I. Disposiciones Generales

UNIVERSIDAD DE ZARAGOZA

ACUERDO de 29 de junio de 2022, del Consejo de Gobierno de la Universidad de Zaragoza, por el que se aprueba la política de seguridad de la información y protección de datos personales de la Universidad de Zaragoza.

Exposición de motivos

El Real Decreto 3/2010, de 8 de enero, que regulaba el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS), tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos y estableció los principios básicos y los requisitos mínimos que han venido garantizando una protección adecuada de la información tratada. El ENS ha sido de obligada aplicación para todas las Administraciones públicas, que - a día de hoy - deben disponer formalmente de su política de seguridad aprobada por el órgano superior correspondiente. La política de seguridad debe establecerse con base en los principios básicos recogidos en la propia norma y desarrollar los requisitos mínimos en ella consignados.

Este Real Decreto ha sido sustituido por el reciente Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que actualiza su regulación con la finalidad explícita de cumplir tres grandes objetivos: alinearlo con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital; introducir el concepto de "perfil de cumplimiento específico" para permitir a ciertos colectivos y tipos de sistemas alcanzar una adaptación del ENS más eficaz y eficiente y, en tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por su parte, el 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 (conocido como Reglamento General de Protección de Datos o RGPD), que entró en aplicación a partir del 25 de mayo de 2018, señala que la protección de los derechos y libertades de las personas físicas incluye la protección de sus datos personales y exige, en el tratamiento de estos datos, la obligación de atenerse a una serie de principios y la adopción de toda una serie de medidas técnicas y organizativas que garanticen su cumplimiento. Entre dichas medidas se encuentran la de demostrar que el tratamiento es conforme al RGPD y la de dotarse de una política de protección de datos que así lo aplique.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD) ha venido a completar y desarrollar aquellas partes del RGPD que han quedado a la disposición normativa de los Estados miembros, completando así el marco regulatorio del derecho fundamental a la protección de datos personales en el ámbito de la Unión Europea. Su disposición adicional primera, relativa a medidas de seguridad en el ámbito del sector público, establece que el ENS incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD y obliga a las Administraciones, órganos y entidades del sector público, entre las que se incluyen las Universidades Públicas, a aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de entre las previstas en el ENS.

La legislación general en materia del Procedimiento Administrativo Común de las Administraciones Públicas (Ley 39/2015, de 1 de octubre) y de Régimen Jurídico del Sector Público (Ley 40/2015, de 1 de octubre) afianzan las interrelaciones entre la protección de los datos personales y la seguridad y confidencialidad de la información que figure en sus respectivos tratamientos, sistemas y aplicaciones al igual que pretenden asegurar la interoperabilidad de éstos garantizando la seguridad de la información y la protección de los datos de carácter personal que contengan. Y, por último, el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (Real Decreto 203/2021, de 30 de marzo) exige la permanente actualización del marco de ciberseguridad pública.

Todo ello aconseja que se acometa la regulación y adopción de una política conjunta de seguridad de la información y protección de datos personales en donde se recojan y deli-

csv: BOA20220726001

miten, de manera armónica, tanto las responsabilidades y funciones en materia de seguridad de la información y de protección de aquella información que contenga datos personales como cuestiones comunes a ambos ámbitos y las propias de cada una de ellas de modo que, sin entorpecerse la una a la otra, se complementen adecuadamente como exige la legislación vigente.

El Consejo de Gobierno aprobó, mediante Acuerdo de 24 de noviembre de 2016, la Política de Seguridad de la Información de la Universidad de Zaragoza.

En la actualidad, las transformaciones legislativas enumeradas y la conjunción operada entre seguridad de la información y protección de datos personales hacen necesario aprobar un nuevo acuerdo que no se limite a modificar o ampliar aspectos parciales, sino que, para una mayor seguridad jurídica y mejor conocimiento de los destinatarios, se integre en un único documento comprensivo de la Política de seguridad de la información y protección de datos personales de la Universidad de Zaragoza. Así, este documento se constituye en documento base mediante el cual se define el marco de referencia que permite la gestión de la seguridad de la información, incluida la de los datos personales, delimitando con claridad las funciones y responsabilidades en orden a definir, implantar y gestionar la política de seguridad de la información y de protección de datos en la Universidad de Zaragoza.

Por ello, a propuesta del Comité de Seguridad de la Información y Protección de Datos, se acuerda:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Se aprueba la Política de Seguridad de la Información y de Protección de Datos cuyo objeto es garantizar la seguridad, integridad, calidad y disponibilidad de la información y de los datos de carácter personal que la Universidad de Zaragoza gestiona, en el ámbito de sus competencias.

2. Esta política será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal que incumben a la Universidad de Zaragoza ya sea como responsable o como encargada de dicho tratamiento y ya sean gestionados, tratados, custodiados y conservados por medios electrónicos o en soporte papel.

3. También será de obligado cumplimiento para todas las oficinas, unidades, servicios, centros, institutos de investigación y otras estructuras que integran la Universidad, así como para todos cuantos, con independencia de su condición funcionarial o laboral, personal propio o ajeno, estudiantes, becarios o en prácticas, tengan acceso a la información o a los datos personales de los que es responsable o encargada del tratamiento la Universidad de Zaragoza.

4. Esta política se adopta en cumplimiento de lo dispuesto en la normativa que regula los sistemas de información en el ámbito de la administración pública (Esquema Nacional de Seguridad y Esquema Nacional de Interoperabilidad), en el de la protección de datos personales (Reglamento UE 2016/679 General de Protección de Datos, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y sus normas de desarrollo) y en aquella que regula la reutilización de la información del sector público y los tratamientos de datos con fines de archivo en interés público y patrimonio documental e histórico (Ley 37/2007, de 16 de noviembre, y Real Decreto 1164/2002, de 8 de noviembre).

5. Esta política es aplicable a los Sistemas de Información del Consorcio Campus Iberus vinculados a la Universidad de Zaragoza, por su adscripción a la misma conforme a lo establecido en sus estatutos.

Artículo 2. *Principios de seguridad de la información.*

La Universidad de Zaragoza tratará la información bajo su responsabilidad conforme a los siguientes principios de seguridad:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

b) Seguridad integral: La seguridad de la información es el resultado de un proceso integral constituido por todos y cada uno de los elementos humanos, materiales, técnicos, jurídicos y organizativos que intervienen en su tratamiento con el fin de preservar la confidencialidad, integridad y disponibilidad de la misma.
Consecuentemente, la seguridad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

csv: BOA20220726001

Para preservar la integridad del sistema, todo elemento físico o lógico requerirá autorización formal previa a su instalación en el mismo.

c) Gestión de riesgos: La gestión de riesgos es el conjunto de actividades coordinadas para dirigir y controlar el efecto de la incertidumbre sobre los procesos de seguridad de la información y protección de datos personales de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
La reducción de estos niveles de riesgo se realizará mediante el despliegue de las medidas de seguridad apropiadas en todas las fases de vida de las aplicaciones y servicios relacionados con el tratamiento de la información y de los datos personales, estableciendo un equilibrio y proporcionalidad entre la naturaleza de los datos, los tratamientos realizados, la probabilidad de los riesgos, el impacto sobre los sistemas y sobre los derechos de los sujetos afectados y la eficacia y el coste de las medidas de seguridad a aplicar.
Al evaluar el riesgo, la Universidad de Zaragoza tendrá en cuenta los riesgos que se derivan para los derechos y libertades de las personas con respecto al tratamiento de sus datos personales.
El análisis y gestión de riesgos es parte esencial de los procesos de seguridad y de protección de datos personales y deberá mantenerse permanentemente actualizado.

d) Proporcionalidad: La Universidad de Zaragoza establecerá las medidas de prevención, detección, reacción recuperación y conservación que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.
- Las medidas de prevención: Se establecerán medidas que permitan eliminar o al menos reducir la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema y para los datos. Se aplicarán las medidas de seguridad contempladas en el Esquema Nacional de Seguridad (ENS) asociadas al nivel de cada uno de los Sistemas de Información, así como cualquiera otra identificada como necesaria a través de las evaluaciones de amenazas y riesgos.
- Las medidas de detección: Dado que los servicios se pueden degradar rápidamente debido a incidentes, se monitorizarán las operaciones de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecerán mecanismos de detección, análisis e informe y comunicación a los responsables cuando se produzca una desviación significativa de los parámetros que se hayan establecido como normales.
- Las medidas de reacción o respuesta: Tendrán como objetivo atajar a tiempo los incidentes de seguridad que se produzcan. La Universidad establecerá protocolos de actuación para responder eficazmente a los incidentes de seguridad que se produzcan y para el intercambio de información relacionado con el incidente, incluyendo las comunicaciones o notificaciones al CCN-CERT, a la AEPD y, en su caso, a los ciudadanos afectados.
- Las medidas de recuperación: Deberán permitir la restauración de la información y la continuidad de los servicios de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales de trabajo.
- Las medidas de conservación: Sin merma de los principios básicos en materia de seguridad de la información y de la protección de datos personales, se garantizará la conservación de los datos e información en soporte electrónico instrumentándose los procedimientos adecuados para la preservación del patrimonio digital de la Universidad.

e) Líneas de defensa: Junto a las medidas antedichas, se adoptarán las medidas de naturaleza organizativa, física y lógica que permitan disponer de múltiples capas de seguridad que minimicen el impacto de los incidentes que puedan producirse.
Con este fin, para garantizar la disponibilidad de los servicios críticos, la Universidad deberá desarrollar planes de continuidad de los Sistemas TIC (Tecnologías de la Información y la Comunicación) como parte de su plan general de continuidad de negocio y actividades de recuperación.

f) Mejora continua: La gestión de la seguridad de la información y la de los datos personales requiere una actualización y monitorización continua de las medidas técnicas y organizativas adoptadas para adaptar su eficacia a la constante evolución de los riesgos y sistemas de protección, así como una reevaluación periódica que permita contrastar su permanente adecuación.

g) Protección de datos y seguridad desde el diseño: La Universidad de Zaragoza promoverá la implantación del principio de protección de datos desde el diseño con el objetivo

csv: BOA20220726001

de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente desde las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información.

h) Protección de datos y seguridad por defecto: La Universidad de Zaragoza promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen un grado de seguridad y de protección de datos por defecto, otorgando los mínimos privilegios necesarios para su correcto desempeño conforme a lo dispuesto en el artículo 20 del Real Decreto. 311/2022, de 3 de mayo.

Artículo 3. *Principios de protección de datos personales.*

La Universidad de Zaragoza, cuando la información bajo su responsabilidad contenga datos de carácter personal, aplicará, además de los principios de seguridad de la información enumerados en el artículo 2, los siguientes principios:

a) Licitud, lealtad y transparencia: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado. Para ello se tendrá en cuenta la existencia de título habilitante para el tratamiento, se adoptarán las medidas y procedimientos que garanticen a los afectados el adecuado ejercicio de sus derechos y se ofrecerá información suficiente sobre los tratamientos de datos que se realicen.
b) Limitación de la finalidad: Los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines.
c) Minimización de datos: Los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
d) Exactitud de los datos: Los datos de carácter personal serán exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación aquellos datos que sean inexactos.
e) Limitación del plazo de conservación: Los datos de carácter personal serán mantenidos de forma que no se permita la identificación de los interesados durante más tiempo del necesario para los fines que justificaron su tratamiento.
f) Integridad y confidencialidad: Los datos de carácter personal serán tratados de manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de datos estarán sujetos al deber de secreto incluso después de haber concluido aquél.

Artículo 4. *Principios comunes en materia de seguridad de la información y protección de datos personales.*

Todos los usuarios de los sistemas, aplicaciones y servicios de seguridad de la información y de tratamientos de datos personales se regirán por los siguientes principios:

a) Inventario de activos de información y de actividades de tratamiento.
Todos los activos de información serán inventariados y categorizados conforme a las determinaciones del Esquema Nacional de Seguridad.
La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
Del mismo modo, se mantendrá permanentemente actualizado un Registro de actividades de tratamiento de datos personales, cuyo Inventario se hará público en la Sede electrónica y en la página web de la Universidad mediante un apartado destinado específicamente a la protección de datos.
b) Seguridad ligada a las personas.
Las personas juegan un papel fundamental en la política de seguridad de la información y de protección de datos personales de la Universidad.
A estos efectos, se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
Entre estos mecanismos se contemplarán, necesariamente, los siguientes:
- Acceso a la información: Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular las autorizaciones de acceso a los sistemas y recursos de información, incluido el acceso físico a las instalaciones, conforme a los criterios establecidos por su responsable.

csv: BOA20220726001

Las autorizaciones concedidas a cada usuario se limitarán al mínimo estrictamente necesario para cumplir con sus obligaciones.

- Control de acceso: Se implantarán los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso, la identificación de forma única de cada usuario y auditar su uso adecuado.

- Deber de secreto: Todos los usuarios están obligados a guardar secreto profesional de toda aquella información y de los datos personales de los que tengan conocimiento con ocasión del ejercicio de su cargo o actividad profesional. Esta obligación se mantendrá incluso después de haber finalizado su relación con la Universidad de Zaragoza. El deber de confidencialidad y secreto profesional se establecerá de forma expresa en todo tipo de relaciones -administrativas, civiles o mercantiles- que impliquen o supongan acceso o tratamiento de la información y/o de datos personales, incluidos los servicios de simple alojamiento, transporte o soporte técnico.

c) Seguridad física: Los sistemas y los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad y estarán suficientemente protegidos frente a amenazas físicas o ambientales. A estos efectos se realizarán evaluaciones de riesgos que tendrán especialmente en cuenta los riesgos para los datos personales y los derechos y libertades de los ciudadanos.

d) Seguridad de la información almacenada y en tránsito: En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que se analizarán especialmente para lograr una adecuada protección.

e) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr la adecuada gestión de la seguridad y velar por la actualización de las Tecnologías de la Información y Comunicaciones (TIC) empleadas por la Universidad.

Se protegerá el perímetro del sistema de información y se tendrá en cuenta igualmente la seguridad y protección de la información que se transmita a través de redes de comunicaciones, adecuada a los distintos niveles de sensibilidad y criticidad.

f) Ciclo vital de la información: La seguridad y la protección de datos estarán presentes durante todo el ciclo de vida de la información, garantizando su seguridad por defecto. La adquisición, desarrollo y mantenimiento de los sistemas, aplicaciones y servicios de información y de almacenamiento y tratamientos de datos que realice la Universidad deberá cumplir con las determinaciones establecidas al respecto para las Administraciones Públicas por la normativa específica que rige en materia de seguridad de la información y de protección de datos personales.

g) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación de los incidentes de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad y en la Instrucción Técnica correspondiente.

Artículo 5. *Alcance estratégico y responsabilidad proactiva.*

La seguridad de la información y la protección de datos personales contarán con el compromiso y apoyo de todos los órganos de dirección de la Universidad de Zaragoza.

Para lograrlo, se estima imprescindible asumir el cumplimiento de los principios anteriormente señalados y la adopción de las medidas técnicas y organizativas que le permitan estar en condiciones de dicho cumplimiento conforme a las determinaciones establecidas a continuación.

Artículo 6. *Gestión de los riesgos de seguridad de la información.*

La gestión de los riesgos de seguridad de la información debe realizarse de manera continua conforme a los principios de gestión de la seguridad basada en riesgos y reevaluación periódica.

Se establecerá un marco de directrices básicas para armonizar los criterios a seguir para llevar a cabo el análisis de riesgos que permita identificar, gestionar y minimizar los riesgos hasta niveles que puedan considerarse aceptables.

Artículo 7. *Análisis de riesgos y evaluaciones de impacto.*

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

csv: BOA20220726001

- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información y Protección de Datos (en adelante, CSIPD) establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del CSIPD.

El Comité dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El CSIPD procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

Cuando los Sistemas de Información contengan datos de carácter personal, el análisis de riesgos deberá identificar los factores de riesgo para los derechos y libertades de los interesados cuyos datos están presentes en el tratamiento con el fin de hacer una primera evaluación del riesgo intrínseco, adoptar las medidas y garantías que lo mitiguen y estimar el riesgo residual.

Cuando sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, será obligatorio realizar una evaluación de impacto que determine las medidas a adoptar para abordarlos. Para ello se seguirán las determinaciones establecidas por el RGPD y las orientaciones facilitadas por la Agencia Española de Protección de Datos (AEPD).

Para el análisis y gestión de riesgos se utilizarán las herramientas facilitadas por el Centro Criptológico Nacional (CCN) así como, en lo que respecta a análisis de riesgos y evaluaciones de impacto en el tratamiento de datos de carácter personal, las guías, recomendaciones y herramientas proporcionadas por la Agencia Española de Protección de Datos (AEPD).

Artículo 8. *Incidentes y brechas de seguridad.*

Se atenderá especialmente a la seguridad de los sistemas de información y se dispondrá de un proceso integral para hacer frente a los incidentes que contemple las medidas de detección, contención, reacción y recuperación y que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.

Se notificarán al Centro Criptológico Nacional (CCN-CERT) y, en su caso, al Instituto Nacional de Ciberseguridad (INCIBE) aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información, de acuerdo con lo dispuesto en la normativa reguladora del Esquema Nacional de Seguridad (ENS).

De conformidad con lo dispuesto en el artículo 33 del RGPD, la Universidad adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos de carácter personal que pudieran producirse, a través del procedimiento establecido al efecto por la Agencia Española de Protección de Datos (AEPD).

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, conforme a lo dispuesto en el artículo 34 del RGPD.

Artículo 9. *Revisión y auditoría.*

Con carácter ordinario, los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, encaminada a la verificación, evaluación y eficacia de las medidas técnicas y organizativas adoptadas para garantizar la seguridad de los sistemas de información y de los tratamientos de datos de carácter personal en cumplimiento de los requerimientos del Esquema Nacional de Seguridad y del Reglamento General de Protección de Datos así como los que puedan derivarse de la presente Política de Seguridad y Privacidad.

Con independencia de lo anterior, se realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en los sistemas de información que

csv: BOA20220726001

puedan repercutir en el cumplimiento de las medidas de seguridad implantadas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años establecidos para la realización de la siguiente auditoría regular ordinaria.

El plazo de dos años señalado podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la Universidad. Las auditorías serán propuestas por el Comité de Seguridad de la Información y supervisadas por el/la Responsable de Seguridad de la información y por el Delegado/a de Protección de Datos.

En la realización de las auditorías se seguirán las determinaciones establecidas en el artículo 31 y anexo III del Real Decreto 311/2022, de 3 de mayo.

Artículo 10. *Responsabilidad diferenciada.*

Se observará el principio de responsabilidad diferenciada de modo que se delimiten las diferentes responsabilidades y roles en materia de seguridad de la información y de protección de datos personales.

Teniendo en cuenta las pautas establecidas por el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos, la estructura organizativa para la gestión de la seguridad de la información y de los tratamientos de datos personales estará compuesta por los siguientes agentes:

a) El Comité de Seguridad de la Información y Protección de Datos (CSIPD).
b) Responsable de la información.
c) Responsable de los servicios y del tratamiento de datos personales.
d) Responsable de Seguridad TIC.
e) Responsables de los Sistemas.
f) Jefe de Proyecto de Seguridad.
g) Responsables internos del tratamiento de datos personales.
h) Encargados internos del tratamiento de datos personales.
i) Usuarios.
j) Unidad de Protección de Datos.
k) Delegado de Protección de Datos.

Artículo 11. *El Comité de Seguridad de la Información y Protección de Datos (CSIPD).*

1. Se crea el Comité de Seguridad de la Información y Protección de Datos (CSIPD) como órgano colegiado encargado de gestionar y coordinar todas las actuaciones relacionadas con la política de seguridad y privacidad de la Universidad, dando cuenta de ello al Consejo de Dirección y al Consejo de Gobierno. Actuará en el ámbito de cumplimiento de las medidas establecidas por el Esquema Nacional de Seguridad (ENS) y por el Reglamento General de Protección de Datos (RGPD) y sus respectivas normas de desarrollo.

2. El CSIPD está formado por los siguientes miembros:

a) El Secretario General de la Universidad quien, en su condición de Responsable de la Información, lo presidirá.
b) El gerente de la Universidad que, en su condición de responsable de los servicios y, por delegación del rector, de la protección de datos personales, actuará como vice-presidente.
c) El Vicegerente de Tecnologías de la Información y la Comunicación, en su condición de Responsable de la Seguridad de los Sistemas.
d) El Técnico del Servicio de Informática y Comunicaciones como Jefe de Proyecto de Seguridad de la Información con las atribuciones que se definen en esta Política.
e) El Delegado de Protección de Datos participará con voz pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.
f) Quienes, en calidad de invitados, sean convocados por el presidente del CSIPD en función de los asuntos a tratar en una sesión determinada. Los invitados tendrán voz pero no voto.
g) Un miembro del personal de administración y servicios que actuará como Secretario.

3. El CSIPD se reunirá en sesión ordinaria al menos una vez por trimestre y en sesión extraordinaria cuando los asuntos relacionados con sus funciones así lo requieran. Las reuniones serán convocadas por la presidencia, ya sea por propia iniciativa o a petición motivada de al menos dos de sus componentes, con una antelación mínima de 5 días hábiles en el caso

csv: BOA20220726001

de tratarse de una sesión ordinaria y de 48 horas cuando se trate de una sesión extraordinaria.

El CSIPD podrá dotarse de su propia norma organizativa interna.

4. Corresponden al CSIPD las siguientes funciones:

a) Aprobar criterios para la designación de roles y responsabilidades dentro de los ámbitos de seguridad de la información y de la protección de datos conforme a las directrices de la presente Política de Seguridad de la Información y de Protección de Datos.
b) Aprobar los protocolos de actuación en materia de seguridad de la información, incluyendo aquella que afecte a la protección de datos personales.
c) Aprobar criterios para el procedimiento de análisis de riesgos en materia de seguridad de la información y de la protección de datos, incluidas las evaluaciones de impacto.
d) Acordar y proponer las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones que incumben a la Universidad en materia de seguridad de la información y de protección de datos.
e) Acordar y proponer la realización de evaluaciones de impacto y auditorías externas.
f) Acordar y proponer la monitorización de los principales riesgos residuales y las actuaciones posibles en este ámbito.
g) Acordar y proponer los recursos y medios que estime necesarios para la concienciación y formación en materia de seguridad de la información y protección de datos personales para todo el personal de la Universidad.
h) Acordar y proponer planes de mejora de seguridad de la información y de los tratamientos de datos.
i) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
j) Conocer y analizar los informes relativos a los incidentes de seguridad y brechas de datos; los resultados de análisis de riesgos, evaluaciones de impacto y auditorías realizadas, así como los proyectos, iniciativas y acciones de mejora de la seguridad requeridas.
k) Conocer los informes anuales que deban realizarse en materia de seguridad de la información (informe INES) y de protección de datos.
l) Elaborar las propuestas de modificación y actualización permanente de la Política de Seguridad y Privacidad de la Universidad.
m) Velar por el cumplimiento de la Política de Seguridad y Privacidad y su normativa de desarrollo.
n) Ser consultado en la toma de decisiones que afecten a la seguridad de la información y de la protección de datos.

Artículo 12. *Responsable de la información.*

1. Es responsable de la información el Secretario/a General de la Universidad.

2. Le corresponde:

a) Velar por el buen uso de toda la información de la Universidad de acuerdo con los principios de protección, integridad y confidencialidad.
b) La determinación de los niveles y medidas de seguridad de la información, a propuesta del CSIPD, dentro del marco previsto en los anexos I y II del Esquema Nacional de Seguridad (ENS).

Artículo 13. *Responsable de los servicios y del tratamiento de datos personales.*

1. El Gerente tiene bajo su responsabilidad a todos los servicios de la Universidad, incluídos los relativos a seguridad de la información y de tratamientos de datos.

Como responsable de los servicios le corresponden las siguientes funciones:

a) Aprobar los requisitos básicos de los servicios en materia de seguridad, interoperabilidad, accesibilidad y disponibilidad.
b) Determinar los niveles de seguridad de los Servicios.
c) Trabajar en colaboración con el Responsable de Seguridad y el Responsable del Sistema, en el mantenimiento de los sistemas catalogados, según el anexo I del ENS.

2. La Universidad de Zaragoza, como entidad que determina los fines y medios de sus tratamientos, es la responsable de todas las actividades de tratamiento de datos que realiza. La figura del responsable de tratamiento se centraliza en la persona de su Rector y, por delegación, en el Gerente de la misma.

Le corresponden las siguientes funciones:

a) La autorización de todos los tratamientos de datos en los que la Universidad vaya a ser responsable, corresponsable o encargada del tratamiento;
b) La asignación de responsabilidades dentro de cada tratamiento;

csv: BOA20220726001

c) La determinación de las medidas de seguridad aplicables, previo informe del responsable de seguridad;
d) La aprobación, a propuesta del CSIPD, de los protocolos de actuación en materia de protección de datos personales;
e) La aprobación, a propuesta del CSIPD, de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento, conforme a lo exigido en el RGPD.
f) Todas las actuaciones y obligaciones que incumben al responsable del tratamiento conforme al RGPD.

Artículo 14. *Responsable de Seguridad TIC.*

1. El Vicegerente de Tecnologías de la Información y Comunicación (TIC) es el máximo responsable técnico del Servicio de Informática y Comunicaciones (SICUZ) y, como tal, asume el rol de Responsable de Seguridad de la Universidad.

2. Le corresponden, en este ámbito, las siguientes funciones:
a) Establecer los requisitos técnicos de los servicios de información en materia de seguridad, incluyendo los de interoperabilidad, accesibilidad y disponibilidad.
b) Determinar los niveles de seguridad en cada uno de los servicios a su cargo.
c) Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y de los servicios prestados.
d) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
e) Apoyar la efectiva implementación de los mecanismos de gestión y evaluación de riesgos en materia de seguridad de la información y de protección de datos, incluidas las evaluaciones de impacto cuando fueran preceptivas o se estimara conveniente.
f) Coordinar la investigación de los incidentes de seguridad, desde su notificación hasta su resolución.
g) Aprobar los procedimientos técnicos de seguridad elaborados por los Responsables de los distintos Sistemas.
h) Analizar, completar y autorizar toda la documentación técnica relacionada con la seguridad del sistema.
i) Promover la formación y concienciación del SICUZ, dentro de su ámbito de responsabilidad.

Artículo 15. *Responsables de los Sistemas.*

1. Son responsables de los sistemas de información de la Universidad cada uno de los Directores de Área del SICUZ.

2. Les corresponden, dentro de su respectiva área de actuación, las siguientes funciones:
a) Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la tipología y política de gestión del Sistema, estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
d) Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
e) Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema, durante las etapas de desarrollo, instalación y prueba del mismo.
f) Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
g) Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
h) Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
i) Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
j) Determinar la categoría del Sistema según el procedimiento descrito en el anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el anexo II del ENS.
k) Elaborar y aprobar la documentación de seguridad del Sistema.
l) Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.

csv: BOA20220726001

m) Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
n) Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
o) Además, el responsable del Sistema puede acordar la suspensión del manejo de una cierta información, o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutada.
p) Elaboración de los procedimientos de seguridad necesarios para la operativa en el Sistema.

Artículo 16. *Jefe de Proyecto de Seguridad de la Información.*

1. El Jefe de Proyecto de Seguridad de la Información será el técnico del SICUZ designado a tal efecto.

2. Le corresponden las siguientes funciones:
a) Hacer seguimiento y colaborar en la implementación y mantenimiento de las medidas de seguridad, aplicables al Sistema de Información.
b) Hacer seguimiento y colaborar en la gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
c) Hacer seguimiento y colaborar en la aplicación de los Procedimientos Operativos de Seguridad.
d) Controlar los cambios en la configuración vigente del Sistema de Información.
e) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
f) Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida, y que en todo momento se ajustan a las autorizaciones pertinentes.
h) Monitorizar el estado de seguridad del Sistema, proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el Sistema.
i) Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
k) Colaborar técnicamente con el/la DPD aquellos aspectos en materia de seguridad TIC que tengan relación con la protección de datos.

Artículo 17. *Responsables internos del tratamiento de datos personales.*

1. Son responsables internos del tratamiento de datos las personas designadas por el gerente que, en calidad de tales, deben velar por el cumplimiento de las condiciones asignadas a cada tratamiento.

2. Son responsables internos las personas que dirigen las diferentes unidades organizativas y que, en cumplimiento de sus tareas administrativas, necesitan tratar datos de carácter personal. De ellos dependen administrativamente uno o varios encargados internos de tratamiento.

En el caso de los tratamientos bajo la responsabilidad de grupos de investigación, la responsabilidad interna corresponde al investigador principal (IP).

En el caso de los trabajos dirigidos de índole académica, la responsabilidad interna corresponde al Director/Tutor.

3. Les corresponde:
a) Dirigir y coordinar el cumplimiento de las condiciones establecidas para cada tratamiento;
b) la asignación de funciones específicas sobre tratamiento de datos a su respectivo personal;
c) conservar los documentos de recogida de datos y llevar a cabo las operaciones de seudonimización y disociación, cuando proceda;
d) la efectiva implantación de las medidas de seguridad asignadas al tratamiento que esté bajo su responsabilidad;

csv: BOA20220726001

e) velar por el respeto a los deberes de secreto y confidencialidad de la información dentro de su ámbito de actuación;
f) participar, junto con el responsable de seguridad, en los procedimientos de análisis de riesgos en materia de seguridad de la información y de la protección de datos, incluidas las evaluaciones de impacto conforme a lo establecido en el respectivo protocolo de actuación.
g) participar, junto con el responsable de seguridad, en la comunicación y resolución de los incidentes de seguridad y las brechas de datos personales, conforme a lo establecido en el respectivo protocolo de actuación;
h) comunicar al gerente la terminación del tratamiento bajo su responsabilidad velando por la efectiva y segura destrucción de los datos, cuando proceda;
i) cuantas otras funciones y responsabilidades puedan serles asignadas por el gerente en materia de seguridad de la información y protección de datos personales.

Artículo 18. *Encargados internos del tratamiento de datos personales.*

1. Son encargados internos de cada tratamiento las personas designadas por el gerente o, en su defecto, por el respectivo responsable interno del tratamiento.

En el caso de los tratamientos bajo la responsabilidad de grupos de investigación, el encargado será uno de los miembros del grupo.

En el caso de los trabajos dirigidos de índole académica, será encargado interno el alumno autor de dicho trabajo.

2. Les corresponde:
a) Dar cumplimiento a las directrices de su respectivo responsable interno en cuanto a tratamiento y seguridad de los datos;
b) garantizar que el tratamiento de datos se realiza conforme a las condiciones de su autorización y, en su caso, a las resultantes de los análisis de riesgos y evaluaciones de impacto;
c) comunicar de modo inmediato a su responsable interno cualquier incidente de seguridad y/o brecha de datos personales;
d) cumplir las determinaciones que reciba de su responsable en orden a la finalización del tratamiento y a la destrucción segura de los datos, en su caso;
e) cuantas otras funciones y responsabilidades puedan serles asignadas por el responsable interno del tratamiento en materia de seguridad de la información y protección de datos personales.

Artículo 19. *Usuarios en seguridad de la información y del tratamiento de datos personales.*

1. Son usuarios todas las personas que tengan asignadas funciones en materia de seguridad de la información y protección de datos de carácter personal.

2. Todo el personal implicado en razón de sus respectivas competencias y funciones debe cumplir las obligaciones previstas con carácter general para el uso de recursos TIC y sistemas de información de la Universidad de Zaragoza.

3. Todo el personal implicado en razón de sus respectivas competencias y funciones debe cumplir las siguientes obligaciones en materia de tratamiento y protección de datos personales:
a) Realizar el tratamiento de datos de acuerdo con la normativa vigente y de esta Política de Seguridad de la Información y de Protección de Datos.
b) En el caso en que le corresponda recabar datos de carácter personal, hacerlo de acuerdo con el procedimiento establecido por el gerente de la Universidad en su calidad de máximo responsable por delegación del rector en materia de protección de datos.
c) Respetar las finalidades de cada tratamiento.
d) Informar al responsable o al encargado interno del tratamiento de cualquier incidencia detectada en el tratamiento de datos.
e) Responder con la máxima celeridad a los requerimientos en materia de tratamiento de datos de los responsables internos de tratamiento, encargados internos de tratamiento y responsable de seguridad.
f) Cumplir con las medidas de seguridad adoptadas de acuerdo con lo que se especifica en el documento de autorización del tratamiento y, en su caso, según las indicaciones del responsable interno del tratamiento.
g) Respetar los procedimientos establecidos en materia de atención a los ejercicios de información, acceso, rectificación y cancelación, cesiones de datos y creación y modi-

csv: BOA20220726001

ficación de tratamientos, así como cualquier otro procedimiento interno que se establezca en esta materia.

h) Respetar el régimen de tratamiento y comunicación de datos personales establecido al efecto.

i) Respetar los deberes de secreto profesional y confidencialidad de la información a la que tengan acceso aún después de dejar de ocupar su puesto de trabajo; en particular cada usuario será responsable de la confidencialidad de su contraseña personal sobre la que debe guardar reserva absoluta. Los usuarios accederán al sistema utilizando siempre el propio identificador.

j) Consultar al encargado o al responsable interno del tratamiento sobre las dudas que surjan sobre tratamiento de datos.

Artículo 20. *Unidad de Protección de Datos.*

1. La Unidad de Protección de Datos es la unidad organizativa encargada de colaborar con el gerente en la supervisión de los tratamientos de datos de carácter personal que se realizan en la Universidad.

2. Le corresponden las siguientes funciones:

a) Asesorar e informar a los miembros de la comunidad universitaria en materia de protección de datos.

b) Aplicar los protocolos y procedimientos autorizados por el gerente en materia de protección de datos personales.

c) Informar, junto con el Jefe de Proyecto de la Seguridad de la Información sobre la cumplimentación y medidas de seguridad a aplicar en los distintos tratamientos de datos.

d) Recibir y tramitar las peticiones que versen sobre ejercicio de derechos en materia de protección de datos personales, proponiendo al gerente su resolución.

e) Recibir y tramitar las peticiones de comunicación de datos, dentro de la propia Universidad o a terceros, proponiendo al gerente la resolución que proceda.

f) Recibir y tramitar las peticiones de autorización, modificación o supresión de tratamientos de datos, proponiendo al gerente la resolución que proceda.

g) Incorporar los tratamientos autorizados al Registro de Actividades de Tratamiento y llevar el Inventario de Tratamientos, manteniéndolo permanentemente actualizado.

h) Supervisar, junto con el Jefe de Proyecto de la Seguridad de la Información, la efectiva aplicación de las indicaciones y medidas de seguridad autorizadas para cada tratamiento. En particular, vigilar la efectiva terminación de los tratamientos que sean temporales y la destrucción segura de los datos, en su caso.

i) Realizar, junto con el Jefe de Proyecto de la Seguridad de la Información, las evaluaciones de riesgos en materia de protección de datos personales y, en su caso, las evaluaciones de impacto que procedan.

j) Llevar la página de protección de datos de la Universidad ofreciendo en ella toda la información pertinente, incluyendo los distintos protocolos de actuación y el Inventario de Actividades de Tratamiento.

Artículo 21. *El Delegado de Protección de Datos.*

1. El Delegado de Protección de Datos es la persona designada por el Rector que actúa como garante del cumplimiento de la normativa de protección de datos en la Universidad y ejerce sus funciones con independencia y confidencialidad.

2. Le corresponden las siguientes funciones:

a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de las restantes disposiciones en materia de protección de datos;

b) Supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 RGPD;

d) Cooperar con la autoridad de control;

e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

csv: BOA20220726001

3. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

4. El Delegado de Protección de Datos actuará en coordinación con la Unidad de Protección de Datos y con el Jefe de Proyecto de la Seguridad de la Información en todos los aspectos referidos a los tratamientos de datos que se realizan en la Universidad.

5. En el desempeño de sus tareas el Delegado de Protección de Datos tendrá acceso a todos los datos personales y procesos de tratamiento.

Artículo 22. *Resolución de conflictos.*

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad de la información y de Protección de Datos corresponderá su resolución, en última instancia, al Rector en su condición de máximo responsable de la institución.

2. El Rector estará asistido por el CSIPD y, cuando proceda, por el Delegado de Protección de Datos.

Artículo 23. *Obligaciones del personal.*

Todos los miembros de la comunidad universitaria tienen la obligación de conocer y cumplir lo previsto en esta Política de Seguridad de la Información y de Protección de Datos, así como en las normas y protocolos que la desarrollen.

Todo el personal que presta servicio en la Universidad tiene el deber de colaborar en la mejora de los principios y requisitos en materia de seguridad de la información y protección de datos personales, evitando y minorando los riesgos en la medida de sus respectivas responsabilidades.

Todos los órganos y unidades de la Universidad prestarán su colaboración en las actuaciones de implementación de la Política de Seguridad de la Información y de Protección de Datos.

Artículo 24. *Concienciación y formación.*

A todos los miembros de la comunidad universitaria se les informará adecuadamente sobre concienciación en materia de seguridad de la información y protección de datos personales y se desarrollarán actividades formativas para ello.

Se establecerá un programa de concienciación y formación continua para atender a todos los miembros de la Universidad, en particular a los de nueva incorporación, en materia de seguridad de la información y protección de datos.

Artículo 25. *Desarrollo normativo y revisión de la Política de Seguridad de la Información y de Protección de Datos.*

1. Corresponde al Consejo de Gobierno, a propuesta del Consejo de Dirección, la revisión y, en su caso, modificación de la Política de Seguridad de la Información y de Protección de Datos.

2. Corresponde al Consejo de Dirección, a propuesta del Comité de Seguridad de la información y de Protección de Datos, el desarrollo normativo de esta Política mediante la aprobación de las normas y procedimientos de actuación que se estimen adecuados.

Artículo 26. *Terceras partes.*

1. Cuando la Universidad de Zaragoza preste servicios de información y/o de tratamientos de datos por cuenta de terceros, se les hará partícipes de esta Política de Seguridad de la Información y de Protección de Datos, se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción frente a incidentes de seguridad.

2. Cuando la Universidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de Protección de Datos y de la normativa de seguridad que ataña a dichos servicios o información y quedarán sujetos a las obligaciones establecidas en esta normativa y en el respectivo documento suscrito entre las partes. Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y de protección de datos personales.

3. Cuando algún aspecto de la Política de Seguridad de la Información y de Protección de Datos no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre

csv: BOA20220726001

y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Disposición adicional primera.

Las menciones genéricas en masculino que aparecen en el articulado de este Acuerdo se entenderán referidas también a su correspondiente femenino.

Disposición adicional segunda.

La presente Resolución se publicará en el “Boletín Oficial de Aragón” y en el Boletín Oficial de la Universidad de Zaragoza.

Disposición derogatoria única.

Queda derogado el acuerdo del 24 de noviembre de 2016, del Consejo de Gobierno, por el que se aprueba la Política de Seguridad de la Información de la Universidad de Zaragoza, así como todo su desarrollo normativo posterior.

Disposición final única.

Esta Resolución entrará en vigor el día de su publicación en el “Boletín Oficial de Aragón”.

Zaragoza, 12 de julio de 2022.— El Rector, José Antonio Mayoral Murillo.

csv: BOA20220726001