CEADE
SAN ISIDORO
CENTRO UNIVERSITARIO

MEDIDAS ORGANIZATIVAS Y DE SEGURIDAD

De conformidad con: Reglamento (UE) 2016/679 (RGPD)
y Ley Orgánica 3/2018 (LOPDGDD)

1. Introducción y objeto

El presente documento establece las Medidas Organizativas y de Seguridad obligatorias en el Centro Universitario San Isidoro para dar estricto cumplimiento al Artículo 32 del Reglamento General de Protección de Datos (RGPD) y a la Ley Orgánica 3/2018 (LOPDGDD), relativos a la seguridad del tratamiento de datos de carácter personal.

Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, el Centro ha adoptado un enfoque proactivo para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de sus sistemas. El objeto principal de esta política es estructurar un Sistema Unificado de Autorizaciones y Permisos de Acceso Restringido adecuado a. Con esto se erradican los silos de datos dispersos e informales, asegurando bajo los principios de "mínimo privilegio" y "necesidad de conocer" que únicamente las personas estrictamente implicadas y legitimadas puedan acceder a los ficheros correspondientes.

2. Ámbito de aplicación y colectivos

Esta normativa es de obligado cumplimiento para todo el personal que preste servicios en el Centro Universitario San Isidoro, clasificado en los siguientes estamentos organizativos según la Cadena de Valor institucional:

- PDI (Profesorado Docente e Investigador). Miembros del claustro académico, directores, subdirectores, coordinadores y responsables de asignaturas.
- PTGAS (Personal Técnico de Gestión y Administración de Servicios). Personal integrado en las áreas de Gerencia, Administración, Secretaría General, Admisiones, Recursos Humanos, Comunicación y relaciones externas, Deportes, Voluntariado, Igualdad y diversidad funcional, Calidad, Biblioteca e Informática.
- Alumnado. Estudiantes matriculados en grados, dobles grados y másteres oficiales impartidos por el centro, incluyendo participantes de programas de movilidad nacional o internacional.
- Terceros. Proveedores externos de servicios informáticos, soporte técnico, ciberseguridad, asesoría contable o mutuas (vincular de forma obligatoria mediante contratos bajo el Art. 28 del RGPD).

3. Clasificación de ficheros

A efectos de control de acceso, el Centro Universitario San Isidoro segmenta sus repositorios en nueve grandes categorías de ficheros de datos personales incluidas en el RAT, cada una con sus correspondientes sistemas de permisos atendiendo a la finalidad de los datos contenidos en los ficheros.

4. Medidas técnicas de seguridad e infraestructura

Para materializar el sistema de acceso restringido y cumplir con las garantías de seguridad que se aplican de forma obligatoria las siguientes salvaguardas técnicas:

4.1. Configuración del entorno cloud (Google Workspace)

- Drive corporativo y unidades compartidas. Toda la documentación administrativa, académica y de investigación del Centro debe alojarse en las unidades cloud como Drive y Unidades Compartidas, controladas jerárquicamente por la organización en base a permisos.
- Prohibición de compartición externa genérica. Todo documento compartido externamente requiere autorización expresa de la Dirección y la inclusión del correo individualizado del destinatario.
- Trazabilidad y auditoría de acceso. El Administrador de Sistemas revisará periódicamente los accesos anómalos, los intentos de inicio de sesión fallidos o las descargas masivas de ficheros sensibles.

4.2. Entorno intranet

- Servidores internos. El centro dispone de estructura cliente-servidor, en la cual cada usuario inicia sesión en los equipos de las instalaciones con su usuario y clave. La infraestructura está basada en Active Directory de Windows Server. Se dispone de dos dominios a nivel de autenticación de Red, separando la actividad prestada por dirección del centro, secretaría y despachos en el dominio: OFICINA y la actividad en las aulas en el dominio: AULAS. Contienen documentación administrativa, académica y de investigación del Centro.
- Seguridad perimetral, cifrado y control de red:
    - Segmentación de red mediante cortafuegos Fortinet. Implementación y actualización continua de firewalls Fortinet de última generación como sistema de seguridad perimetral. Se segmenta físicamente la red del edificio, aislando por completo el tráfico de la red pública para alumnos de las redes privadas destinadas a administración (PTGAS) y profesorado (PDI).
    - Doble factor de autenticación (MFA / 2FA). La verificación en dos pasos para todo el personal técnico de gestión (PTGAS) y profesorado (PDI) en sus cuentas corporativas y plataformas de gestión del Centro.
    - Gestión de identidades y accesos (IAM). Sincronización robusta para la asignación dinámica de permisos según el estado laboral/académico del usuario, automatizando los procesos de alta, modificación y baja de accesos.

4.3. Servidores externos

- Data Center (Valencia). Datos gestionados bajo un acuerdo de nivel de servicio (SLA) que garantiza alta disponibilidad física y lógica. La confidencialidad e integridad están aseguradas por sistemas de prevención de intrusiones (IPS/IDS) y firewalls administrados por el agente externo, junto con el control de acceso físico al centro. La resiliencia se garantiza con redundancia de sistemas críticos (energía, refrigeración) y monitorización de seguridad diaria. Se destina al almacenamiento de la web y backups.

5. Medidas organizativas y protocolos

La seguridad técnica es ineficaz sin una cultura institucional alineada. Por ello, se despliegan las siguientes medidas organizativas.

5.1. Formación en ciberseguridad

Todo el personal (PDI y PTGAS) recibirá formación específica obligatoria en materia de protección de dato y ciberseguridad.

5.2. Compromiso de confidencialidad

El quebrantamiento del sistema de permisos o la cesión de credenciales propias a terceros dará lugar a las sanciones disciplinarias correspondientes bajo la legislación laboral española, sin perjuicio de las responsabilidades civiles o penales derivadas.

5.3. Protocolo de incidentes de seguridad y gestión de crisis

Ante cualquier sospecha de brecha de seguridad (pérdida de credenciales, acceso no autorizado, malware o extravío de un dispositivo corporativo), el afectado debe notificar de forma inmediata (en un plazo máximo de 24 horas desde su detección) a la Gerencia y al DPD. En caso de confirmarse una quiebra de seguridad que afecte a datos personales, el Centro ejecutará el protocolo formal para la notificación a la Agencia Española de Protección de Datos (AEPD) en el plazo máximo de 72 horas regulado por el artículo 33 del RGPD.

5.4. Auditorías y revisiones periódicas

El centro establecerá un calendario de revisiones y auditorías preventivas para acompañar la evolución natural de la tecnología. Estas acciones evaluarán el estado de la infraestructura mediante los siguientes controles periódicos:

- Inventario técnico. Mantener actualizado de forma constante el registro de activos informáticos.
- Control de obsolescencia. Supervisar los sistemas próximos al fin de su soporte oficial.
- Plan de renovación: programar la sustitución progresiva del hardware no compatible con nuevas versiones.
- Revisión de almacenamiento. Verificar periódicamente el uso, riesgos y actualizaciones del sistema NAS.
- Reactivación de monitorización. Implementar herramientas activas para detectar fallos previos en dispositivos poco visibles.
- Seguridad perimetral y control de cortafuegos. Revisar recurrentemente las reglas de filtrado por el equipo informático.
- Aislamiento de redes. Confirmar la separación estricta entre la red de alumnado y la administrativa.

6. Solicitud y revocación de permisos

- Alta de permisos. Al incorporarse un nuevo miembro al PTGAS o PDI, Recursos Humanos notificará al Área de Informática y Campus Virtual el rol asignado. Los accesos se concederán de forma manual y estrictamente vinculados al perfil del puesto.

- Peticiones extraordinarias. Si un docente o gestor requiere acceso temporal a un fichero ajeno a su perfil (por ejemplo, para una investigación académica coordinada), deberá formalizar una solicitud por escrito argumentando la legitimación.
- Revocación inmediata (bajas) para PDI y PTGAS. En el momento en que cese la relación laboral de un empleado se procederá a la suspensión y desactivación inmediata de la cuenta corporativa y la revocación total de accesos en cascada en un plazo máximo de 24 horas.
- Revocación inmediata (bajas) para alumnado. En el momento en que se extinga la matrícula del alumno, en los 10 días naturales siguientes a dicha fecha, se cancelará su cuenta de usuario Google corporativa y se revocarán todos los permisos de acceso al campus virtual e intranet del centro.