrán instalar cuentas de correo de proveedores externos en los sistemas de información de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. En los envíos masivos de información, se utilizará el campo de copia oculta (CCo), especialmente si se trata de envíos comerciales o cualquier otra situación en la cual las direcciones de correo electrónicas de personas o empresas distintas pudieran quedar visiblemente expuestas el resto de destinatarios. En los casos en los que un correo electrónico resultara sospechoso de contener un virus, no se abrirá y se consultará con los responsables de los sistemas de información. En general, se prohíbe el uso del correo con intereses ajenos a los de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L., así como participar en cadenas de e-mails, difundir contenidos ilegales (tales como piratería, pornografía, virus, fraudes, entre otros) o enviar mensajes que comprometan la reputación de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. a foros, blogs u otras listas de distribución.

9.- En relación con el uso de la red de Internet, el trabajador es el único responsable de las sesiones iniciadas en Internet desde su puesto de trabajo, siendo considerado su uso como estrictamente laboral, estando prohibido con fines distintos. En concreto no se podrán modificar las configuraciones de los navegadores del equipo ni la activación de servidores o puertos sin autorización de los responsables de los sistemas de información. No se podrán utilizar imágenes, sonido o videos para fines ajenos a la actividad laboral de la empresa, debido a que el tamaño de estos archivos satura los canales de comunicación y disminuye la velocidad de transmisión perjudicando al funcionamiento de la red en su conjunto. Además, se prohíbe expresamente el acceso, la descarga y el almacenamiento en cualquier soporte, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres, así como el uso de canales de chat cualquier que sea su proveedor o páginas webs de juegos en línea o dispositivos similares. INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. colaborará con en cualquier investigación contra este tipo de actos o cualquier otra utilización ilegal con las Fuerzas y Cuerpos de Seguridad del Estado así como con la Administración de Justicia.

La obligación general señalada anteriormente será complementaria con los deberes de secreto profesional que les apliquen.

El abajo firmante entiende que en este sentido asume una obligación laboral específica, y que en caso de incumplirla, dicho incumplimiento podrá ser motivo de despido por justa causa, generándose además a favor de INSTITUTO DE CIENCIAS EMPRESARIALES IMF S.L. una acción judicial por cualquier daño o perjuicio que pudiera derivarse para el mismo y/o a terceras personas derivado del incumplimiento de los compromisos anteriores.

Y para que surta plenos efectos, firmo la presente declaración.

En a de de 201_

EMPLEADO CARGO

D.N.I. FIRMA

CELA OPEN INSTITUTE (COI) Nº 01/18

Contrato de LCMS para creación, gestión e impartición de formación online

COMPARECEN

De una parte, **D. José Luis Del Rincón Ruiz** con D.N.I. **16557974-K**, representante legal de **ADR Infor S.L.** con C.I.F. nº **B-26265835** y domicilio social en **Avda. Vara de Rey 41 bis. 8º Of. 6 de Logroño, 26002 La Rioja, España** (en adelante, "**ADR Formación**").

De otra parte, **D. Antón Miret Serra** con D.N.I. **35042220H** representante legal de **CELA OPEN INSTITUTE, S.L.** con C.I.F. nº **B-86344108** y domicilio social en **calle Costanilla de San Pedro, 2 – 28005 Madrid** (en adelante, **"el cliente"**).

Ambas partes, ADR Formación y el cliente, están interesados en formalizar el presente CONTRATO, reconociéndose capacidad legal suficiente para hacerlo y aceptando los términos y condiciones establecidos en las siguientes

CLÁUSULAS

1ª.- OBJETO DEL CONTRATO

El siguiente contrato tiene por objeto regular las condiciones en las que el cliente solicita y ADR Formación presta el servicio de **LCMS que incluye portal web personalizado, alquiler de plataforma eLearning y explotación del sistema de autor** por parte del cliente, con las características descritas en el presente contrato, así como la determinación de las condiciones y forma de remuneración del cliente a ADR Formación por el servicio prestado.

2ª.- DESCRIPCIÓN DEL SERVICIO

2.1 Alquiler y administración de la plataforma

El servicio de **Alquiler de Plataforma ó LCMS (Learning and Content Mangement System)** se ajustará a las siguientes características:

a) ADR Formación desarrollará un portal eLearning personalizado acorde con la imagen corporativa del cliente desde donde se accederá a la plataforma.

b) La plataforma estará alojada en el cloud de AMAZON (Irlanda), por lo que el mantenimiento del sistema, copias de seguridad y actualizaciones de las herramientas del LCMS son competencia exclusiva de ADR Formación.

c) La plataforma estará operativa de forma ininterrumpida. Si se produjera una interrupción de servicio motivado por fallo del proveedor de cloud, ADR Formación propondrá soluciones alternativas en un plazo no superior a 48 horas.

d) El cliente dispondrá de las herramientas necesarias para la gestión de la plataforma. Se crearán los perfiles necesarios con las herramientas que el cliente precise.

e) El cliente dispondrá de formación en el uso y manejo del sistema para los distintos perfiles.

f) El aula virtual será configurada por ADR Formación, siendo sus solapas personalizables para cada acción formativa por el propio cliente.

g) El cliente podrá activar el motor de voz que la plataforma incorpora sin coste adicional.

h) El cliente podrá utilizar el entorno de comunicaciones integrado (solapa Llamadas) sin coste adicional.

i) El cliente podrá utilizar servicios de comunicaciones de terceros integrables en la plataforma (Adobe connect, Gootomeeting, Webex) cuyos costes de licencia no están incluidos en este contrato.

j) ADR Formación supervisará y asegurará la capacidad técnica del sistema. Para resolver incidencias el cliente dispone de la herramienta de **HELP DESK** en la plataforma, donde se recogerán los tickets de soporte oportunos. Estos tickets serán atendidos en un plazo inferior a 24h laborales por el equipo técnico de ADR Formación.

k) El cliente será responsable de la matriculación de alumnos a través de las diferentes herramientas disponibles para ello.

l) El cliente será responsable del seguimiento, coordinación y supervisión de las acciones formativas.

m) La plataforma es multiproyecto, lo que permitirá al cliente la contratación de proyectos paralelos, que compartirán infraestructura tecnológica pero que serán independientes entre sí.

2.4 Sistema de Autor

ADR Formación pondrá a disposición del cliente el **Sistema de Autor** de la plataforma para la creación de nuevos cursos:

a) El Sistema de Autor es un conjunto de herramientas del LCMS que permite la creación y publicación de contenidos online por parte del cliente.

b) Los contenidos generados por el cliente serán propiedad del cliente y registrados a su nombre o del autor. ADR Formación no será propietaria de contenidos desarrollados por sus clientes.

c) ADR Formación ofrece al cliente de forma gratuita cursos online tutorizados para que sus empleados puedan desarrollar contenidos adecuados y explotar todas las posibilidades que la plataforma ofrece.

d) Los contenidos del cliente serán tutorizados por personal del cliente. ADR Formación no contempla la tutorización para contenidos ajenos a su catálogo.

e) Los contenidos generados por el cliente sí pueden ser impartidos sin tutorización si el cliente así lo considera.

f) El cliente dispondrá de un espacio de almacenamiento para la realización de cursos propios, establecido en la cláusula 4ª IMPORTE Y CONDICIONES DE PAGO del presente contrato.

g) Los contenidos desarrollados por el cliente serán exportables en formato SCORM.

h) El cliente podrá disponer de herramientas de exportación, control y gestión de licencias SCORM de su propio contenido.

3ª - COMPATIBILIDAD DE LA PLATAFORMA CON CONTENIDOS DE TERCEROS

La plataforma de ADR Formación es compatible con contenidos SCORM. Esto significa que es capaz de interpretar un contenido SCORM y mostrarlo, así como registrar los datos que el contenido SCORM reporte.

Los contenidos creados mediante el sistema de autor de la plataforma se pueden exportar en formato SCORM

4ª.- IMPORTE Y CONDICIONES DE PAGO

4.1 Condiciones

Como contraprestación de estos servicios, el cliente se compromete a abonar las siguientes cantidades en tiempo y forma establecidos:

Portal web y LCMS	Importe
Implantación de LCMS que incluye: • Dos Campus Personalizados alojados en las url: https://campus.coi.es/ https://campusvirtual.coi.es/ • Aula Virtual • Motor de voz • Comunicación en tiempo real integrada • Sistema de Autor • Herramientas para itinerarios/másters • Herramienta de exportación/Importación SCORM y control de licencias exportadas	(Sin coste por reedición)
Plataforma, precio anual, que incluye: • Hosting de alta disponibilidad • Mantenimiento del LCMS • Hasta 5.000 altas entre ambos campus	13.500 € (1.125 €/mes)
Exceso matrículas anuales: • Hasta 10.000 altas	1,30 €/alta
Capacidad almacenamiento datos: Hasta 50 GB (entre ambos campus)	Sin coste
Exceso GB a partir de 50 GB	1,10 €/GB/mes

Formación en el uso del sistema	Importe
Curso de iniciación al desarrollo de contenidos	Sin coste
Curso de especialista en desarrollo de contenidos	Sin coste
Curso de tutor online	Sin coste
Curso de supervisor/administrador	Sin coste

Equipo Técnico*	Importe
horas de soporte (tarifa vigente 2018)	50 €/hora (en fracciones de 30min)
Bolsa de horas adicional (25Horas)	1.125 €
Bolsa de horas adicional (50 Horas)	2.000 €
Bolsa de horas adicional (100 Horas)	3.500 €
Bolsa de horas adicional (150 Horas)	5.250 €
Bolsa de horas adicional (500 Horas)	15.000 €

* Las horas del equipo técnico serán facturadas con cargo a las bolsas de horas adquiridas o bien según la tarifa vigente. En este concepto se tendrán en cuenta todas aquellas horas que el equipo de ADR Formación invierta en el desarrollo de trabajos para el cliente (a modo de ejemplo: formación en el uso del sistema más allá de la formación incluida, soporte a autores, supervisores o tutores en el uso de la plataforma, desarrollos de herramientas a medida, diseño). En ningún caso se cobrarán los trabajos derivados de un mal funcionamiento de la plataforma, mejoras que ADR Formación decida implementar, elaboración de presupuestos o atención comercial. En este sentido ADR Formación será totalmente transparente para que el cliente conozca en cada momento el concepto por el que es facturado y puede solicitar previamente un presupuesto o estimación de horas a consumir.

Consumo SMS	Importe/sms
En caso de activar el servicio, se facturarán los sms enviados. En ningún caso se facturan los sms enviados a los tutores de ADR Formación	0,15 €/sms

4.2 Sistema de facturación automático

La facturación se realizará con una periodicidad mensual. Todos los servicios facturados están sujetos al Impuesto sobre el Valor Añadido al tipo vigente en cada momento, salvo el servicio de Tutorización que está exento de IVA en virtud del artículo 20.UNO.9º de la Ley 37/92 de IVA.

La plataforma de ADR Formación incorpora un **sistema de facturación** mediante el que el cliente podrá comprobar en tiempo real los datos provisionales de las facturas del mes en curso, así como acceder a los datos de las facturas de meses anteriores. El cliente **da su conformidad mediante la firma de este contrato para no recibir la factura en formato papel y muestra su compromiso a imprimirla desde la herramienta "Facturación" de la plataforma.**

Las facturas serán abonadas **mediante transferencia bancaria**. El cliente se compromete a descargar las facturas emitidas y realizar el abono mediante **transferencia bancaria a 30 días fecha factura, siendo el día 10 el día de pago establecido.**

DATOS PARA EL ABONO DE LAS FACTURAS:

Titular de la cuenta: ADR INFOR, S.L.

Entidad bancaria: BANKIA

Nº Cuenta: ES33 2038 7490 1160 0001 6875

ADR Formación comunicará al cliente cualquier cambio en los datos facilitados para el pago con al menos una semana de antelación. El cliente se compromete a realizar los pagos en el tiempo y forma establecidos, sin demoras ni excepción.

5ª.- DURACIÓN DEL CONTRATO Y RESOLUCIÓN CONTRACTUAL

5.1 Duración del contrato

El presente contrato entra en vigor el día 01 enero 2018 y tiene validez hasta el día 31 diciembre de 2018, renovándose tácitamente por periodos anuales (año natural), si ninguna de las partes expresa su deseo de terminación con al menos un mes de antelación.

5.2 RESOLUCIÓN CONTRACTUAL

Son causas de resolución del presente contrato las siguientes:

a) El transcurso del plazo de duración del contrato en los términos previstos en la Cláusula 5.1. anterior.

b) El mutuo acuerdo de las partes.

c) El incumplimiento por ADR Formación de las obligaciones asumidas en relación con la prestación de servicios objeto del presente contrato de acuerdo con lo dispuesto en la Cláusula 2ª anterior.

d) El incumplimiento por el cliente de las obligaciones de pago asumidas en virtud del presente contrato de acuerdo con lo establecido en la Cláusula 4ª.

e) El uso malicioso por el cliente de las herramientas puestas a su disposición en virtud del presente contrato, o la realización por el cliente de prácticas malintencionadas que pudieran repercutir en la seguridad del sistema.

f) La realización por el cliente de prácticas de competencia desleal con los clientes de ADR Formación.

Cada una de las partes responderá frente a la otra por los daños y perjuicios causados como consecuencia del incumplimiento de sus obligaciones asumidas en virtud del presente contrato.

En caso de resolución del contrato por las causas señaladas en los apartados a), b) y c) anteriores, ADR Formación se compromete a ejecutar el **Plan de Continuidad de Negocio** en la modalidad denominada "**transferencia ordenada**" que se especifica en el Anexo I del presente contrato.

6ª.- PROPIEDAD INTELECTUAL E INDUSTRIAL

El cliente reconoce los derechos de propiedad intelectual y, en su caso, industrial, de ADR Formación sobre el resultado de sus labores de análisis, programación, reparación, formación y adaptación del portal web de teleformación desarrollado: los entornos de formación, aula virtual, campus y herramientas que conforman el LCMS.

7ª.- CONFIDENCIALIDAD Y POLÍTICA DE PROTECCIÓN DE DATOS

Tanto ADR Formación como el cliente se comprometen a no divulgar la información confidencial referente a la otra parte de la que hayan tenido conocimiento por razón de la ejecución del presente contrato y a mantenerla en secreto, incluso después de la finalización del mismo.

En cumplimiento del artículo 12.2 de la Ley Orgánica 15/99 de Protección de Datos Personales (LOPD) ADR Formación tratará toda información propiedad del cliente de forma estrictamente confidencial, tomando las

medidas necesarias para que su contenido no se divulgue a terceros, ni éstos puedan tener acceso a los mismos sin autorización expresa del cliente, garantizando expresamente el cumplimiento del deber de secreto (Art. 10 LOPD) en relación con los asuntos y datos del cliente, ADR Formación tratará los datos facilitados por el cliente de conformidad con las finalidades y los usos previstos en el presente contrato y se obliga a no utilizarlos para un fin distinto, salvo cuando así le sea indicado por el cliente.

ADR Formación se obliga igualmente a no comunicar los datos de carácter personal facilitados por el cliente ni siquiera para su conservación, a otras personas distintas de las que son parte en el presente Contrato, salvo que sea requerido a ello por una autoridad competente.

Una vez finalizada la relación entre ambas partes, ADR Formación devolverá o destruirá, a indicación del cliente, todos los datos de carácter personal al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del servicio establecido en este contrato.

ADR Formación declara tener implantadas las medidas de seguridad que son requeridas por la vigente legislación de protección de datos, en concreto las establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, donde se recogen las Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. Asimismo, en lo relativo a los datos facilitados para el cumplimiento de las actividades objeto del presente contrato ADR Formación aplicará las medidas correspondientes al nivel básico, las cuales se encuentran recogidas en un documento de seguridad debidamente actualizado.

8ª.- CARÁCTER MERCANTIL DE LA RELACIÓN CONTRACTUAL

El presente contrato tiene carácter mercantil, no existiendo vínculo laboral alguno entre el cliente y el personal de ADR Formación que pueda prestar sus servicios para el cliente en cumplimiento del presente contrato.

9ª.- LEGISLACIÓN APLICABLE Y TRIBUNALES COMPETENTES

Ambas partes se comprometen a resolver, de manera amistosa, cualquier desacuerdo que pueda surgir en la interpretación o ejecución de este contrato. En caso contrario será de aplicación la legislación española y ambas partes se someterán a los Juzgados y Tribunales de la Ciudad de Logroño con renuncia a su propio fuero, si éste fuese otro.

Ambas partes aceptan los términos y las condiciones expuestos en el presente contrato, y para que así conste firman a 22 de enero de 2018.

Fdo.: D. José Luis Del Rincón Ruiz
Cargo: Representante Legal

ADR INFOR, S.L.

Fdo.: D. Antón Miret Serra
Cargo: Representante Legal

CELA OPEN INSTITUTE

Anexo I. Plan de continuidad de negocio

ADR Formación como proveedor de tecnología es consciente de la importancia que tiene el servicio que ofrece en los modelos de negocio de sus clientes. Con el objeto de minimizar los posibles inconvenientes que pudieran surgir del hecho de dejar de utilizar la tecnología de ADR Formación se redacta el siguiente plan de continuidad de negocio.

En atención a las circunstancias que concurran en el momento de resolución contractual por las causas señaladas en los apartados a), b) y c) de la Cláusula 5ª anterior, se aplicará el proceso denominado "**transferencia ordenada**".

Transferencia ordenada

Por transferencia ordenada se entiende el proceso por el cual el cliente puede migrar su negocio de la mejor manera posible de la plataforma de teleformación de ADR Formación a otra plataforma de teleformación.

En caso de resolución contractual por las causas señaladas en los apartados a), b) y c) de la Cláusula 5ª anterior, el presente contrato se entenderá prorrogado en las condiciones económicas vigentes en el momento de resolución contractual por el periodo necesario para extinguir las acciones formativas activas, con un periodo máximo de 2 años a contar desde la fecha de resolución que deberá ser notificada al cliente.

El cliente no podrá iniciar nuevas acciones formativas durante el período de transferencia ordenada.

Durante el período de prórroga citado, ADR Formación continuará prestando los servicios pactados con el fin de facilitar la migración a realizar por el cliente.

En caso de que la migración vaya a implicar la prestación de servicios no contenidos en el contrato, deberán pactarse expresamente estos servicios.

Infraestructura propia

En caso de que ADR Formación no pueda continuar prestando sus servicios a CELA OPEN INSTITUTE por causas de fuerza mayor o por cualquier otra circunstancia que haga imposible que el actual equipo gestor pierda la capacidad de explotar la plataforma, ADR Formación podrá segregar la plataforma actual del cliente, con todos los contenidos del cliente, alumnos y personalizaciones, generando una instancia de la misma en una infraestructura gemela e independiente en AMAZON.

El proceso de segregación se realizará en un plazo máximo de 15 días hábiles y tendrá un coste de 6.000 €.

A partir de la fecha de entrega de la infraestructura propia el cliente se hará cargo de los costes de hosting (AMAZON) así como de la gestión de la plataforma de teleformación.

El cliente adquiere una licencia de uso y modificación de la plataforma, por un plazo mínimo de 20 años, cuyo coste es el especificado en el contrato de la empresa principal del grupo, IMF International Business School, para todos los proyectos asociados.

El cliente podrá actuar sobre la plataforma de teleformación adaptándola a sus necesidades y para su uso exclusivo, no pudiendo comercializar la plataforma a terceros.

COMPROMISO DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ENTRE RESPONSABLE Y ENCARGADO DEL TRATAMIENTO ADENDA MODIFICATIVA AL CONTRATO DE LCMS PARA CREACIÓN, GESTIÓN E IMPARTICIÓN DE FORMACIÓN ONLINE SUSCRITO ENTRE CELA OPEN INSTITUTE, S.L. (AHORA INSTITUTO DE CIENCIAS EMPRESARIALES IMF, S.L.)

En Madrid, a 8 de enero de 2019

REUNIDOS

De una Parte,

Instituto de Ciencias Empresariales IMF, S.L. (en adelante, el "cliente" o "Responsable del Tratamiento"), con domicilio en C/ Costanilla De San Pedro 2 28014 - Madrid y provista de CIF: B86344108 representada en este acto por D. Carlos Martínez Domínguez titular del D.N.I. 22144543M, actuando en su calidad de Representante.

Y de otra,

ADR Infor S.L. (en adelante, "Proveedor" o el "Encargado del Tratamiento"), con domicilio en Avda. Vara de Rey 41 bis.8º Of.6 de Logroño, 26002 La Rioja y provista de CIF: B86344108 representada en este acto por D. José Luis del Rincón Ruiz titular del D.N.I. 16557974K, actuando en su calidad de Representante.

A los efectos del presente documento, el Responsable del Tratamiento y el Encargado del Tratamiento podrán ser designados conjuntamente como las "Partes", e individual e indistintamente como la "Parte".

Ambas Partes, reconociéndose mutuamente capacidad legal suficiente para contratar y obligarse mediante este documento, y manifestando los comparecientes tener vigentes sus poderes y ser suficientes para obligar a sus representadas, y a tal efecto,

MANIFIESTAN

I. Que las Partes suscribieron en fecha 22 de enero de 2018 un Contrato de LCMS para Creación, Gestión e Impartición de formación online (en adelante, el "Contrato") el cual sigue vigente. En virtud de este, el Responsable del Tratamiento encargó determinados servicios al Encargado del Tratamiento.

II. Que, las Partes están interesadas en realizar una novación modificativa no extintiva del Contrato, a los efectos de adaptar el mismo a las obligaciones regulatorias relativas a la protección de datos de carácter personal derivadas del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

III. Que, expuesto cuanto antecede, las Partes, de mutuo acuerdo, libre y espontáneamente, convienen en suscribir la presente Adenda modificativa y no extintiva al Contrato (en adelante, la "Adenda"), y ello, de conformidad con los siguientes:

CLÁUSULAS

PRIMERA.- NOVACIÓN MODIFICATIVA NO EXTINTIVA DEL CONTRATO

Las Partes expresamente acuerdan sustituir en su totalidad la Cláusula 7ª "Confidencialidad y Política de protección de datos" del Contrato, e incorporar el anexo correspondiente, quedando éstos redactados del tenor literal que sigue:

1.1. Objeto

Mediante las presentes cláusulas se habilita a la entidad encargada del tratamiento, para tratar por cuenta del responsable del tratamiento, los datos de carácter personal necesarios para prestar los servicios objeto del contrato, así como para la integración de sistemas de identificación biométrica y desarrollo de módulo de exámenes.

1.2. Duración

El presente acuerdo tiene la misma duración que el Contrato de Servicios profesionales al que acompaña.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

1.3. Titularidad de los datos

El tratamiento de datos automatizados o no de carácter personal será responsabilidad del CLIENTE, quien mantendrá dicha titularidad en todo momento, con las modificaciones que sufran como consecuencia de sus actualizaciones, altas, bajas y modificaciones.

Así, en todo momento EL CLIENTE conservará el derecho exclusivo de propiedad y uso de los datos y todos sus procesos de actualización.

1.4. Tratamiento de los datos.

4.1 EL PROVEEDOR, en el tratamiento de datos de carácter personal del CLIENTE, podrá tratarlos en las propias instalaciones de éste o bien fuera de ellas, y lo hará de conformidad con las finalidades y los usos previstos en el presente Contrato, de forma que accederá únicamente a aquellos datos que EL CLIENTE le proporcione y procederá a su tratamiento de acuerdo con las instrucciones proporcionadas por el mismo, no constituyendo, en ningún caso, dicho acceso una comunicación de datos.

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento, pone a disposición del encargado del tratamiento, la información que se describe a continuación:

a) **Tipos de datos personales objeto de tratamiento:**

- ☐ Datos Identificativos: Nombre y apellidos, imagen/voz.
- ☐ Datos biométricos relativos al reconocimiento facial y dinámica del tecleo.

b) Colectivos o categorías de interesados:

- ☐ Clientes y usuarios (alumnos)
- ☐ Empleados

SEGUNDA.- OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, únicamente para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La seudonimización y el cifrado de datos personales.
b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 15 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección datos@imf-formacion.com.La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la

solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información. Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de correo electrónico, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2.- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
3.- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
4.- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad siguientes:

1.- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2.- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
3.- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4.- Seudonimizar y cifrar los datos personales, en su caso.

No obstante lo anterior, el Proveedor garantiza que cuenta con los controles de seguridad especificados en la política de seguridad de servicios biométricos, detallada en el Esquema Funcional de los Servicios Biométricos, y que se adjunta como Anexo I al presente contrato.

TERCERA.- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

1. El Responsable deberá entregar al Encargado los datos a los que hace referencia la cláusula primera del presente contrato, que contienen la información necesaria para llevar a cabo las tareas encomendadas en el contrato suscrito. Si los datos anteriores sufriesen alguna variación, deberá comunicárselo al Encargado, para que aquél pueda actualizarlos.

2. Asimismo deberá aplicar las medidas técnicas y organizativas para garantizar y demostrar que el tratamiento de datos es conforme a la normativa de protección de datos.

3. Atender los ejercicios de derechos establecidos en la normativa vigente de protección de datos de carácter personal aunque dicho ejercicio se dirija ante el Encargado de tratamiento.

4. Igualmente, deberá velar, durante todo el tratamiento, por el cumplimiento de la normativa en materia de protección de datos por parte del Encargado por el cumplimiento del RGPD y la ley 3/2018 LOPDGDD

CUARTA.- RESPONSABILIDAD

1. En el caso de que EL PROVEEDOR en su calidad de encargado de tratamiento, destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

2.Ninguna de las partes asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud del presente Contrato si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor o caso fortuito admitido como tal por la Jurisprudencia, en particular: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico o cualquier otra medida excepcional adoptada por las autoridades administrativas o gubernamentales.

QUINTA.- CONFIDENCIALIDAD

1. EL PROVEEDOR garantiza que mantendrá la más estricta confidencialidad y expreso cumplimiento del deber de secreto profesional, en relación con los asuntos de EL CLIENTE durante la vigencia de este Contrato y después de su terminación.

2. EL PROVEEDOR durante y con posterioridad a la vigencia de este Contrato tratará toda información propiedad de EL CLIENTE de forma estrictamente confidencial, tomando las medidas necesarias para que su contenido no se divulgue a terceros, bien directamente, bien a través de terceras personas o empresas, ni estos puedan tener acceso a los mismos sin autorización expresa de EL CLIENTE.

3. A los efectos del presente Contrato, tendrá la consideración de información confidencial toda aquella susceptible de ser revelada por palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en un futuro, ya sea

intercambiada como consecuencia de esta relación contractual, conocida antes de la misma o que una parte señale o designe como confidencial a la otra.

4. Las obligaciones de confidencialidad establecidas en el presente contrato estarán en vigor mientras dure la relación entre las partes objeto del presente contrato, así como una vez extinguida la relación contractual por cualquier causa entre EL CLIENTE y EL PROVEEDOR.

Fdo. José Luis del Rincón Ruiz

Fdo. Carlos Martínez Domínguez

En muestra de aceptación y conformidad con todos y cada una de las cláusulas estipuladas, obligándose al cumplimiento de todo lo acordado, lo firman por duplicado en cada una de sus hojas en el lugar y fecha del encabezamiento de la presente adenda.

IMF Instituto de Ciencias Empresariales

Centro adscrito a: Universidad Camilo José Cela

Centro Universitario inscrito en el Registro Nacional de Universidades, Centros y Títulos de España 28053812

Solicitud de preinscripción a los estudios de

GRADO EN AMINISTRACIÓN DE EMPRESAS

1. Datos de la Persona Solicitante

Identificación

Nombre: _____ Número DNI/NIE/Pasaporte: _____

1º Apellido: _____ Nacionalidad: _____ Sexo: ☐ H ☐ M

2º Apellido: _____ Nacimiento (Día/Mes/Año): _____

Dirección

Vía pública: _____ Número: _____ Código postal: _____

Municipio: _____ Provincia: _____ País: _____

Contacto

Correo electrónico: _____ Teléfono: _____

2. Vía de acceso a los estudios y documentación que la acredita

	Vía de acceso	Acreditación (*)
☐	Bachillerato + PAU/EvAU	Libro escolaridad Bachillerato +Título Bachillerato + Tarjeta PAU/EvAU
☐	FPII / Ciclo Formativo de Grado Superior	Libro escolaridad FPII ó Certi cación Académica + Título FP
☐	Estudios universitarios españoles iniciados	Libro escolaridad Bachillerato + tarjeta PAU/EvAU + Certi cación Académica
☐	Estudios universitarios españoles finalizados	Título universitario + Certificación Académica
☐	Acceso mayores de 25 años	Certificado de superación de la prueba
☐	Acceso mayores de 45 años	Certificado de superación de la prueba
☐	Acceso mayores de 40 años	Acreditación experiencia laboral + vida laboral
☐	Bachillerato Internacional	Título Bachillerato + Credencial de la UNED
☐	Bachillerato de la Unión Europea	Título Bachillerato homologado + Certificación Académica
☐	Estudios universitarios no españoles	Título apostillado + Certificación Académica

3. Otra documentación a adjuntar

	Documento	Acreditación (*)
☐	DNI/NIE/Pasaporte	Fotocopia completa
☐	Solicitud reconocimiento de ECTS	Certificación Académica

(*) Todos los documentos deben estar compulsados notarialmente y para estudios extranjeros, además, Apostillado (para Estados Miembros pertenecientes al Convenio de la Haya) o Legalizado por el Consulado (en caso de no pertenecer al Convenio de la Haya).

La persona solicitante declara que todos los datos consignados en la presente solicitud son ciertos, que ha sido informada de las características y condiciones de los estudios a los cuales solicita la admisión, y que acepta las normas que regulan el los estudios, el régimen interno del Centro y la organización y funcionamiento de la Universidad, así como las condiciones económicas del programa, lo cual corrobora a continuación con su firma:

Firma:

Firmado por: _____ Lugar _____ Fecha: _____

La persona admitida recibirá la correspondiente Credencial de Admisión a los estudios solicitados y en ella se le informará detalladamente de los procesos ulteriores de matriculación, así como de los requerimientos particulares que fueran precisos para completar su expediente académico y proceder a su alta como alumno universitario.

Instituto de Ciencias Empresariales

Centro adscrito a: Universidad Camilo José Cela

Centro Universitario inscrito en el Registro Nacional de Universidades, Centros y Títulos de España 28053812

Solicitud de preinscripción a los estudios de

GRADO EN AMINISTRACIÓN DE EMPRESAS

En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se le informa de que el Instituto de Ciencias Empresariales IMF S.L., con dirección: C/ Costanilla de San Pedro, 2 28005 Madrid, Teléfono: 900 318 111, Correo electrónico: **datos@imfice.es** y Delegado de Protección de Datos: **dpd@imf.com** tratará sus datos con la finalidad de gestionar la solicitud realizada por el titular de los datos en relación con los servicios proporcionados por la entidad. Para la correcta gestión de dichos servicios, y en los casos necesarios (becas, prácticas, etc), sus datos serán comunicados a los organismos oficiales necesarios (Fundación Layret, FUE, etc.). Asimismo, como parte de un programa conjunto con la Universidad Camilo José Cela, se le informa de que, en tal caso, los datos recabados por el Instituto de Ciencias Empresariales IMF S.L. deberán ser comunicados a la mencionada Universidad para la correcta gestión de la inscripción, matrícula y expedición de título.

Además, el Instituto de Ciencias Empresariales IMF S.L. tratará sus datos de alumno o antiguo alumno con finalidades comerciales y de publicidad, por cualquier medio, incluido el electrónico, para lo cual se le solicita su autorización:

☐ Marque la casilla si desea que sus datos sean tratados para envío de información comercial personalizada (cursos, eventos, seminarios, nuevos programas, etc)

Asimismo, desde el Instituto de Ciencias Empresariales IMF S.L. y en relación al uso del Campus Virtual de la entidad, le informamos que se encuentra implantado un sistema de verificación consistente en reconocimiento facial y dinámica del tecleo, que permite garantizar inequívocamente su identidad mediante el tratamiento de datos biométricos con el objetivo de poder realizar los exámenes en modalidad online. En este sentido, únicamente se tratarán sus datos biométricos si usted otorga de forma libre su consentimiento, que le será solicitado en el primer acceso al campus virtual. En caso de que no otorgue su consentimiento al tratamiento de datos descrito, podrá realizar los exámenes de forma presencial en la sede de Madrid en las fechas programadas en el calendario académico.

Conforme a lo establecido en la normativa de protección de datos, Usted tiene derecho a obtener confirmación sobre si en el Instituto de Ciencias Empresariales IMF S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Asimismo, podrá oponerse al tratamiento de sus datos, solicitar la limitación al tratamiento y la portabilidad de sus datos. Si considera que sus datos personales no han sido tratados conforme a la normativa, puede contactar con **datos@imfice.es**. Igualmente, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido la satisfacción en el ejercicio de sus derechos, a través de la sede electrónica en **www.aepd.es**. Puede consultar la información adicional al tratamiento de sus datos en **www.imfice.es**

Firmado: D./Dña. _____ DNI nº _____

En _____, a _____ de _____ de _____

Firma

IMF Instituto de Ciencias Empresariales

Centro adscrito a: Universidad Camilo José Cela

Centro Universitario inscrito en el Registro Nacional de Universidades, Centros y Títulos de España 28053812

Solicitud de preinscripción a los estudios de

GRADO EN DERECHO

1. Datos de la Persona Solicitante

Identificación

Nombre: _____ Número DNI/NIE/Pasaporte: _____

1º Apellido: _____ Nacionalidad: _____ Sexo: ☐ H ☐ M

2º Apellido: _____ Nacimiento (Día/Mes/Año): _____

Dirección

Vía pública: _____ Número: _____ Código postal: _____

Municipio: _____ Provincia: _____ País: _____

Contacto

Correo electrónico: _____ Teléfono: _____

2. Vía de acceso a los estudios y documentación que la acredita

	Vía de acceso	Acreditación (*)
☐	Bachillerato + PAU/EvAU	Libro escolaridad Bachillerato +Título Bachillerato + Tarjeta PAU/EvAU
☐	FPII / Ciclo Formativo de Grado Superior	Libro escolaridad FPII ó Certi cación Académica + Título FP
☐	Estudios universitarios españoles iniciados	Libro escolaridad Bachillerato + tarjeta PAU/EvAU + Certi cación Académica
☐	Estudios universitarios españoles finalizados	Título universitario + Certificación Académica
☐	Acceso mayores de 25 años	Certificado de superación de la prueba
☐	Acceso mayores de 45 años	Certificado de superación de la prueba
☐	Acceso mayores de 40 años	Acreditación experiencia laboral + vida laboral
☐	Bachillerato Internacional	Título Bachillerato + Credencial de la UNED
☐	Bachillerato de la Unión Europea	Título Bachillerato homologado + Certificación Académica
☐	Estudios universitarios no españoles	Título apostillado + Certificación Académica

3. Otra documentación a adjuntar

	Documento	Acreditación (*)
☐	DNI/NIE/Pasaporte	Fotocopia completa
☐	Solicitud reconocimiento de ECTS	Certificación Académica

(*) Todos los documentos deben estar compulsados notarialmente y para estudios extranjeros, además, Apostillado (para Estados Miembros pertenecientes al Convenio de la Haya) o Legalizado por el Consulado (en caso de no pertenecer al Convenio de la Haya).

La persona solicitante declara que todos los datos consignados en la presente solicitud son ciertos, que ha sido informada de las características y condiciones de los estudios a los cuales solicita la admisión, y que acepta las normas que regulan el los estudios, el régimen interno del Centro y la organización y funcionamiento de la Universidad, así como las condiciones económicas del programa, lo cual corrobora a continuación con su firma:

Firma:

Firmado por: _____ Lugar _____ Fecha: _____

La persona admitida recibirá la correspondiente Credencial de Admisión a los estudios solicitados y en ella se le informará detalladamente de los procesos ulteriores de matriculación, así como de los requerimientos particulares que fueran precisos para completar su expediente académico y proceder a su alta como alumno universitario.

Instituto de Ciencias Empresariales

Centro adscrito a: Universidad Camilo José Cela

Centro Universitario inscrito en el Registro Nacional de Universidades, Centros y Títulos de España 28053812

Solicitud de preinscripción a los estudios de

GRADO EN DERECHO

En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se le informa de que el Instituto de Ciencias Empresariales IMF S.L., con dirección: C/ Costanilla de San Pedro, 2 28005 Madrid, Teléfono: 900 318 111, Correo electrónico: **datos@imfice.es** y Delegado de Protección de Datos: **dpd@imf.com** tratará sus datos con la finalidad de gestionar la solicitud realizada por el titular de los datos en relación con los servicios proporcionados por la entidad. Para la correcta gestión de dichos servicios, y en los casos necesarios (becas, prácticas, etc), sus datos serán comunicados a los organismos oficiales necesarios (Fundación Layret, FUE, etc.). Asimismo, como parte de un programa conjunto con la Universidad Camilo José Cela, se le informa de que, en tal caso, los datos recabados por el Instituto de Ciencias Empresariales IMF S.L. deberán ser comunicados a la mencionada Universidad para la correcta gestión de la inscripción, matrícula y expedición de título.

Además, el Instituto de Ciencias Empresariales IMF S.L. tratará sus datos de alumno o antiguo alumno con finalidades comerciales y de publicidad, por cualquier medio, incluido el electrónico, para lo cual se le solicita su autorización:

☐ Marque la casilla si desea que sus datos sean tratados para envío de información comercial personalizada (cursos, eventos, seminarios, nuevos programas, etc)

Asimismo, desde el Instituto de Ciencias Empresariales IMF S.L. y en relación al uso del Campus Virtual de la entidad, le informamos que se encuentra implantado un sistema de verificación consistente en reconocimiento facial y dinámica del tecleo, que permite garantizar inequívocamente su identidad mediante el tratamiento de datos biométricos con el objetivo de poder realizar los exámenes en modalidad online. En este sentido, únicamente se tratarán sus datos biométricos si usted otorga de forma libre su consentimiento, que le será solicitado en el primer acceso al campus virtual. En caso de que no otorgue su consentimiento al tratamiento de datos descrito, podrá realizar los exámenes de forma presencial en la sede de Madrid en las fechas programadas en el calendario académico.

Conforme a lo establecido en la normativa de protección de datos, Usted tiene derecho a obtener confirmación sobre si en el Instituto de Ciencias Empresariales IMF S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Asimismo, podrá oponerse al tratamiento de sus datos, solicitar la limitación al tratamiento y la portabilidad de sus datos. Si considera que sus datos personales no han sido tratados conforme a la normativa, puede contactar con **datos@imfice.es**. Igualmente, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido la satisfacción en el ejercicio de sus derechos, a través de la sede electrónica en **www.aepd.es**. Puede consultar la información adicional al tratamiento de sus datos en **www.imfice.es**

Firmado: D./Dña. _____ DNI nº _____

En _____, a _____ de _____ de _____

Firma

CLÁUSULA PARA RECABAR EL CONSENTIMIENTO DE LOS ALUMNOS PARA RECONOCIMIENTO FACIAL Y PATRÓN DE TECLEO

- Responsable: Instituto de Ciencias Empresariales de IMF. S.L.
- Dirección: C/ Costanilla de San Pedro, 2 28005 Madrid
- Teléfono: 900 318 111
- Correo electrónico: datos@imfice.es
- Delegado de Protección de Datos: Pablo Perancho Ruiz]

En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se le informa de que INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L es la entidad responsable del tratamiento de sus datos personales biométricos relativos a la identificación de sus rasgos faciales, permitiendo su reconocimiento facial; así como de la dinámica del tecleo que permite el reconocimiento de su patrón de tecleo.

En cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en concreto en base a su artículo 83 se pretende por parte del Responsable de Tratamiento el establecimiento de un sistema educativo que garantice la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales. En consecuencia y en aras de los nuevos derechos digitales, se establece en los estudios, la implantación de un sistema de exámenes que garanticen unívocamente la identidad del alumno mediante la combinación del sistema de reconocimiento facial, así como de dinámica de tecleo, garantizando de este modo la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

La finalidad del tratamiento es utilizar las mencionadas técnicas de reconocimiento facial para poder autentificarle como alumno y usuario del Campus, y poder verificar así su identidad a la hora de realización de pruebas online (exámenes) asegurando de este modo el debido cumplimiento de las obligaciones que le vinculan a usted como alumno de INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L.

El procedimiento requiere que los alumnos se tomen tres fotografías en algún momento previo al examen, y que servirán como base de verificación; una vez llegado el momento de realizar la prueba, el ordenador tomará un determinado número de fotografías tanto en el momento de autentificarse en el sistema como en momentos aleatorios, durante el examen, comparando las diferentes capturas con las que se tomaron como base. Asimismo, se irá registrando su patrón de teclado a lo largo de todo el proceso definido, tanto durante el momento de alta en el Campus, durante la utilización del mismo, como en el momento de realización de la prueba online.

El tratamiento se legitima mediante el consentimiento expreso que se le solicita y usted otorga libremente.

Asimismo, se le informa de que el tratamiento de los datos personales de los que usted es titular únicamente se efectuará con las finalidades señaladas y con ninguna otra no declarada.

Los datos personales proporcionados se conservarán durante los plazos legalmente exigidos conforme a la legislación vigente.

Asimismo, como parte de un programa conjunto con la Universidad Camilo José Cela, se le informa de que, en tal caso, los datos recabados por INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L deberán ser comunicados a la mencionada Universidad con la finalidad de tramitar el título oficial de los estudios.

No están previstas transferencias internacionales de sus datos personales fuera del Espacio Económico Europeo.

Cualquier persona tiene derecho a obtener confirmación sobre si en INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L estamos tratando datos personales que les conciernan, y en tal caso, derecho de acceso a sus datos personales, a los fines del tratamiento, y a las categorías de datos personales de que se trate.

Asimismo, tendrá derecho a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, los datos ya no sean necesarios para los fines que fueron recogidos; se haya retirado el consentimiento en el que se basa el tratamiento o se oponga al tratamiento; los datos personales se hayan tratado de manera ilícita; o deban suprimirse para el cumplimiento de una obligación legal establecida en el derecho de la Unión o de los Estados miembros.

Podrá solicitar la limitación del tratamiento de sus datos cuando, impugne la exactitud de los datos personales durante el plazo que permita al responsable verificar la exactitud de los mismos; el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. En tales casos, únicamente conservaremos los datos para el ejercicio o la defensa de reclamaciones.

En determinadas circunstancias y por motivos relacionados con su situación particular, usted podrá oponerse al tratamiento de sus datos. INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

Tendrá derecho a recibir los datos personales que le incumban, y que haya facilitado, en un formato estructurado, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando, el tratamiento este basado en el consentimiento; o le tratamiento se efectúe por medios automatizados.

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, deberán comunicarlo por correo electrónico a la dirección datos@imfice.es

Si considera que sus datos personales no han sido tratados conforme a la normativa, puede contactar con datos@imfice.es Asimismo, podrá presentar una reclamación ante la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido la satisfacción en el ejercicio de sus derechos, a través de la sede electrónica en www.aepd.es.

Los datos personales que tratamos en INSTITUTO DE CIENCIAS EMPRESARIALES DE IMF. S.L proceden del propio interesado.

Puede consultar la información adicional al tratamiento de sus datos en https://www.imfice.es/legales/politica-de-privacidad/

Por último, se informa al interesado de que la consecuencia de no otorgar el consentimiento que se le solicita será la imposibilidad de realizar el examen en su modalidad online. En tanto no es posible verificar su identidad fehacientemente, en caso de no prestar su consentimiento al tratamiento de datos descrito, necesariamente deberá realizar el examen de forma presencial en Madrid para lo cual se programarán las fechas correspondientes.

¿Consiente expresamente el tratamiento de sus datos relativos al reconocimiento facial y patrón del tecleo con los fines anteriormente descritos?

☐ SI

☐ NO

Podrá revocar su consentimiento en cualquier momento en la dirección datos@imfice.es