UNIVERSIDAD D SEVILLA

Plan bienal de formación, concienciación y difusión para Protección de Datos y Seguridad de la Información en la Universidad de Sevilla

2025-2026

Índice

1. Introducción

La información corporativa que maneja la Universidad de Sevilla para el cumplimiento de su misión, incluidos los tratamientos de datos personales, tiene unos requisitos de seguridad que deben ser conocidos por todos los miembros de la comunidad universitaria.

La Universidad tiene cada vez mayor dependencia del uso de las tecnologías para la realización de las funciones que tiene asignadas. La evolución hacia modalidades de enseñanza online y de trabajo remoto exige de habilidades para el uso de herramientas de trabajo en equipo y de conocimientos específicos para la compartición de información en la nube. Sin la formación y la concienciación de seguridad adecuados, nuestro activo más valioso, la información corporativa, puede perder su confidencialidad, integridad o autenticidad, e incluso se puede producir la pérdida total de datos.

2. Justificación de la necesidad

Como administración pública, tenemos la obligación de cumplir con la normativa vigente sobre protección de datos y seguridad de la información. La formación en estas materias está incluida entre las medidas organizativas para el adecuado cumplimiento y protección de un derecho fundamental.

El Reglamento General de Protección de Datos, en su artículo 39, establece como una función del Delegado de Protección de Datos la concienciación y formación del personal que participa en las operaciones de tratamiento. El artículo 47 del RGPD establece que las normas corporativas vinculantes deben contemplar la supervisión de dicha formación.

De igual forma, el RD311/2022 que regula el Esquema Nacional de Seguridad establece que se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema en el que se trata la información alcance los niveles exigidos. De forma más concreta, establece que formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones:

a) Protección de la identidad de acceso a los servicios.

b) Protección del puesto de trabajo.

c) Gestión de la información en cualquier soporte en el que se encuentre, cubriendo, al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

La Política de Seguridad de la Información de la Universidad de Sevilla recoge la responsabilidad del Delegado de Protección de Datos y del Responsable de Seguridad de la Información de supervisar y promover la concienciación y formación del personal que participa en las operaciones de tratamiento y en la gestión de tecnologías y sistemas de información. Es una medida organizativa que pone de manifiesto la actitud proactiva de la institución.

Se recordará regularmente:

a) Las Políticas y sus normativas de desarrollo relativas a protección de datos personales y seguridad de la información corporativa.

b) Normativa del buen uso de los sistemas tecnológicos en los que se trata la información.

c) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

d) El procedimiento de notificación de violaciones y reporte de incidentes de seguridad, sean reales o falsas alarmas.

e) Buenas prácticas en materia de protección de datos y seguridad de la información en el trabajo diario.

Al margen del cumplimiento legal, en la Universidad nos encontramos ante tres factores que justifican la necesidad de impartir formación:

1. Por la naturaleza de nuestra institución, la disponibilidad y publicidad de la información son valores primordiales, lo que dificulta implantar medidas técnicas más propias de otros entornos restrictivos como el sector bancario o de salud.

2. Sin perjuicio de invertir en la puesta en marcha y mantenimiento de medidas técnicas de seguridad tecnológicas basadas en antivirus, cortafuegos o copias de seguridad que ayuden a minimizar posibles ciberataques y su impacto, la realidad de los últimos años es que las principales brechas de seguridad provienen de riesgos asociados a la naturaleza humana: son los fallos de las personas en relación con el uso del equipamiento informático, la información y los datos que manejan, sus contraseñas, los servicios corporativos y los soportes de información (Ref. MAGERIT v3.0, 5.3 [E] Errores y fallos no intencionados).

3. En materia de protección de datos es imprescindible la concienciación del uso diario que se realiza de datos personales de personas físicas, cuyos derechos y libertades hemos de proteger, realizando los tratamientos oportunos de forma adecuada y segura.

4. Objetivos del Plan

El Plan bienal de 2023-2024 impuso la obligatoriedad de realizar cursos de formación básica para todo el personal interno (PDI y PTGAS) durante ese período. El presente Plan de 2025-2026 pretende dar continuidad a esa formación básica utilizando campañas de concienciación dirigidas e impartiendo cursos específicos de seguridad y protección de datos personales para perfiles concretos, que sirvan de recordatorio al usuario. Una vez más el objetivo no es que el trabajador "cumpla" la normativa sino conseguir un cambio en su comportamiento que le permita intuir anomalías y actuar con precaución ante ellas. Los materiales formativos de este nuevo plan incidirán en la capacidad del ser humano para cuestionar y reflexionar sobre un hecho concreto de forma que pueda tomar la mejor decisión ante una situación anómala, evitando ser el eslabón débil de la seguridad.

Por ello, la visión del Plan 2025-2026 es**: "El espíritu crítico de los trabajadores de la Universidad protege nuestros activos más valiosos de los continuos ciberataques."**

Para conseguirlo se establecen los siguientes objetivos generales:

- Que el personal conozca los riesgos asociados al tratamiento de datos e información corporativa, especialmente en el uso las tecnologías.
- Que el personal conozca la normativa sobre protección de datos y su aplicación práctica (principios, tratamientos…) para conseguir el adecuado cumplimiento por parte de la US como responsable de los tratamientos.
- Que el personal adquiera las competencias que necesita en protección de datos y seguridad de la información en función de su puesto de trabajo.
- Que el usuario modifique su comportamiento ante anomalías que puedan suponer un riesgo para la seguridad de la información.

El plan, por tanto, está orientado a reducir los riesgos asociados a las amenazas de naturaleza humana mediante la adquisición de competencias de seguridad para las cuales se han usado marcos de referencia reconocidos internacionalmente. El plan tratará, además, de eliminar la idea equivocada de que la protección de datos y seguridad de la información suponen una carga de trabajo adicional a una ya sobrecargada agenda. La seguridad es beneficiosa, ayuda a proteger la privacidad de las personas, la información corporativa y a la propia institución. En materia de protección de datos estamos ante un derecho fundamental ya que estamos protegiendo a las

personas del riesgo y los perjuicios que les puede ocasionar un mal tratamiento de sus datos. Como beneficio adicional, lo aprendido para el entorno laboral es aplicable a la privacidad y seguridad en el entorno personal.

5. Desarrollo del Plan

El presente Plan bienal de formación, concienciación y difusión para Protección de Datos y Seguridad de la Información está dirigido a toda la Comunidad Universitaria con la intención de sensibilizar a sus miembros sobre los riesgos de la digitalización y sobre el beneficio de modificar su comportamiento mediante una formación continua, atractiva, dinámica, con mensajes claros y escenarios reales orientados a su perfil laboral y sus conocimientos, usando, en los casos necesarios, un lenguaje no técnico.

Incluye jornadas de sensibilización a directivos, campañas dirigidas de formación y concienciación básica para todos los miembros de la Comunidad Universitaria, acciones formativas concretas para determinados colectivos específicos y una campaña de difusión para dar a conocer los eventos puntuales más significativos que se producen en torno al proceso de Protección de Datos y Seguridad de la Información en la Universidad.

Cada acción o campaña incluirá los destinatarios, objetivos concretos, acciones específicas, metodología y contenidos.

5.1. Sensibilización de directivos

Destinatarios: personas con responsabilidad en el Gobierno de la Universidad.

Objetivos concretos:

- Que tomen conciencia de los riesgos inherentes al tratamiento de datos personales e información corporativa, así como del proceso de digitalización
- Que tomen conciencia del grado de implicación que tienen en el proceso de gestión de la protección de datos y la seguridad de la información en función del puesto que ocupan.
- Que conozcan las consecuencias económicas y de reputación de una perdida de datos o una cibercrisis.

- Que conozcan las decisiones estratégicas a tomar en tiempo real si se produce una crisis, con el objetivo de contener y mitigar de la mejor manera el impacto del ataque.
- Que aprendan a gestionar la comunicación oficial, que debe incluir cuándo, cómo y con qué información hay que dirigirse tanto a los empleados como al público general en una situación de crisis.
- Que adquieran las competencias básicas necesarias para la protección de la información corporativa y las tecnologías que la tratan.

Acciones específicas:

1) Presentación al Equipo de Gobierno de los procesos de Gestión de Datos Personales y de Gestión la Seguridad de la Información en la Universidad de Sevilla.
2) Presentación del proceso de Gestión de Cibercrisis de la Universidad de Sevilla a las personas del Equipo de Gobierno con responsabilidad en el mismo.
3) Campañas dirigidas de formación y concienciación básica en protección de datos y ciberseguridad a los responsables de Centros, Departamentos y Servicios.

Metodología:

- Seminario dirigido al Equipo de Gobierno sobre la importancia del cumplimiento normativo en materia de protección de datos, cómo se está desarrollando, y cómo impulsarlo desde el gobierno de la US.
- Seminarios presenciales para el Equipo de Gobierno y para los responsables de la Gestión de una Cibercrisis sobre cómo abordar una situación de crisis provocada por un incidente de seguridad de la información.
- Lanzamiento de campañas de formación y concienciación dirigidas, bien por encuestas o simulacros de ataque, que llevan asociados materiales formativos y/o cursos online.

Contenidos:

- Se impartirá un seminario dedicado a presentar al Equipo de Gobierno las actuaciones realizadas en materia de protección de datos que sirva también de seminario de concienciación.
- Se impartirá un seminario al Equipo de Gobierno y otro a los implicados en el proceso de Gestión de una Cibercrisis de una duración a determinar en función de los contenidos, no superior a una hora y que se agendará de acuerdo a la disponibilidad de los mismos a lo largo de la duración del presente Plan de formación, concienciación y difusión sobre Protección de Datos y Seguridad de la Información. Los contenidos se determinarán de común acuerdo entre la empresa externa especializada que imparta la formación y los responsables de la Protección de Datos y la Gestión de la Seguridad de la información en

la Universidad, priorizando en la necesidad de una estrategia de seguridad alineada con el negocio, el cumplimiento legal, la estructura organizativa, la valoración de activos esenciales y la gestión de los riesgos.

- Los contenidos de los cursos dirigidos a responsables de Centros, Departamentos y Servicios cubrirán las competencias básicas necesarias para la protección de la información corporativa y las tecnologías que la tratan.

5.2. Campañas de formación y concienciación básica

Destinatarios: todos los miembros de la Comunidad Universitaria.

Objetivos concretos:

- Que la Comunidad Universitaria sea consciente de los riegos y las repercusiones del uso de la tecnología.
- Que tenga unas nociones básicas acerca de la Gestión de Datos Personales y el Proceso de Gestión de la Seguridad de la Información
- Que adquiera las competencias básicas necesarias para la protección de la información corporativa que manejan y las tecnologías con las que trabajan.
- Que adopte los comportamientos más adecuados para evitar el compromiso de los datos o la información corporativa.

Acciones específicas:

1) Campañas de formación dirigidas por simulacros de ataque o por encuesta inicial a través de correo electrónico a distintos colectivos del PDI y PTGAS. Se utilizarán ataques conocidos y actuales, de tipo robo de credenciales, robo de información, fraude, adjunto malicioso, URLs falsas, etc. basados en temas actuales. Si el usuario resulta engañado, se le proporcionará de forma automática información sobre el supuesto ataque y del peligro de determinadas acciones, redireccionando al portal de formación para la revisión de píldoras formativas relacionadas con el tipo de ataque concreto o realización de algún curso básico de seguridad. Pasado un tiempo después de la formación, se repetirá el ataque dirigido para comprobar la mejora en la madurez de la concienciación en seguridad.

2) Cursos online voluntarios para empleados (PDI/PTGAS) en el que se transmitirá información útil sobre protección de datos personales y seguridad de la información:

   - Cursos básicos sobre protección de datos personales
   - Talleres sobre protección de datos para tratamientos específicos
   - Cursos de formación básica en seguridad informática

- Cursos sobre el uso seguro de las tecnologías

Metodología:

- Las campañas dirigidas que se lanzarán desde la propia Universidad de Sevilla utilizando la "Plataforma de Campañas de concienciación en Seguridad de la Información", desarrollada en el proyecto de cooperación CONSEG en el que han participado 16 universidades públicas españolas. Este proyecto está amparado por el Real Decreto 641/2021, de 27 de julio, por el que se regula la concesión directa de subvenciones a universidades públicas españolas para la modernización y digitalización del sistema universitario español en el marco del Plan de Recuperación, Transformación y Resiliencia. Es un entorno de aprendizaje digital para adquisición de competencias de ciberseguridad en el uso de las tecnologías digitales y la protección de la información por parte de los miembros de la comunidad universitaria que incluye materiales formativos originales, elaborados ad hoc para el entorno universitario en base a las competencias de seguridad necesarias.
- Los cursos online se ofrecerán a través de la plataforma de Enseñanza Virtual: consistirán en una explicación teórico-práctica y test final de autoevaluación. El material de apoyo consistirá en un manual con la materia teórica del curso y otros documentos informativos.
- La evaluación de los cursos se llevará a cabo por parte del Centro de Formación del PAS (para PTGAS) y del Instituto de Ciencias de la Educación (para PDI) en los términos que corresponda.

Contenidos:

Los contenidos contemplados en cada formación están organizados en torno a bloques temáticos:

- Conocimiento de las Políticas y Normativas de Protección de Datos y Seguridad de la Información de la Universidad de Sevilla.
- Protección de la Información Corporativa, incluyendo Datos Personales.
- Detección y comunicación de fraudes e incidentes de seguridad
- Uso correcto del Usuario Virtual (UVUS) y el doble factor: protección de la contraseña
- Gestión de privilegios de acceso a la información y los equipos informáticos
- Protección del puesto de trabajo: espacio físico y equipamiento informático
- Uso de dispositivos móviles
- Perfiles corporativos y personales en Redes Sociales

5.3. Formación para colectivos específicos

A fin de establecer el programa anual de cursos de formación para colectivos específicos, se recabará información de los destinatarios para concretar las acciones formativas necesarias para realizar la programación anual.

5.3.1. Personal TI

Destinatarios: Personal TI con participación directa en alguna de las tareas del proceso de Protección de Datos y Seguridad de la Información.

- Responsables de la Información y de los Servicios.
- Responsables de Seguridad y Administradores de la Seguridad del Sistema.
- Responsables de las Infraestructuras de Tecnología de la Información.
- Responsable de Aplicaciones Informáticas.
- Auditores internos de seguridad.
- Miembros de la Comisión de Seguridad de la Información.
- Personas designadas por alguno de los anteriores para la realización de alguna tarea relacionada con la seguridad que les haya sido delegada.

Objetivos concretos: que el personal TI conozca los riesgos de la tecnología, adquiera los conocimientos para realizar sus tareas específicas y esté preparado para adecuarse a los requisitos de seguridad, cada más exigentes, de las tecnologías emergentes.

Acciones específicas:

1) Formación sobre tratamientos de datos personales.
2) Formación sobre el nuevo RD 311/2022 del Esquema Nacional de Seguridad.
3) Formación sobre el Plan de Gestión de Cibercrisis con simulación de ataque informático con afectación de servicios críticos.
4) Itinerarios curriculares personalizados para distintos perfiles TI basados en los Planes de Formación del Portal de Gobernanza de la Ciberseguridad Nacional que el Centro Criptológico Nacional pone a disposición de la Universidad de Sevilla.

Metodología:

- Los cursos podrán realizarse de manera presencial o virtual a partir de una explicación teórico-práctica y la realización de dinámicas de grupo para la resolución de casos y supuestos prácticos.

- El material de apoyo consistirá en un documento con la materia teórica del curso.
- Para la realización de los Itinerarios Curriculares utilizaremos la plataforma ANGELES del CCN-Cert.

Contenidos:

Los contenidos contemplados en este módulo de formación específica estarán relacionados con los siguientes temas:

- Marco regulatorio: RGPD, LOPDyGDD, ENS, Políticas de protección de Datos y de Seguridad de la US y normativas de desarrollo.
- Aplicación práctica del proceso de seguridad: Gestión de Datos Personales, Gestión de la Seguridad de la Información y Seguridad operativa y tecnológica

Evaluación y revisión:

- La evaluación del curso se llevará a cabo por parte del Centro de Formación del PAS (para PTGAS) en los términos que corresponda.

5.3.2. Responsables tratamientos de datos personales

Destinatarios: Responsables delegados y tecnológicos de protección de datos, y gestores de datos personales en la plataforma de cumplimiento “lopdyens.us.es”.

Objetivos concretos: que el personal de la universidad implicado directamente en la gestión de datos personales adquiera los conocimientos para realizar sus tareas específicas y esté preparado para el cumplimiento de la legislación vigente (RGDP/LOPDYGDD/ENS).

Acciones específicas:

1) Formación sobre tratamientos de datos personales.
2) Formación sobre las medidas de seguridad del ENS.
3) Formación sobre el uso de la plataforma lopdyens.us.es.

Metodología:

- Los cursos podrán realizarse de manera presencial o virtual a partir de una explicación teórico-práctica y la realización de dinámicas de grupo para la resolución de casos y supuestos prácticos.
- El material de apoyo consistirá en un documento con la materia teórica del curso.

Contenidos:

Los contenidos contemplados en este módulo de formación específica estarán relacionados con los siguientes temas:

- Marco regulatorio: RGPD, LOPDyGDD, ENS, Políticas de protección de Datos y de Seguridad de la US y normativas de desarrollo, y Normativa sectorial de cada tratamiento.
- Aplicación práctica del proceso de gestión de datos personales: Gestión de Datos Personales, Gestión de la Seguridad de la Información y uso de la plataforma de seguimiento de gestión de los tratamientos de datos personales "lopdyens.us.es".

Evaluación y revisión:

- La evaluación del curso se llevará a cabo por parte del Centro de Formación del PTGAS (para PAS) en los términos que corresponda.

5.3.3. Otros colectivos: financiero, personal investigador, etc.

Si la universidad tiene interés en impartir formación específica sobre ciberseguridad y protección de datos personales a colectivos concretos podrá solicitarlos a través del FORPAS/ICE. La Delegada de Protección de Datos y el Responsable de Seguridad de la Información podrán dar soporte a la elaboración del índice de contenidos de los cursos para garantizar que cubren las necesidades del colectivo específico.

5.4. Campaña de difusión

Destinatarios: a todos los miembros de la Comunidad Universitaria.

Objetivos concretos: que toda la Comunidad Universitaria esté informada acerca de los eventos puntuales más significativos que se producen en torno al proceso de Seguridad de la Información en la Universidad.

Acciones específicas:

1) Coincidiendo con el comienzo del Plan bienal de formación, concienciación y difusión para Protección de Datos y Seguridad de la Información en la Universidad de Sevilla se enviara un comunicado a Directores/Decanos de Centros y a Responsables de Unidades Administrativas en el que se les informará de las acciones del Plan y se hará hincapié en la necesidad de promover desde el Centro o la Unidad la participación del Personal Docente e Investigador, el Personal de Administración y Servicios y los Estudiantes del Centro en dichas acciones.

2) Distribución de materiales informativos de concienciación: se articula esta acción concreta utilizando materiales de sensibilización facilitados por el Instituto Nacional de Ciberseguridad (INCIBE) que ha sido adecuados a Universidades por la CRUE-Digitalización, así como materiales formativos originales elaborados ad hoc para el entorno universitario en base a las competencias de seguridad necesarias dentro del proyecto CONSEG. Entre otros materiales, se distribuirán:

   a. Trípticos informativos e infografías para distribuir entre el personal y estudiantes a través de las Conserjerías, Bibliotecas, eventos como el Ferisport, etc.

   b. Carrusel de imágenes y vídeos en las pantallas de Centros con consejos de ciberseguridad.

3) Soporte a la difusión de eventos mediante su publicación a través del Portal de la Universidad, de la página web de la Oficina de Seguridad de la información, de la TVUS, de las pantallas de Centros y/o de los perfiles corporativos en Redes Sociales, en colaboración con la Dirección de Comunicación de la Universidad. Son, entre otros, los siguientes eventos:

   - Consejos de seguridad sobre el uso de la Identidad Digital Corporativa y las Tecnologías de la información.
   - Actualización de políticas, normativas, procedimientos y guías de buenas prácticas.
   - Apertura de convocatorias de formación.
   - Procedimientos para comunicación de incidentes o violaciones de datos.
   - Publicación de acuerdos y decisiones de la Comisión de Seguridad de la Información de interés para la Comunidad Universitaria.
   - Notificación de resultados de auditorías de interés para la Comunidad Universitaria.
   - Notificación de resultados del Plan bienal de formación, concienciación y difusión.
   - Información sobre vulnerabilidades que puedan afectar a nuestros usuarios.

Apéndice: Lenguaje de género

Este documento ha sido redactado con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.