* * *

Acuerdo del Consejo de Gobierno de 21 de junio de 2016, por el que se aprueba el Documento de Política de Seguridad de la Información de la Universidad de Cádiz.

A propuesta de la Secretaría General, el Consejo de Gobierno, en su sesión ordinaria de 21 de junio de 2016, en el punto 22º. del Orden del Día, aprobó por asentimiento el Documento de Política de Seguridad de la Información de la Universidad de Cádiz, en los siguientes términos:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CÁDIZ

(Aprobada por Acuerdo de Consejo de Gobierno de 21 de junio de 2016)

La sociedad de la información y la administración electrónica se basa en la necesaria confianza de los ciudadanos en que la relación a través de medios electrónicos está debidamente garantizada, sobre todo, lo concerniente a que los sistemas de información prestan sus servicios y custodian la información de acuerdo con sus especificaciones funcionales.

En este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

1 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

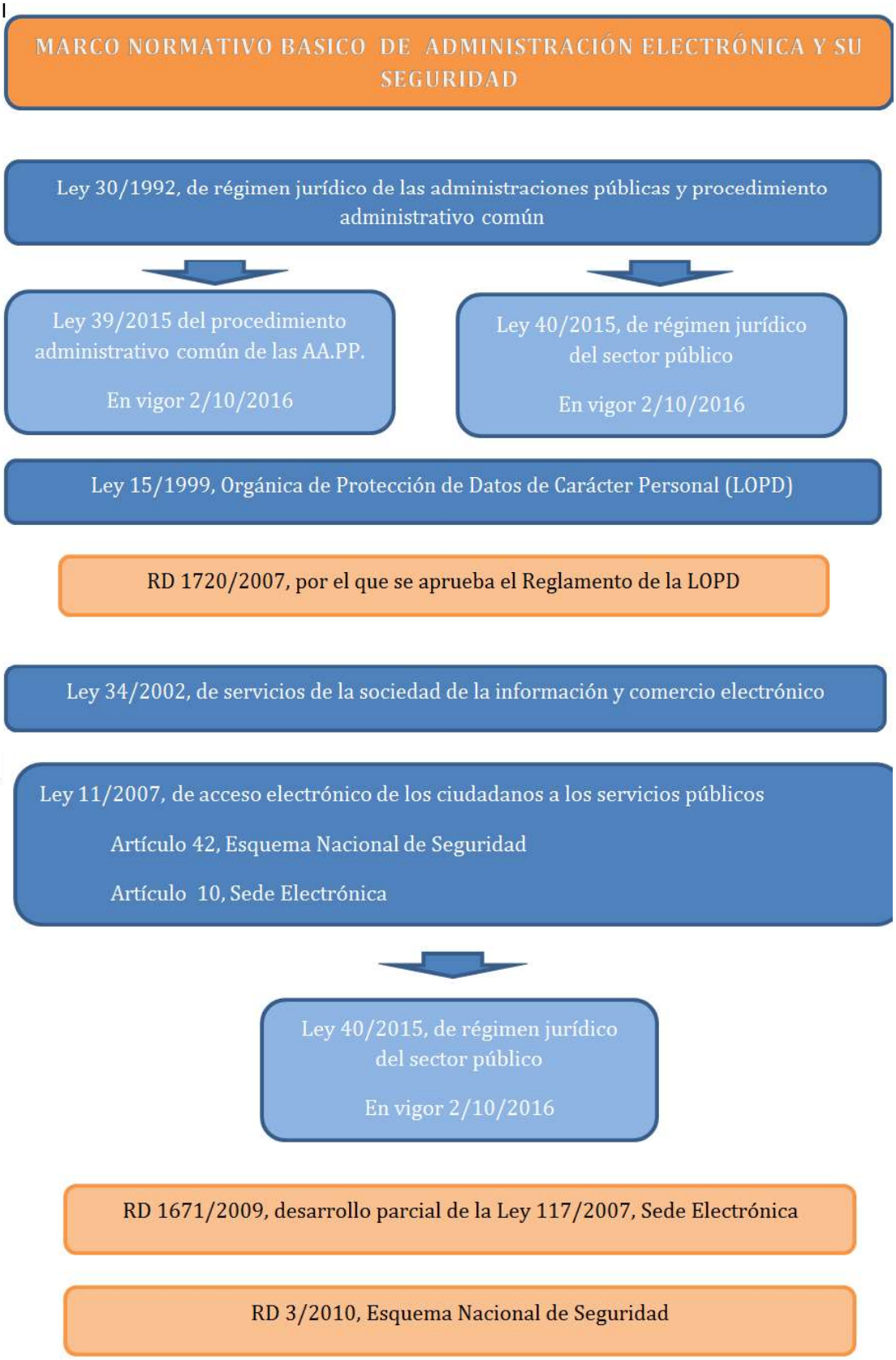
La Universidad de Cádiz depende de los sistemas de Tecnologías de Información y Comunicaciones (TIC) para dar respuesta a su misión de ofrecer a la comunidad universitaria servicios adecuados, protegidos de la destrucción, indisponibilidad, manipulación o revelación no autorizada de la información.

El presente documento establece el compromiso de la Universidad con la seguridad de los sistemas de información, definiendo los objetivos y criterios básicos para su tratamiento, sentando los pilares del marco normativo de seguridad de esta administración y la estructura organizativa y de gestión que velará por su cumplimiento con el objetivo de garantizar, en la mejor medida posible, la confidencialidad, la integridad y disponibilidad de sus sistemas de información, de las comunicaciones y de los servicios telemáticos con el fin de proporcionar a la comunidad universitaria unos servicios fiables, de calidad y de confianza para permitirles el ejercicio de derechos y el cumplimiento de deberes a través de estos medios tal y como exige la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

2 MARCO NORMATIVO

El Real Decreto 3/2010, , de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS) establece el marco regulatorio de la Política de Seguridad de la Información que debe ser plasmada en un documento accesible y comprensible para todos los miembros, definiendo lo que significa seguridad de la información en la Universidad, y que rige la forma en que esta gestiona y protege la información y los servicios que considera críticos.

El marco normativo de la Universidad de Cádiz en la materia está constituido, además de por la legislación universitaria, por las normas específicas en materia de Seguridad de la Información, disponibles en la página de administración electrónica (http://ae.uca.es); cuyo esquema básico es el siguiente:


MARCO NORMATIVO BASICO DE ADMINISTRACIÓN ELECTRÓNICA Y SU SEGURIDAD
Ley 30/1992, de régimen jurídico de las administraciones públicas y procedimiento administrativo común
Ley 39/2015 del procedimiento administrativo común de las AA.PP.
En vigor 2/10/2016
Ley 40/2015, de régimen jurídico del sector público
En vigor 2/10/2016
Ley 15/1999, Orgánica de Protección de Datos de Carácter Personal (LOPD)
RD 1720/2007, por el que se aprueba el Reglamento de la LOPD
Ley 34/2002, de servicios de la sociedad de la información y comercio electrónico
Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos
Artículo 42, Esquema Nacional de Seguridad
Artículo 10, Sede Electrónica
Ley 40/2015, de régimen jurídico del sector público
En vigor 2/10/2016
RD 1671/2009, desarrollo parcial de la Ley 117/2007, Sede Electrónica
RD 3/2010, Esquema Nacional de Seguridad

3 PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los principios que conforman la Política de Seguridad de la Universidad de Cádiz son los siguientes:

Universalidad. La política de seguridad se aplica a todos los sistemas TIC (tanto servicios como información) y en particular a todos los sistemas enmarcados en el ámbito de la Administración Electrónica. Deberá ser aplicado por todos los centros, departamentos, áreas y unidades administrativas, órganos, entidades creadas o participadas mayoritariamente por la Universidad, por todos los miembros de la comunidad universitaria (personal de administración y servicios, personal docente e investigador y estudiantes) que acceden a los sistemas de información de la Universidad de Cádiz, así como por los organismos o empresas y profesionales colaboradores.

Confidencialidad. La información debe ser protegida contra accesos y alteraciones no autorizadas. Todos los que accedan a ella deberán guardar sigilo sobre su contenido en los términos previstos en la legislación aplicable. Se establecerán los protocolos de acceso adecuados.

Integridad y trazabilidad. Tanto la información como los recursos donde reside, viaja o es procesada la información deben estar adecuadamente protegidos contra accesos o alteraciones no autorizadas. El tratamiento de datos de carácter personal siempre se realizará de acuerdo a la legislación aplicable en todo momento.

Disponibilidad. La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.

Proporcionalidad. Las medidas de seguridad implantadas estarán en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se puedan producir en ella. Se seguirán como mínimo las medidas de seguridad aplicables y exigidas por el ENS.

Adaptabilidad. La seguridad de la información debe controlarse de forma constante y debe revisarse periódicamente para responder a las necesidades detectadas

Información y formación. La política de seguridad debe ser conocida y aplicada por todos los miembros de la comunidad universitaria, por lo que deberá recibir la formación adecuada. Igualmente deberán conocer y aplicar aquellos aspectos del desarrollo de la política de seguridad que les sean de aplicación, recibiendo la formación necesaria.

Responsabilidad. Cualquier persona que tenga acceso a la información de la Universidad está sometida a la presente política de seguridad, siendo responsable de su cumplimiento. En caso de incumplimiento de los deberes previstos en la misma se le exigirá la responsabilidad de acuerdo con la normativa que le resulte de aplicación.

4 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.1. ESTRUCTURA REGULATORIA

La normativa relativa a la Seguridad de la Información estará clasificada en tres niveles de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- **Primer nivel**: Política de Seguridad de la Información

El presente documento, de obligado cumplimiento, aprobado por el Consejo de Gobierno.

- **Segundo nivel**: Normativas o Políticas de Seguridad específicas.

Describe el uso correcto de equipos, servicios e instalaciones, lo que se considerará uso indebido, así como la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Estos documentos son propuestos por el Comité de Seguridad y aprobados por el Consejo de Gobierno.

- **Tercer nivel**: Procedimientos de Seguridad e Instrucciones Técnicas

Detallan de forma clara y precisa como llevar a cabo las tareas habituales, quien debe hacer cada tarea y como, identificar y reportar comportamientos anómalos.

Estos documentos técnicos son aprobados por el Comité de Seguridad a propuesta del Responsable de Seguridad.

El Responsable de Seguridad es responsable en su ámbito de actuación de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a ella.

Se podrán seguir en todo momento los procedimientos STIC, las normas STIC, las instrucciones técnicas STIC y las guías CCN–STIC de las series 400, 500 y 600.

4.2. ESTRUCTURA ORGANIZATIVA

4.2.1. Comité de Seguridad

El Comité de Seguridad coordinará las actividades y controles de seguridad establecidos en la Universidad y velará por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos y seguridad.

El Comité estará compuesto por los siguientes miembros:

- El Responsable de la Información o persona en quien delegue, que asumirá la Presidencia.
- Un miembro de la Secretaría General con responsabilidad en materia de administración electrónica, que asumirá la Secretaría.
- El Responsable de Seguridad.
- Dos responsables de los servicios.

- Los miembros del equipo de gobierno con competencias en materia de seguridad de la información.
- El Gerente o persona en quien delegue.
- Los Responsables del Sistema.

Los miembros que componen el Comité de Seguridad, en caso de no poder asistir a las reuniones del mismo, podrán ser sustituidos por quienes designen.

A las sesiones del Comité de Seguridad podrá ser convocada, con voz y sin voto, cualquier persona que se estime conveniente para el tratamiento de los puntos del orden del día.

Son funciones del Comité de Seguridad:

- Elaborar propuestas de modificación y actualización de la presente Política.
- Velar por el cumplimiento y difusión de la presente Política, promoviendo actividades de concienciación y formación en materia de seguridad.
- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de esta Política en toda la Universidad, así como aquellas que sean necesarias para la adecuación al ENS.
- Proponer para su aprobación por el Consejo de Gobierno las normativas de segundo nivel (Normativas de Seguridad).
- Aprobar los procedimientos de seguridad e instrucciones técnicas.
- Coordinar, supervisar y hacer seguimiento de las decisiones y actuaciones del Responsable de Seguridad.
- Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.
- Aprobar el informe anual de seguridad, del que se informará al Consejo de Gobierno.
- Identificar los responsables y responsabilidades en materia de seguridad de la información.
- Acordar todas aquellas decisiones que garanticen, en última instancia, la seguridad de la información y servicios de la Universidad, incluyendo las garantías de cumplimiento de la protección de los datos de carácter personal.
- Proponer y acordar la realización de revisiones independientes sobre la vigencia e implementación de la presente Política con el objetivo de garantizar que las prácticas en la Universidad reflejan adecuadamente sus disposiciones.

El Comité se reunirá con carácter ordinario cada seis meses, y con carácter extraordinario cuando lo decida la Presidencia.

4.2.2. Responsable de la Información

Conforme a los arts. 10 y 44 del ENS, el Responsable de la Información es la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

Esta responsabilidad recaerá en el Secretario General de la Universidad de Cádiz.

Son funciones del Responsable de la Información:

- Clasificar, junto con los responsables del servicio, la información conforme a los criterios y categorías establecidos en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).
- Junto al Responsable del Servicio, aceptar los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control. Esta función puede ser delegada.
- Velar por la inclusión en los contratos y convenios de las cláusulas que obliguen al cumplimiento de la normativa de protección de datos y de la seguridad de la información.

4.2.3. Responsable del Servicio

Conforme a los artículos 10 y 44 del ENS, el Responsable del Servicio es la persona que determina los requisitos de seguridad de los servicios prestados en cada una de las áreas dentro de su ámbito de actividad.

Los responsables de los servicios serán los contemplados en el Anexo I del presente documento, que podrá ser modificado por el Comité de Seguridad como consecuencia de las necesidades detectadas en las revisiones periódicas que realice.

Son funciones del Responsable del Servicio

- Determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).
- Junto al Responsable de la Información, aceptar los riesgos residuales calculados en el análisis y realizar su seguimiento y control. Esta función puede delegarse.

4.2.4. Responsable de Seguridad

Conforme al art.10 del ENS, el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Se designará un Responsable de Seguridad cuyo ámbito de responsabilidad será la información y servicios afectados por los sistemas de información gestionados por la Universidad, así como, si se considera oportuno, la relativa a lo establecido en el art. 95 del RLOPD y a lo detallado en el Documento de Seguridad LOPD de la Universidad.

Esta responsabilidad recaerá en el Director del Área de Informática en tanto no exista una figura específica a estos efectos en la organización de la Universidad de Cádiz.

Son funciones del Responsable de Seguridad:

- Supervisar el cumplimiento de la presente Política, y de sus normas y procedimientos derivados de ella.
- Proponer al Comité de Seguridad para su aprobación la normativa de seguridad de tercer nivel (Procedimientos de Seguridad e Instrucciones Técnicas).
- Establecer las medidas adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad siguiendo las directrices del Comité de Seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información concreta para la toma de decisiones.
- Ejecutar, directamente o delegando, las decisiones del Comité de Seguridad.
- Asesorar, en colaboración con los Responsables del Sistema, a los Responsables de los Servicios y de la Información en los correspondientes análisis de riesgos, y revisar el proceso de gestión de riesgos.
- Promover la realización de auditorías periódicas para verificar las obligaciones en materia de seguridad de la información y analizar los informes de auditoría resultantes.
- Asumir las funciones relativas a la funciones LOPD estipuladas en el Documento de Seguridad, si procede.
- Determinar la resolución de incidentes de seguridad detectados en los servicios o sistemas de información de la Universidad.
- Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a lo exigido por el ENS.
- Mantener contactos periódicos con grupos de interés, otras entidades u organismos que resulten relevantes en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener su seguridad.
- Junto al Responsable de la Información y contando con la participación y asesoramiento de los Responsables del Sistema, se encargará de realizar los correspondientes análisis de riesgos y de seleccionar las salvaguardas a implantar.
- Coordinar los conocimientos y las experiencias disponibles en la Universidad con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

4.2.5. Responsables del Sistema

El Responsable del Sistema es el titular responsable del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.

Esta responsabilidad recaerá en las personas que tengan asignadas esas funciones en el Área de Informática.

Son funciones de los Responsables del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, sus especificaciones, instalación, y verificar su correcto funcionamiento.
- Implantar las medidas de seguridad exigidas por el ENS sobre los sistemas de información y conforme a la categoría de estos.
- Integrar adecuadamente las medidas de seguridad dentro del marco general de seguridad.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de la Información y del Servicio afectado.
- Elaborar y mantener los Planes de Continuidad de los Sistemas de Información.

4.2.6. Ejercicio de las competencias

Las competencias previstas en el presente documento podrán ser encomendadas en los términos y condiciones previstos en la guía CCN-STIC 801 o la que la sustituya. En caso de conflicto de competencias, y de acuerdo al principio de jerarquía que rige en la Universidad, este será resuelto por el superior jerárquico. En caso de no poder resolverse el conflicto aplicando el criterio anterior, prevalecerá en todo caso la decisión del Comité de Seguridad.

En caso de que exista conflicto entre los responsables que componen la estructura organizativa de la presente Política y lo estipulado en el Documento de Seguridad LOPD, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de datos de carácter personal.

Las responsabilidades definidas en este documento de Política de Seguridad, y en el ENS, vendrán determinadas por el desempeño de los diferentes cargos y/o destinos, estatutarios o no, a los que se atribuyen.

5 CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN

La Universidad asume el compromiso de controlar sus riesgos de seguridad así como de dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas). Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables del Sistema realizarán, con periodicidad al menos anual, un análisis de

riesgos cuyas conclusiones se plasmarán en actuaciones para tratar de mitigar el riesgo, o incluso replantear la seguridad de los sistemas en caso necesario.

Se realizarán análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

- Se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.
- Ocurran incidentes graves de seguridad que puedan repercutir en las medidas de seguridad requeridas.
- Se reporten vulnerabilidades graves que puedan repercutir en las medidas de seguridad requeridas.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y al Comité de Seguridad.

6 APLICACIÓN DE LA POLÍTICA DE SEGURIDAD

La presente Política de seguridad debe ser conocida y aplicada por todos los miembros de la comunidad universitaria, por lo que deberá recibir la formación adecuada. Igualmente deberán conocer y aplicar aquellos aspectos del desarrollo de la política de seguridad que les sean de aplicación, recibiendo la formación necesaria.

Todo el personal que se incorpore a la Universidad o vaya a tener acceso a algunos de los sistemas de información gestionada por ellos deberá ser informado de la presente Política.

Para lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todos los miembros de la Universidad y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el art. 5 del ENS, la Universidad propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren incluyéndose estas actividades en el Plan de Formación anual del organismo.

Es responsabilidad del Comité de Seguridad disponer de los medios necesarios para que la información llegue a todos los afectados, para ello tanto el Comité de Seguridad como el Responsable de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad.

Por tanto, cualquier persona que tenga acceso a la información de la Universidad está sometida a la presente Política de seguridad, siendo responsable de su cumplimiento. En caso de incumplimiento de los deberes previstos en la misma se le exigirá la responsabilidad de acuerdo con la normativa que le resulte de aplicación pudiendo dar lugar al inicio de medidas disciplinarias.

Tratamiento de datos de carácter personal

Para el tratamiento de los datos de carácter personal en los sistemas de información de la Universidad se seguirá en todo momento lo desarrollado en el Documento de Seguridad y su documentación asociada conforme a lo exigido en el capítulo II del Título VIII de

las medidas de seguridad en el tratamiento de datos de carácter personal del 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.

7 REVISIÓN DE LA POLÍTICA DE SEGURIDAD

El Comité de Seguridad velará por la revisión, distribución y cumplimiento de la presente Política de Seguridad.

La revisión de la Política y de sus normativas y procedimientos derivados se realizará al menos una vez al año, así como cada vez que ocurran cambios significativos en los elementos de los sistemas de información que pueden afectarle directa o indirectamente, distribuyéndose a todo el personal afectado.

La versión más actualizada de la Política de Seguridad estará disponible en la sede electrónica de la Universidad de Cádiz.

8 APROBACIÓN Y ENTRADA EN VIGOR

El presente documento sobre Política de Seguridad entrará en vigor al día siguiente de su publicación en el BOUCA.

9 DISPOSICIÓN ADICIONAL

Las referencias a personas, cargos y colectivos figuran en el presente documento en género masculino, como género gramatical no marcado.

ANEXO I

RESPONSABLES DE LOS SERVICIOS (*)	
Coordinadora de Gestión de Investigación	Servicios Apoyo a la Investigación
Director del Área de Atención al Alumnado:	Servicios Área de Atención Alumnado.
Director del Área de Biblioteca y Archivo	Servicios e Información de la Biblioteca Virtual y Servicios e Información del Archivo
Director del Área de Deportes	Servicios Área de Deportes
Director del Área de Economía	Servicios del Área de Economía
Director del Área de Informática	Campus Virtual (Cursos y Formación), Servicio Correo Electrónico Institucional
Director del Área de Personal	Servicios del Área de Personal
Director del Gabinete Jurídico	Información del Gabinete Jurídico
Director del Servicio de Actividades Culturales	Otra Formación
Director del Servicio de Prevención	Servicios del Servicio de Prevención
Gerente	Otros Trámites Oficina Virtual, Buzón de Atención al Usuario (BAU)
Jefa de la Unidad de Prácticas de Empresa y Empleo	Servicio de Prácticas
Jefe de la Oficina de Coordinación de Posgrado	Servicios Posgrado
Subdirectora de la Oficina de Relaciones Internacionales	Oficina de Relaciones Internacionales
Director del Gabinete de Comunicación y Marketing	Página Web

(*) El presente listado podrá ser modificado por el Comité de Seguridad.