UCA Universidad de Cádiz

Área de Sistemas de Información

Ed. CITI. Avda. Rep. Saharaui s/n
Campus del Río S. Pedro
11519 Puerto Real (Cádiz)
Tel. 956 01 6400
https://sistinfo.uca.es

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CÁDIZ

ÍNDICE

1. Aprobación y entrada en vigor de la Política de Seguridad (PSI) de la Universidad de Cádiz

Texto aprobado el día xxx de xxxx de 2025 por acuerdo del Consejo de Gobierno de la Universidad de Cádiz, y publicado en el Boletín Oficial de la Universidad de Cádiz (BOUCA) n.º xxx el día xxx de xxx de 2025.

El presente Documento de Política de Seguridad de la Información (DPSI) entra en vigor al día siguiente de su publicación en el BOUCA, hasta que sea reemplazado por una nueva versión, y está publicado en la página web de la sede electrónica de la universidad: https://sedelectronica.uca.es

2. Introducción

Esta Política instituye el compromiso de la Universidad de Cádiz con la seguridad de sus sistemas de Tecnologías de la Información y Comunicaciones (sistemas TIC), definiendo los criterios básicos para su tratamiento, el marco normativo de seguridad de esta institución y la estructura organizativa y de gestión que velará por su cumplimiento, con el objetivo de garantizar, en la mejor medida posible, la confidencialidad, integridad y disponibilidad de sus sistemas de información, las comunicaciones y los servicios telemáticos, proporcionando unos servicios fiables, de calidad y confianza a la comunidad universitaria y a la ciudadanía.

3. Misión de la Universidad de Cádiz

La Universidad de Cádiz depende de los sistemas TIC para cumplir su misión de dar a la comunidad universitaria los servicios adecuados a su función, protegidos de la destrucción, interrupción, manipulación o revelación no autorizada de la información, y de ofrecer a la ciudadanía la realización de trámites *on line* y nuevas vías de participación que le permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Estos sistemas TIC deben ser administrados con diligencia, aplicando las medidas de seguridad adecuadas de prevención frente a incidentes, accidentales o deliberados, y contra las amenazas con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información y los servicios.

Para hacer frente a estas amenazas y dar una respuesta efectiva a los posibles incidentes, se requiere de una estrategia que se adapte a los cambios en las condiciones del entorno, realizando un seguimiento continuo de los niveles de prestación de los servicios, monitorizando y analizando las vulnerabilidades reportadas.

La seguridad en los sistemas TIC es una parte integral de todo el ciclo de vida del sistema, desde su diseño hasta su retirada de servicio, incluyendo las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y sus necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de las ofertas y en los pliegos de licitación para todos los proyectos TIC.

4. Principios básicos de Seguridad de la Información

Los principios básicos son directrices fundamentales de seguridad que deben estar presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes principios:

- **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 esté coordinada e integrada con el resto de iniciativas estratégicas de la organización de modo coherente y eficaz.

- **Diferenciación de responsabilidades**: Se designará quién es el *Responsable de la Información*, el *Responsable del Servicio*, el *Responsable del Sistema*, y el *Responsable de la Seguridad*, cada uno con las atribuciones que se les asignan en esta Política. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
- **Seguridad integral y por defecto**: La seguridad se entenderá como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas TIC, procurando evitar cualquier actuación ocasional o tratamiento coyuntural; debe considerarse como parte de la operativa habitual, estando presente y aplicándose por defecto, desde el diseño y configuración inicial de los sistemas TIC, durante todo su ciclo de vida.
- **Gestión de riesgos**: El análisis y gestión de riesgos serán parte esencial del proceso de seguridad, manteniendo el entorno controlado, minimizando los riesgos hasta niveles aceptables con el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de la información, se deben tener en cuenta los riesgos específicos derivados del tratamiento de datos de carácter personal.
- **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos, y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y los sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

5. Objetivos de la Seguridad de la Información

La Universidad de Cádiz establece como objetivos de seguridad de la información los siguientes:

- **Gestión de activos de información**: Los activos de información se encontrarán inventariados y categorizados, y estarán asociados a un responsable.
- **Concienciación**: Se impulsarán acciones de formación y concienciación en la seguridad de la información, para que cualquier persona que acceda a los activos de información conozca sus responsabilidades y, de este modo, se reduzca el riesgo derivado de un uso indebido.
- **Seguridad física**: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad, y a salvo frente a potenciales amenazas físicas o ambientales.
- **Seguridad en las comunicaciones**: La información que se transmita a través de las redes de comunicaciones deberá estar adecuadamente protegida, teniendo en cuenta su nivel de privacidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- **Control de acceso**: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información, mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, aplicando el principio del *mínimo privilegio*. Además, quedará registrada la utilización del sistema, con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado y conforme a la actividad de la organización.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información**: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- **Gestión de los incidentes de seguridad**: Se implantarán protocolos para la correcta identificación, notificación, resolución y registro de los incidentes de seguridad acontecidos.

- **Continuidad de los servicios**: Se establecerán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
- **Protección de datos personales**: Se adoptarán las medidas específicas que correspondan para minimizar los riesgos en el tratamiento de datos personales, cumpliendo la legislación de seguridad y privacidad vigente relacionada.
- **Cumplimiento legal**: Se asumirán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la legislación vigente en materia de seguridad de la información.

6. Alcance de la Política de Seguridad de la Información

Esta Política aplica a los sistemas TIC de la Universidad de Cádiz relacionados con el ejercicio de sus competencias, y a todos los usuarios con acceso autorizado a ellos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Universidad; todos ellos tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información (PSI) y su normativa de seguridad derivada.

7. Marco normativo de la Seguridad de la Información

El marco normativo de la Universidad de Cádiz en materia de Seguridad de la Información está constituido por las normas españolas y europeas relacionadas con la ciberseguridad y la protección de datos, siendo las más relevantes el RD 311/2022, de 3 de mayo, *por el que se regula el Esquema Nacional de Seguridad* (ENS), el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos, RGPD), la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD), la Ley 39/2015, de 1 de octubre, *del Procedimiento Administrativo Común de las Administraciones Públicas* y la Ley 40/2015, de 1 de octubre, *de Régimen Jurídico del Sector Público.*

También forman parte del marco normativo las normas universitarias específicas de la materia, así como las aplicables a la administración electrónica de la Universidad de Cádiz, derivadas de las anteriores y dentro del ámbito de aplicación de la presente política.

Se dispone de un listado de identificación de la legislación aplicable, de actualización permanente, con las referencias a dichas normas, en la página web de la sede electrónica: https://sedelectronica.uca.es

8. Marco de gobernanza de Seguridad de la Información

8.1. Roles y órganos de la Seguridad de la Información

La Universidad de Cádiz, teniendo en cuenta el principio de *diferenciación de responsabilidades*, según está establecido en el ENS, para organizar la seguridad de la información designará los siguientes roles:

- **Responsable de la Información**: Establece los requisitos de seguridad de la información tratada.
- **Responsable de los Servicios**: Determina los requisitos de seguridad de los servicios prestados.
- **Responsable del Sistema**: Por sí o a través de recursos propios o contratados se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de su operación diaria, pudiendo delegar en administradores u operadores bajo su responsabilidad.
- **Responsable de Seguridad**: Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos e informará sobre estas cuestiones.
  Este rol:

- corresponderá a un cargo o funcionario, de nivel ejecutivo, y no podrá ser un órgano de gobierno unipersonal de la universidad,
- no deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC, y
- no deberá estar bajo la dependencia jerárquica del Responsable del Sistema (y viceversa).

- **Delegado de Protección de Datos (DPD)**: Con las funciones que le atribuye el art. 39 del RGPD.

Además, se constituirá un **Comité de Seguridad de la Información**, como órgano colegiado, para la toma de decisiones estratégicas en materia de Seguridad de la Información. Este comité será presidido por una persona física, que asumirá la responsabilidad formal de las decisiones adoptadas.

El Comité de Seguridad de la Información estará constituido por:

- **Presidencia:** Rector o persona en quien delegue
- **Secretario del Comité**: Secretario General o persona en quien delegue
- **Vocales:**

- **Miembros permanentes:**
  - Responsable de la Información
  - Responsable de los Servicios
  - Responsable del Sistema
  - Responsable de Seguridad
  - Delegado de Protección de datos (DPD).
- **Miembros no permanentes:**
  Podrán ser convocados como asesores otros representantes de la información y los servicios de la universidad, o especialistas externos de los sectores público o privado, cuya presencia, por razón de su experiencia o vinculación con los asuntos tratados, sea necesaria o aconsejable.

El Secretario del Comité realizará las convocatorias y levantará actas de las reuniones del Comité.

El Delegado de Protección de Datos será convocado, con voz pero sin voto, solo a las reuniones sobre cuestiones relacionadas con los tratamientos de datos de carácter personal; si un asunto se sometiese a votación, siempre se hará constar su opinión en el acta de la reunión.

A las reuniones podrán asistir en calidad de asesores las personas que, en cada caso, considere oportuno el Presidente:

- Los representantes de la información y los servicios de la universidad (puestos de responsabilidad en distintas áreas o unidades) que sean convocados, participarán como vocales con un voto por área representada, sin perjuicio de que acudan varios representantes de ella.
- Los especialistas externos de los sectores público y privado que sean convocados participarán como vocales sin voto.

8.2 Responsabilidades de los roles y órganos de la Seguridad de la Información

Responsable de la Información y Responsable del Servicio
Determinar los requisitos y niveles de seguridad de la información y de los servicios, con el asesoramiento del Responsable de Seguridad y el Responsable del Sistema, para aprobación por el Comité de Seguridad de la Información.
Regular los derechos de acceso, autorizaciones y privilegios a la información y los servicios.

Aceptar los niveles de riesgo residual que afecten a la información y los servicios.
Cualquier cambio o nueva incorporación en la información o los servicios será comunicada al Responsable de Seguridad, quien informará al Comité de Seguridad de la Información.
Responsable del Sistema
Gestionar el sistema TIC durante todo su ciclo de vida, aprobar los cambios de configuración, elaborar los **Procedimientos de Seguridad** necesarios para su mantenimiento, y asegurar su implantación y actualización permanente.
Monitorizar el estado de seguridad del sistema TIC con herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica, asegurando el cumplimiento estricto de los controles de seguridad establecidos; detener el acceso a información o servicios si se evidencian deficiencias graves de seguridad.
Supervisar la gestión de acceso y privilegios de los usuarios del sistema TIC, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado por el Responsable de la Información y el Responsable del Servicio.
Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución; informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad del sistema.
Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los **Responsables de Sistema Delegados** que considere necesarios, quienes tendrán dependencia funcional directa de él, y serán responsables, en su ámbito, de todas aquellas acciones o funciones concretas delegadas.
Responsable de Seguridad
Verificar el nivel adecuado de seguridad de la información y de los servicios, en colaboración con el Responsable del Sistema, para la aprobación por el Comité de Seguridad de cambios o nuevos requisitos de seguridad.
Promover la formación y concienciación en ciberseguridad.
Elaborar la **Normativa de Seguridad**, que forma parte del marco normativo, y poner en conocimiento del Comité de Seguridad las modificaciones que se realicen.
Gestionar la elaboración e implantación de un **Plan de Adecuación al ENS** de los servicios TIC y un **Plan Director de Ciberseguridad** en la universidad.
Gestionar los procesos de auditorías y certificaciones en seguridad de los servicios.
Delegado de Protección de Datos
Recabar información de los tratamientos de datos personales realizados en la Universidad de Cádiz, y elaborar un registro actualizado; analizar y comprobar la conformidad legal de las actividades de tratamientos.
Analizar las actividades de tratamientos con base en los riesgos: asesorar sobre evaluaciones de impacto relativas a la protección de datos, metodología, salvaguardas a aplicar, etc.

Informar y asesorar a la Universidad de Cádiz y, en particular, a los usuarios que participan en las actividades de tratamientos de datos personales, de sus obligaciones según la normativa vigente de protección de datos, mediante acciones de formación y concienciación en la materia; asesorar en el principio de la protección de los datos personales desde el diseño y por defecto.
Supervisar el cumplimiento de lo dispuesto en las normativas de seguridad y en las políticas internas de la Universidad de Cádiz relacionadas con datos personales, incluida la asignación de responsabilidades y las auditorías correspondientes.
Cooperar con la *Agencia Española de Protección de Datos* y el *Consejo de Transparencia y Protección de Datos de Andalucía* cuando lo requieran, actuando como punto de contacto de la Universidad para cuestiones relacionadas con los tratamientos de datos personales.
Comité de Seguridad
Promover la obtención de la **Certificación de Conformidad con el ENS** de los servicios TIC de la universidad, prestando el apoyo y los recursos necesarios al desarrollo de un **Plan de Adecuación al ENS**. Conocer la normativa que regula la Certificación de Conformidad con el ENS, así como la relación de esquemas de certificación de la seguridad, las entidades de certificación acreditadas y las organizaciones públicas y privadas certificadas, con los que la Administración Pública tiene establecidos acuerdos de reconocimiento mutuo de certificados.
Encargar y valorar análisis de riesgos periódicos, reconociendo formalmente el riesgo residual: proponer directrices y recomendaciones en función de estas valoraciones, informando regularmente del estado de la seguridad al Consejo de Gobierno de la Universidad.
Aprobar el Plan de Adecuación al ENS, el Plan Director de Ciberseguridad y las Normativas y Procedimientos de Seguridad.
Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que sean consistentes y alineados con la estrategia institucional en la materia, resolviendo los conflictos de responsabilidad.
Difundir la Política de Seguridad de la Información (PSI), proponiendo las revisiones pertinentes y elevando su aprobación al Consejo de Gobierno de la Universidad.
Periodicidad de las reuniones y adopción de acuerdos: -Durante el desarrollo del Plan de Adecuación al ENS, para evaluar su seguimiento, las reuniones se procurarán una vez al trimestre. -Una vez alcanzada la Certificación de Conformidad con el ENS, el Comité se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones. En cualquier caso, las reuniones se convocarán por el presidente, a través del secretario, a su iniciativa o por mayoría de sus miembros permanentes. Las decisiones se adoptarán por consenso de los miembros permanentes.

8.3 Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la seguridad, se constituye la Oficina de Seguridad TIC, cuyas competencias estarán relacionadas con la adecuación al ENS, normativas de seguridad, análisis de riesgos y planes de mejora continua.

Composición de la Oficina:

- Director: será el Responsable de Seguridad, o la persona en quien delegue.
- Administradores especialistas de seguridad: los que el Director determine que sean necesarios.
- Secretario: a propuesta del Director, entre los miembros de la Oficina.

Las funciones de la Oficina de Seguridad TIC serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad, las siguientes:

- Elaboración y desarrollo del **Plan de adecuación al ENS**, enfocado a la obtención de la **Certificación de Conformidad con el ENS** de los servicios TIC de la universidad, incluyendo las tareas de encargo y gestión de las auditorías pertinentes.
- Trabajar con el Responsable del Sistema en la revisión de los planes de mejora de la seguridad, realizando **análisis de riesgos** regulares y el seguimiento de los riesgos residuales.
- Elaborar un **Plan Director de ciberseguridad** de la Universidad, incluyendo las valoraciones presupuestarias necesarias, para su debate en el Comité de Seguridad, y aprobación si procede.
- Elaborar la **Normativa de Seguridad** de la Información, que será aprobada por el Comité de seguridad.
- Diseñar acciones formativas y de concienciación en materia de ciberseguridad y protección de datos personales.
- Revisar regularmente la Política de Seguridad (PSI), adecuando su contenido a los cambios de contexto.

Periodicidad de las reuniones y adopción de acuerdos:

- El Director de la Oficina de Seguridad TIC convocará las reuniones de trabajo de sus miembros, y podrán organizarse grupos de trabajo para el análisis y realización de propuestas específicas.
- Se reunirá, al menos, una vez al mes y siempre antes de las reuniones del Comité de Seguridad.
- Las propuestas planteadas en la Oficina de Seguridad TIC serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad.

Análisis de riesgos:

Todos los sistemas afectados por la presente Política de Seguridad (PSI) estarán sujetos a un análisis continuo y actualizado de riesgos, con el objetivo de evaluar las amenazas a los que están expuestos y las salvaguardas necesarias para minimizarlos.

Este análisis se revisará al menos una vez al año, o puntualmente, cuando haya cambios significativos en la información o los servicios manejados, si ocurre un incidente grave de seguridad o se detectan vulnerabilidades graves.

El Director de la Oficina de Seguridad TIC, como Responsable de Seguridad, será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad, que aprobará la selección de medidas de seguridad a aplicar, si considera que son proporcionales a los riesgos y están justificadas, dinamizando la disponibilidad de recursos para atenderlas y asumiendo el riesgo residual.

Para realizar el análisis de riesgos, como norma general, se utilizará una metodología reconocida de análisis y gestión de riesgos.

8.4 Procedimiento de designación de responsables

La creación del Comité de Seguridad y las designaciones de los responsables identificados en esta Política serán formalizadas por el Rector de la Universidad, siendo sus nombramientos publicados en el Boletín Oficial de la UCA (BOUCA), así como las renovaciones sucesivas tras los cambios por vacantes o por nuevo equipo rectoral.

9. Gestión de incidentes

Para proteger a la información y los servicios de posibles incidentes de seguridad, la Universidad de Cádiz implementa las medidas establecidas por el Esquema Nacional de Seguridad para los sistemas de nivel de seguridad MEDIO, así como otros controles y refuerzos adicionales que se valoren como necesarios, a través de la evaluación de amenazas y riesgos.

Estas medidas y controles, así como los roles de seguridad y responsabilidades de todo el personal, están definidos en esta Política, y para garantizar su cumplimiento, la Universidad de Cádiz:

- autoriza los sistemas antes de entrar en operación, y evalúa regularmente su seguridad, incluyendo el análisis de los cambios de configuración, y
- solicita la revisión periódica del cumplimiento normativo en materia de seguridad por parte de terceros, con el fin de obtener una evaluación independiente (auditorías).

9.1 Prevención y detección de incidentes

La Universidad de Cádiz establece controles de operación en sus sistemas TIC, con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia, según lo dispuesto en el artículo 10 del ENS (*Vigilancia continua y reevaluación periódica*).

Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales, se activarán los mecanismos de evaluación inicial del incidente, desarrollando una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizando el impacto final sobre él (artículo 9 del ENS, *Existencia de líneas de defensa).*

9.2 Notificación de incidentes

De conformidad con lo dispuesto en el artículo 33 del ENS, la Universidad de Cádiz notificará al Equipo de Respuesta a Emergencias del Centro Criptológico Nacional (CCN-CERT) sobre los incidentes detectados que tengan un impacto significativo en la seguridad de la información y los servicios. Además, se realizará una notificación al CERT de referencia en la Comunidad Autonóma de Andalucía (Andalucía-CERT).

Si se han visto comprometidos datos personales, se comunicará el incidente a la Agencia Española de Protección de Datos (AEPD), al Consejo de Transparencia y Protección de Datos de Andalucía, y a los afectados, tal como indica el Reglamento General de Protección de Datos (RGPD).

Para las notificaciones, el Responsable de Seguridad o en quien delegue esta tarea, será el encargado de realizar las comunicaciones oportunas con el personal interno afectado y el externo, como proveedores, soporte técnico, equipos CERT y Fuerzas y Cuerpos de Seguridad del Estado.

9.3 Respuesta a incidentes y recuperación

En caso de incidente, se actuará rápida y eficazmente en la contención de daños y minimización de riesgos, adoptando decisiones en función de prioridades:

- Proteger la seguridad de las personas, como máxima prioridad.
- Proteger cualquier tipo de información con un determinado nivel de criticidad, especialmente valiosa para la Universidad.
- Proteger los equipos y sistemas de la organización, minimizando el tiempo que estos se encuentran detenidos.

Para garantizar la disponibilidad de los servicios críticos, la Universidad de Cádiz dispone de recursos que posibilitan su recuperación en caso de incidente de seguridad.

10. Tratamientos de datos personales

La Universidad de Cádiz solo recogerá y tratará datos de carácter personal cuando sean adecuados, pertinentes y no excesivos, y estén relacionados con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas técnicas y organizativas necesarias para el cumplimiento de la legislación de Protección de Datos Personales.

11. Desarrollo de la Política de Seguridad de la Información (PSI)

La presente Política de Seguridad (PSI) será complementada por normativas, procedimientos de seguridad e instrucciones técnicas de seguridad.

La estructuración de la documentación relativa a la Seguridad de la Información está organizada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel precedente:

a) **Primer nivel:** este documento de Política de Seguridad (PSI), de obligado cumplimiento, que complementa a la Política de Privacidad de la Universidad de Cádiz en materia de protección de datos personales.

b) **Segundo nivel:** normativas o políticas de seguridad específicas. Describen el uso correcto de equipos, servicios e instalaciones, lo que se considera 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.

c) **Tercer nivel**: procedimientos de seguridad e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad (PSI), determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al Consejo de Gobierno de la Universidad la aprobación de la Política de Seguridad (PSI) y las normativas de seguridad, siendo el Comité de Seguridad el responsable de la revisión anual, actualización y aprobación de los restantes documentos.

El Responsable de Seguridad es encargado, en su ámbito de actuación, de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos para que sea conocida y esté a disposición de todos los miembros de la universidad en la página web de la sede electrónica: https://sedelectronica.uca.es/

12. Obligaciones del personal de la Universidad de Cádiz y terceras partes

Todo el personal de la Universidad de Cádiz dentro del ámbito del ENS participará obligatoriamente en las actividades de los planes de formación y concienciación en ciberseguridad que se definan, en particular el personal de nueva incorporación.

Cualquier persona que tenga acceso a la información de la Universidad está sometida a la presente Política de Seguridad (PSI), siendo responsable de su cumplimiento. En caso de incumplimiento de los deberes previstos en ella, se le exigirá la responsabilidad de acuerdo con la normativa que le resulte de aplicación, pudiendo dar lugar al inicio de medidas disciplinarias.

Terceras partes

Cuando la Universidad de Cádiz preste o utilice servicios, maneje o ceda información a terceros, se les hará participes de esta Política de Seguridad (PSI) y de la normativa de seguridad relacionada, y se establecerán procedimientos de actuación y canales de comunicación ante incidentes de seguridad. Esta tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, y garantizará que está adecuadamente concienciada en materia de ciberseguridad.

Si algún aspecto de esta Política de Seguridad (PSI) no puede ser satisfecho, se requerirá un informe previo del Responsable de Seguridad, que precise los riesgos en que se incurre y la forma de tratarlos, para la aprobación por el Responsable de la Información y por el Responsable de los Servicios.

13. Disposición adicional

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

14. Disposición derogatoria única

Queda derogada la Política de Seguridad de la Información de la Universidad de Cádiz aprobada por 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*. y publicada en el BOUCA n.º 212 de 31 de junio de 2016.