Universidad de Alcalá

UNIVERSIDAD DE ALCALÁ, PATRIMONIO DE LA HUMANIDAD

POLÍTICA DE SEGURIDAD

DE LA INFORMACIÓN

Universidad de Alcalá

Elaborado por	Comisión de Administración Electrónica y Seguridad	**29/04/2020**
Aprobado por	Consejo de Gobierno	**15/07/2020**

ACUERDO DE 15 DE JULIO DE 2020, DEL CONSEJO DE GOBIERNO DE LA UAH POR EL QUE SE APRUEBA LA MODIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE ALCALÁ.

Universidad de Alcalá

CONTROL DE VERSIONES

Versión	Fecha	Modificado por	Descripción
1	30/03/2017		Aprobación por Acuerdo de Consejo de Gobierno de la UAH de 30 de marzo de 2017 (BOUAH marzo 2017)
2	18/07/2020	CAES	Modificación aprobada por Acuerdo del Consejo de Gobierno de la UAH de 15 de julio de 2020 (BOUAH julio 2020)

La Universidad de Alcalá (UAH) depende de los sistemas y tecnologías de la información para su funcionamiento en todas sus áreas de actuación.

El Esquema Nacional de Seguridad (ENS), aprobado mediante Real Decreto 3/2010, de 8 de enero y modificado por Real Decreto 951/2015, de 23 de octubre, define las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitan a los ciudadanos y las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Como medida prioritaria para una gestión integral de la seguridad, el ENS obliga a todos los órganos superiores de las Administraciones Públicas a disponer formalmente de su "Política de Seguridad de la Información".

Por su parte, el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales (LOPDGDD) y sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal; la Ley 40/2015 hace referencia a las medidas de seguridad que deben adoptarse de conformidad con lo dispuesto en el ENS en el funcionamiento electrónico del sector público, y la Ley 39/2015 recoge, entre los derechos de las personas en sus relaciones con la Administración Pública, el relativo a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones. Asimismo, el Real Decreto Ley 14/2019 establece las medidas relacionadas, esencialmente, con el desarrollo de las Administración electrónica y con la identificación electrónica de los ciudadanos en sus relaciones con las Administraciones públicas y los datos personales que obran en poder de las mismas.

El 30 de marzo de 2017 se aprobó la Política de Seguridad de la Información de la UAH, tal y como exigía la normativa vigente. Dados los avances tecnológicos y las modificaciones y aprobaciones normativas citadas anteriormente, la Política de Seguridad de la Información se ha visto sometida a una serie de cambios que debe recoger y que deben ser aprobados por Consejo de Gobierno. El presente texto viene a sustituir a la Política de Seguridad aprobada en 2017.

Por todo ello, el Consejo de Gobierno de la Universidad de Alcalá, en su sesión celebrada el día 15 de julio de 2020 acuerda aprobar la siguiente

POLÍTICA DE SEGURIDAD DE LA INFORMACION DE LA UAH

1. Introducción

La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección integral, apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

Con esta Política de Seguridad, la UAH asume los principios, requisitos y medidas definidos en el ENS.

La consolidación del uso de las tecnologías de la información y las comunicaciones en la UAH exige el establecimiento de un conjunto global de actividades y procedimientos para el tratamiento y gestión de los riesgos asociados a la seguridad de la información. La gestión de la seguridad de los sistemas de información es un proceso complejo que implica a toda la Organización y que incluye a personas, tecnologías, normas y procedimientos.

Por todo ello, el propósito de la presente Política de Seguridad de la Información de la UAH es establecer las bases de la fiabilidad con que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.

La UAH debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

La UAH debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del Real Decreto 3/2010, por medio del cual se aprueba el ENS.

Las medidas de **prevención** deben eliminar, o al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema, contemplando la disuasión y reducción de la exposición.

La UAH debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, implementará las medidas mínimas de seguridad determinadas por el ENS, el RGPD y la LOPDGD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de este principio, la UAH debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.
- Realizar las correspondientes evaluaciones de impacto y análisis de riesgos.

Las medidas de **detección** estarán acompañadas de medidas de **reacción,** para garantizar que los incidentes de seguridad se atajen a tiempo. Por ello, la UAH:

- Establecerá mecanismos para responder eficazmente a los incidentes de seguridad.
- Designará un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos para la colaboración y el intercambio de información relacionada con el incidente, incluyendo comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), especialmente con el CERT de las Administraciones Públicas (CCN-CERT).
- Establecerá los protocolos de actuación y de información a la Delegada de Protección de Datos en caso de una brecha de seguridad en materia de protección de datos personales con el fin de dar cumplimiento a la normativa e informar, si corresponde, tanto a la Agencia Española de Protección de Datos (AEPD) como a los interesados.

Las medidas de **recuperación** permitirán restaurar la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales. Para garantizar la disponibilidad de los servicios críticos, la UAH desarrollará planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2. Misión

De conformidad con lo establecido en el artículo 1.1 de los Estatutos de la Universidad de Alcalá, aprobados por Decreto 221/2003, de 23 de octubre, del Consejo de gobierno de la Comunidad de Madrid, la UAH es una institución de Derecho público encargada de la prestación del servicio público de la educación superior, que desarrolla mediante la investigación, la docencia y el estudio.

De forma estrechamente relacionada con el cumplimiento de esta misión, la infraestructura y los sistemas TIC de la UAH deben primar y fomentar las operativas abiertas, enfocadas a la funcionalidad, conectividad y

servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales. El análisis de riesgos determinará los niveles de seguridad asumibles según estas prioridades.

Además, la UAH reconoce que la colaboración y comunicación con otras Universidades, Administraciones Públicas y CERTs es un aspecto fundamental en su estrategia para la gestión de la seguridad.

3. Marco Normativo de la UAH

El marco normativo en el que la UAH desarrolla su actividad, es el siguiente:

- 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 (Reglamento General de Protección de Datos).
- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales.
- Ley 59/2003, de 19 de diciembre, de Firma electrónica.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en aquellos artículos que continúen vigentes, de conformidad con lo previsto en la disposición derogatoria única de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Decreto 221/2003, de 23 de octubre, por el que se aprueban los Estatutos de la Universidad de Alcalá.
- 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, en lo que no contradiga al RGPD y a la LOPDGDD.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en aquellos artículos que continúen vigentes, de conformidad con lo previsto en la disposición derogatoria única de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la Administración Electrónica.
- Cualquier otra normativa que pueda entrar en vigor tras la aprobación de la presente Política de Seguridad de la Información, y que resulte de aplicación.

4. Ámbito de aplicación

Esta Política de Seguridad de la Información será de aplicación a todos los recursos TIC corporativos de la UAH, particularmente, sobre todos aquellos sistemas que están relacionados con el ejercicio de derechos, con el cumplimiento de deberes, con el acceso a la información o al procedimiento administrativo por medios electrónicos o con cualquier actividad relacionada con la administración y gestión, la docencia y la investigación por parte de cualquier de los miembros de la comunidad universitaria y de terceros que quieran entablar una relación o contacto con la institución y sus integrantes.

Quedan fuera de este ámbito por no considerarse recursos TIC de la UAH, aquellos ordenadores o dispositivos personales financiados a título individual, no inventariados a nombre la Universidad, aunque pudieran ser usados ocasionalmente para labores propias de investigación o docencia.

No obstante, en el caso de que se acceda a la red corporativa mediante tales elementos o dispositivos, quedarán sujetos a las obligaciones establecidas en la presente Política de Seguridad. La Universidad se reserva el derecho a controlar el acceso y en su caso a retirarlo, respetando los derechos fundamentales de los usuarios, si no se cumplen unos requisitos mínimos de seguridad o existen evidencias de un incidente potencial de seguridad que pueda comprometer la seguridad de la información de los sistemas TIC o el buen nombre o imagen corporativa de la UAH.

5. Protección de Datos de Carácter Personal

La UAH cuenta con las medidas oportunas para garantizar el nivel de seguridad requerido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

El "Documento de Seguridad en materia de Protección de Datos de la Universidad de Alcalá", elaborado conforme a lo dispuesto en el RD 1720/2007 (última versión revisada por la Comisión de Protección de Datos de la Universidad de Alcalá con fecha 25 de mayo de 2016), sigue vigente en lo que no contradiga al RGPD y a la LOPDGDD, y estará disponible en la página web de protección de datos (https://portal.uah.es/portal/page/portal/proteccion_datos). El Documento será accesible exclusivamente a las personas autorizadas y designadas como Responsables de seguridad en materia de protección de datos para los ficheros que contienen datos personales de los niveles que el Real Decreto 1720/2007 calificaba de medio y alto. Dicho documento nombra los ficheros afectados por dicha clasificación, los responsables correspondientes y las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar las medidas de seguridad exigidas, así como las funciones y obligaciones del personal, reflejando las medidas técnicas y organizativas de la institución en materia de tratamiento de datos personales.

Todos los sistemas de información de la UAH se ajustarán a las medidas de seguridad requeridas por la normativa en función de la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad y previstos actualmente tanto por el RGPD como por la LOPDGDD.

Para garantizar dicha protección se han adoptado las medidas de seguridad que, en su momento, se preveían en el Real Decreto 1720/2007, que seguirán vigentes en lo que no contradigan a las medidas también previstas en el RGPD y en la LOPDGDD, que se sumarán a las anteriores.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la UAH. Todo ello, sin perjuicio de las obligaciones que para los denominados Encargados del tratamiento se recojan en los Acuerdos de confidencialidad o Acuerdos a firmar entre dichos Encargados y la Universidad como Responsable de los tratamientos de los datos de los miembros de la comunidad universitaria y llevados a cabo por la propia institución.

6. Organización de la Seguridad

6.1. Comisión de Administración Electrónica y Seguridad: Funciones y Responsabilidades

La Comisión de Administración Electrónica y Seguridad, creada por acuerdo del Consejo de Gobierno de la Universidad de Alcalá de fecha 15 de diciembre de 2016, coordina la Política de Seguridad de la Información en la Universidad de Alcalá y está compuesta por las siguientes personas:

- Presidente/a: El Rector o su Delegado para Administración Electrónica y Seguridad.
- Vocales:
    - Secretaria/o General.
    - Gerente.
    - Delegada/o de Protección de Datos.
    - Director/a de los Servicios Informáticos.
    - Jefe/a de Sección de Archivo Universitario y Registro.
    - Jefe de Servicio Seguridad TIC
- Secretario/a: Jefe/a de Servicio de Nuevos Procesos Administrativos y Administración Electrónica.
- La Comisión podrá incorporar a sus reuniones a las personas que considere oportuno en función de los temas a tratar. Estas personas podrán asistir con voz, pero sin voto.

Las responsabilidades, en el marco del ENS, son las siguientes:

- Responsable de la Información y de los Tratamientos de Datos Personales Secretario/a General.
- Responsable del Servicio: Gerente.
- Responsable de Seguridad: Delegado del Rector para Administración Electrónica y Seguridad.
- Responsable de la supervisión y asesoramiento en materia de protección de datos personales: Delegado/a de Protección de Datos.
- Responsable del Sistema: Director de los Servicios Informáticos.
- Administrador de Seguridad: Jefe de Servicio Seguridad TIC.

En materia de seguridad, la Comisión tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Consejo de Gobierno.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la UAH en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Revisar regularmente la Política de Seguridad de la Información y realizar propuestas de mejora, y someterlas al Consejo de Gobierno para su aprobación.
- Elaborar circulares o instrucciones en desarrollo de lo dispuesto en la Política de Seguridad de la Información de la UAH.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de la seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la UAH y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la UAH. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC, desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando al órgano competente aquellos casos en los que no tenga suficiente autoridad para decidir.

6.2. Roles: Funciones y Responsabilidades

De acuerdo con el artículo 10 del RD 3/2010 por el que se aprueba el ENS y la Guía de Seguridad CCN-STIC-801, se definen los siguientes roles y responsabilidades.

6.2.1. Responsable de la Información / Responsable del Tratamiento

El Secretario General, como responsable de la Información y de los Ficheros de datos de carácter personal de la UAH, tendrá las siguientes funciones y responsabilidades:

- Velar por el buen uso de la información y su protección.
- Ser el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

6.2.2. Responsable del Servicio

El Gerente, como responsable del Servicio, tendrá las siguientes funciones y responsabilidades:

- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

6.2.3. Delegado/a de Protección de Datos

La/el Delegada/o de Protección de Datos tendrá las siguientes funciones y responsabilidades:

- 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 la LOPDGDD.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, en la LOPDGDD y de las políticas del responsable o del encargado del tratamiento 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

- Cooperar con la AEPD.
- Actuar como punto de contacto de la AEPD para cuestiones relativas al tratamiento, incluida la consulta previa y realizar consultas.
- Actuar como interlocutor del Responsable o Encargando del tratamiento ante la AEPD y las Autoridades autonómicas de protección de datos.
- Notificación de brechas de seguridad, en su caso, ante la AEPD y afectados.
- Emitir Recomendaciones en el ámbito de sus competencias.

6.2.4. Responsable de Seguridad

Delegado del Rector para Administración Electrónica y Seguridad, como responsable de la Seguridad, tendrá las siguientes funciones y responsabilidades:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- 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.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes a la Comisión de Administración Electrónica y Seguridad.
- Contactar, cuando sea necesario, con el Centro Criptográfico Nacional (CCN), que ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad de la información.

6.2.5. Responsable del Sistema

El Director de los Servicios Informáticos, como responsable del Sistema, tendrá las siguientes funciones y responsabilidades:

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.

- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

6.2.6. Administrador de Seguridad

El Jefe de Servicio Seguridad TIC, como Administrador de Seguridad, tendrá las siguientes funciones y responsabilidades:

- Gestionar las medidas de seguridad aplicables al sistema de información.
- Gestionar los mecanismos y servicios de seguridad del sistema de información.
- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- 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.
- 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.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.2.7. Procedimiento de Designación

El desempeño de cualquiera de las responsabilidades y funciones definidas en esta Política de Seguridad de la Información vendrá determinado por el acceso a los diferentes cargos que han quedado vinculados a ella. En el caso de que por modificación de la delegación de competencias del Rector o de la Relación de Puestos de Trabajo desapareciese o cambiara de denominación alguno de los puestos definidos en esta Política, será competencia del Rector o del Consejo de Gobierno, según corresponda, oída la Comisión de Administración Electrónica y Seguridad, asignar las funciones y responsabilidades dentro del marco establecido por esta Política. Todo ello sin perjuicio de lo que dispongan las normas vigentes para la composición de la Comisión y respecto de sus funciones, como es el caso de la figura del Delegado/a de Protección de Datos prevista legalmente y cuyo nombramiento depende única y exclusivamente del Rector.

7. Obligaciones del Personal

Todos los miembros de la UAH tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad de la Comisión de Administración Electrónica y Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la UAH recibirán la formación precisa en materia de seguridad para cumplir con esta Política, así como la formación básica y necesaria en materia de protección de datos personales. Se

establecerá un programa de formación continua para atender a todos los miembros de la Universidad, en particular a los de nueva incorporación.

En el caso de detectarse incumplimiento de las medidas contempladas en esta Política de Seguridad, o en los documentos de desarrollo, se podrán aplicar medidas preventivas y correctoras, encaminadas a proteger los sistemas TIC, sin incurrir en la tipificación de infracciones, con pleno respeto a los derechos fundamentales, pero sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas, así como para un correcto tratamiento de los datos personales, en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es una primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

En relación con el personal que trate datos personales en su actividad diaria, se enviarán y publicarán Circulares informativas detallando las normas a cumplir y las consecuencias de no hacerlo. Serán los Responsables de los diferentes Servicios o Unidades los responsables de contribuir a hacer llegar a su personal las citadas Circulares y de velar por el correcto cumplimiento en su Servicio o Unidad.

8. Desarrollo de la Política de Seguridad de la Información

En cumplimiento con lo dispuesto en la legislación aplicable, esta Política de Seguridad de la Información ha de ser objeto de desarrollo para que queden perfectamente definidas las medidas de seguridad específicas para los distintos ámbitos contemplados. En todo caso, las diferentes políticas, normativas y regulaciones específicas que resulten de tal desarrollo deberán respetar lo dispuesto en la presente Política de Seguridad y derivarse de la misma.

De acuerdo con lo anterior, la UAH establecerá un marco normativo propio en materia de seguridad, estructurado en diferentes niveles, a fin de garantizar que los objetivos y medidas establecidos en el presente documento tengan un desarrollo específico:

1. Primer nivel: Política de Seguridad de la Información.
2. Segundo nivel: las normativas generales de seguridad que emanan de la Política de Seguridad de la Información.
3. Tercer nivel: los procedimientos de seguridad, que son el conjunto de documentos que describen paso a paso cómo realizar una cierta actividad.
4. Cuarto nivel: documentación de buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.

La Política de Seguridad de la Información será aprobada por el Consejo de Gobierno de la UAH, al igual que las normativas generales de seguridad que emanan de la Política de Seguridad de la Información, a propuesta de la Comisión de Administración Electrónica y Seguridad. Aquellos procedimientos de seguridad que se estimen oportunos y relacionados con la Política de Seguridad de la Información, serán aprobados por la Comisión de Administración Electrónica y Seguridad, a propuesta del Responsable de la Seguridad de la Información.

9. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos y deberá tenerse en cuenta lo previsto para dichos análisis y evaluaciones de impacto regulados tanto en el RGPD como en la LOPDGDD, tomando como referencia las Guías, Directrices y Aplicaciones elaboradas por las Autoridades de control competentes al respecto. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años.

- Cuando cambie sustancialmente la información manejada.
- Cuando cambien sustancialmente los servicios prestados.
- Cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades graves que impliquen un cambio sustancial en las salvaguardas del sistema.
- Especialmente, cuando se traten datos especialmente protegidos o categorías especiales de datos así reconocidos tanto en el RGPD como en la LOPDGDD, sin perjuicio de otras situaciones previstas igualmente en la normativa de protección de datos vigente.

Para la armonización de los análisis de riesgos, la Comisión de Administración Electrónica y Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diversos servicios prestados. Dicha Comisión dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. Terceras partes

Cuando la UAH preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UAH utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. En todo caso, entre la Universidad, como Responsable del tratamiento de datos personales de la comunidad universitaria, y los citados terceros, como Encargados del tratamiento, deberá mediar el preceptivo Acuerdo de confidencialidad. Se deberá recordar al tercero que la falta de firma de dicho Acuerdo es una infracción en materia de protección de datos personales.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre 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.

En relación con los sistemas de identificación electrónicos entre las Administraciones públicas previstos en la normativa vigente sobre procedimiento administrativo y firma electrónica, y régimen jurídico del sector público, así como los sistemas de información y comunicaciones, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión se deberán encontrar ubicados en territorio de la UE, y para el caso de que se trate de información relativa a datos especialmente protegidos, se encontrarán en territorio español, sin que sea posible su transferencia internacional, salvo que medie declaración de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de obligaciones internacionales.

11. Aprobación y Entrada en Vigor

Esta Política de Seguridad de la Información de la UAH entrará en vigor al día siguiente al de su publicación en el Boletín Oficial de la UAH.