UNIVERSIDAD Ð SEVILLA

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

2023-2024

Índice

1. Introducción

La información corporativa que maneja la Universidad de Sevilla para el cumplimiento de su misión, incluidos los tratamientos de datos personales, tienen 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 teletrabajo, acelerada por la pandemia COVID-19, 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 de los equipos informáticos en el 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 dos problemas:

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. Objetivos del Plan

El presente Plan no trata de que el usuario "cumpla" la normativa sino de conseguir un cambio en su comportamiento que le permita intuir anomalías y actuar con precaución ante ellas.

Para ello 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 y a conseguir competencias de seguridad, para las cuales se han usado marcos de referencia reconocidos internacionalmente. 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 su ya sobrecargada agenda. La seguridad es beneficiosa, ayuda a proteger la privacidad de las personas, la información corporativa y a la propia institución. Lo aprendido para el entorno laboral podemos aplicarlo a la privacidad y seguridad en el entorno personal. 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.

La visión del Plan es**: "Nuestros trabajadores son el eslabón fuerte de la cadena. Son nuestra arma más valiosa para luchar contra ciberataques."**

4. Desarrollo del Plan

El presente Plan de Formación y Difusión de la 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 un lenguaje no técnico.

Incluye jornadas de sensibilización a directivos, una campaña dirigida de 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.

4.1. 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.

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) Curso básico online sobre la organización, políticas y normativas relacionadas con Protección de Datos, Seguridad de la Información de la Universidad de Sevilla y buenas prácticas en el puesto de trabajo a los responsables de Centros, Departamentos y Servicios.

Metodología:

- Seminarios presenciales con encuestas de madurez.
- Cursos online con test final de aprovechamiento.

Contenidos:

- 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 del curso online dirigido a responsables de Centros, Departamentos y Servicios versarán sobre Seguridad de la Información y buenas prácticas en el puesto de trabajo.

4.2. Campaña de formación básica

Destinatarios: a 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 adopte los comportamientos más adecuados para evitar el compromiso de los datos o la información corporativa.

Acciones específicas:

1) Campañas de concienciación automáticas (*), dirigidas por simulacros de ataque o por encuesta inicial a través de correo electrónico a distintos colectivos del PDI y PAS. 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 concienciación para la revisión de píldoras formativas relacionadas con el tipo de ataque concreto. Pasado un tiempo después de la formación, se repetirá el ataque dirigido para comprobar la mejora en la madurez de la concienciación en seguridad.

   (*) Las campañas de concienciación automáticas están supeditadas al desarrollo de la plataforma de campañas automáticas dentro del proyecto UniDigital o la integración en el actual proyecto de campañas dirigidas de RedIris. El resto de la campaña de concienciación básica se realizará según su planificación.

2) Distribución de materiales informativos de concienciación:

   a. Posters impresos para colocar en los distintos Centros y Unidades Administrativas de la Universidad, en zonas de estudio, ascensores, hall, cafeterías, etc.

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

   c. Carrusel de imágenes en las pantallas de Centros con consejos de ciberseguridad.

   Se articula esta acción concreta utilizando materiales de sensibilización facilitados por el Instituto Nacional de Ciberseguridad (INCIBE) y adecuados a Universidades por la CRUE-TIC, organizados en torno a estos bloques temáticos:

   - Información, incluyendo Datos Personales
   - Fraudes
   - Contraseñas
   - Puesto de trabajo
   - Dispositivos móviles
   - Redes Sociales

3) Proceso formativo obligatorio para empleados (PDI/PAS) en el que se transmitirá información útil sobre seguridad de la información y consejos o buenas prácticas a la hora de manejar la información de la organización:

   a. CURSO BÁSICO DE PROTECCIÓN DE DATOS

b. TALLERES SOBRE PROTECCIÓN DE DATOS PARA TRATAMIENTOS ESPECÍFICOS

c. FORMACIÓN BÁSICA EN SEGURIDAD INFORMÁTICA Y BUENAS PRACTICAS EN EL PUESTO DE TRABAJO

Metodología:

- Cursos *online* que 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 PAS) y del Instituto de Ciencias de la Educación (para PDI) en los términos que corresponda.
- Contarán con varias ediciones facilitando así al personal la elección de la convocatoria que mejor se adapte a su calendario.
- Debido al carácter obligatorio de esta formación online básica, se preinscribirá en alguna de las ediciones programadas para los años 2023 y 2024 a todo el personal de la US que no haya realizado aún alguna formación básica sobre seguridad, informando a los Directores de Departamento y Jefes de Servicio correspondientes para contar con su colaboración en la concienciación acerca de la importancia de la realización de este curso.

Contenidos:

Los contenidos contemplados en cada formación serán los siguientes:

- CURSO BÁSICO DE PROTECCIÓN DE DATOS

  Unidad 1: Introducción. Protección de Datos como Derecho Fundamental. Principios de la Protección de datos.

  Unidad 2: Derechos en la Protección de Datos.

  Unidad 3: Actores en la protección de datos. Registro de Actividades de tratamiento. Seguridad.

  Unidad 4: Delegado de Protección de Datos. Autoridades de Protección de Datos. Régimen Sancionador.

- SEGURIDAD DE LA INFORMACIÓN Y BUENAS PRÁCTICAS EN EL PUESTO DE TRABAJO

Introducción. Conceptos básicos sobre Seguridad de la Información en la Universidad de Sevilla.

Módulo I: Aprender a valorar la Información con la que trabajamos.

Módulo II: Riesgos del correo electrónico.

Módulo III: Garantizar la seguridad del usuario y la contraseña.

Módulo IV: Proteger correctamente nuestro puesto de trabajo.

Módulo V: Recomendaciones para el uso de dispositivos móviles.

Módulo VI: Medidas de seguridad para proteger perfiles en Redes Sociales

4.3. 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.

4.3.1. 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 el nuevo RD 311/2022 del Esquema Nacional de Seguridad.
2) Formación sobre tratamientos de datos personales.
3) Formación sobre el Plan de Gestión de Cibercrisis con simulación de ataque informático con afectación de servicios críticos.
4) Itinerarios curriculares personalizados basados en los cursos de formación de la plataforma ANGELES del CCN-Cert.

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
    - Reglamento General de Protección de Datos, Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales y normativa de desarrollo.
    - Esquema Nacional de Seguridad y normativa de desarrollo
    - Política de Protección de Datos de la US.
    - Política de Seguridad de la US y Normas vigentes de Uso de los Servicios TI.
- Aplicación práctica del proceso de seguridad
    - Gestión de Datos Personales
        - Organización: roles, funciones y responsabilidades del proceso
        - Privacy Impact Analysis
        - Medidas de cumplimiento

- Gestión y notificación de violaciones
- Procedimiento de auditoría interna de tratamientos

- Gestión de la Seguridad de la Información
  - Organización de la Seguridad: roles, funciones y responsabilidades del proceso
  - Análisis y gestión de riesgos
  - Procedimiento de gestión de incidentes de seguridad
  - Procedimiento de auditoría interna del ENS
  - Sistemática de Mejora Continua
- Seguridad operativa y tecnológica
  - Arquitectura de Seguridad
  - Procesos de Gestión del Servicio
  - Seguridad de las infraestructuras
  - Desarrollo seguro de aplicaciones
  - Trazabilidad y monitorización
  - Plan de Continuidad
  - Implantación de las medidas de protección del ENS.

Evaluación y revisión:

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

4.3.2. 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 el uso de la plataforma lopdyend.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
    - Reglamento General de Protección de Datos, Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales y normativa de desarrollo.
    - Esquema Nacional de Seguridad y normativa de desarrollo.
    - Política de Protección de Datos de la US.
    - Política de Seguridad de la US.
    - Normativa sectorial de cada tratamiento.
- Aplicación práctica del proceso de gestión de datos personales
    - Gestión de Datos Personales
        - Organización: roles, funciones y responsabilidades del proceso
        - Registro de los tratamientos
        - Privacy Impact Analysis
        - Medidas de cumplimiento
        - Ejercicio de derechos
        - Gestión y notificación de violaciones
        - Procedimiento de auditoría interna de tratamientos
    - Gestión de la Seguridad de la Información
        - Análisis y gestión de riesgos de la tecnología en la que se tratan los datos personales
        - Procedimiento de gestión de incidentes de seguridad que comprometan datos personales

- Procedimiento de auditoría interna del cumplimiento de medidas de seguridad de los tratamientos
- Sistemática de Mejora Continua

- 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 PAS (para PAS) en los términos que corresponda.

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

Si la universidad tiene interés en impartir formación específica sobre ciberseguridad 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.

4.4. 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 de Formación y Difusión de la Seguridad se envía un comunicado a Directores/Decanos de Centros y a Responsables de Unidades Administrativas en el que se les informa de las acciones del Plan de concienciación en Seguridad de la Información y se hace 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. Se acompañará el comunicado con una muestra de los materiales impresos en la Campaña de Concienciación Básica.

2) Impartición de 10 charlas anuales de concienciación presenciales sobre Protección de Datos y Seguridad de la Información para PAS en los distintos Campus de la Universidad de unas dos horas y media con un aforo no superior a 100 asistentes en las que se cuenta a los presentes los aspectos más relevantes de la seguridad en la Universidad en base a los riesgos

de las TI y las competencias de seguridad del personal. Se fomenta la participación de los asistentes a través de una aplicación de encuestas.

3) Soporte a la difusión de eventos mediante su publicación a través del sitio web de seguridad, y de los perfiles corporativos en Redes Sociales en colaboración con el Departamento de Comunicación de la Universidad. Son, al menos, los siguientes eventos:

   - Actualización de políticas, normativas, procedimientos y guías de buenas prácticas.
   - Apertura de convocatorias de formación.
   - 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 de Concienciación bienal.
   - Información sobre vulnerabilidades que puedan afectar a nuestros usuarios.
   - Consejos de seguridad y procedimientos para comunicación de incidentes o violaciones de datos.

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.