INTRODUCCIÓN

La presente memoria recoge las principales actuaciones realizadas por el Área de Tecnologías de la Información y las Comunicaciones (TIC) de la Universidad Pablo de Olavide durante el periodo comprendido entre el 1 de julio de 2024 y el 30 de junio de 2025.

El documento responde a la solicitud anual de la Secretaría General y tiene como objetivo principal ofrecer una visión global y estructurada de las actividades desarrolladas por el Área, permitiendo valorar los avances alcanzados en el despliegue, mantenimiento y mejora de los sistemas de información y tecnología que dan soporte a la actividad universitaria.

La memoria se ha elaborado a partir de las contribuciones de los distintos servicios del Centro de Informática y Comunicaciones, agrupadas en bloques funcionales: Gestión Administrativa, Formación y Desarrollo del Personal, Redes y Equipamiento, Aplicaciones y Sistemas, y Seguridad de la Información.

Cada apartado detalla los hitos alcanzados, los proyectos desarrollados, las mejoras introducidas y los indicadores que permiten valorar de forma objetiva el grado de ejecución y el impacto institucional de las iniciativas acometidas.

El trabajo reflejado en este documento pone de manifiesto el compromiso del Área TIC con la calidad del servicio, la transformación digital de la Universidad, la seguridad de la información y la mejora continua, en coordinación con los distintos órganos universitarios y con una clara orientación a las necesidades de la comunidad universitaria.

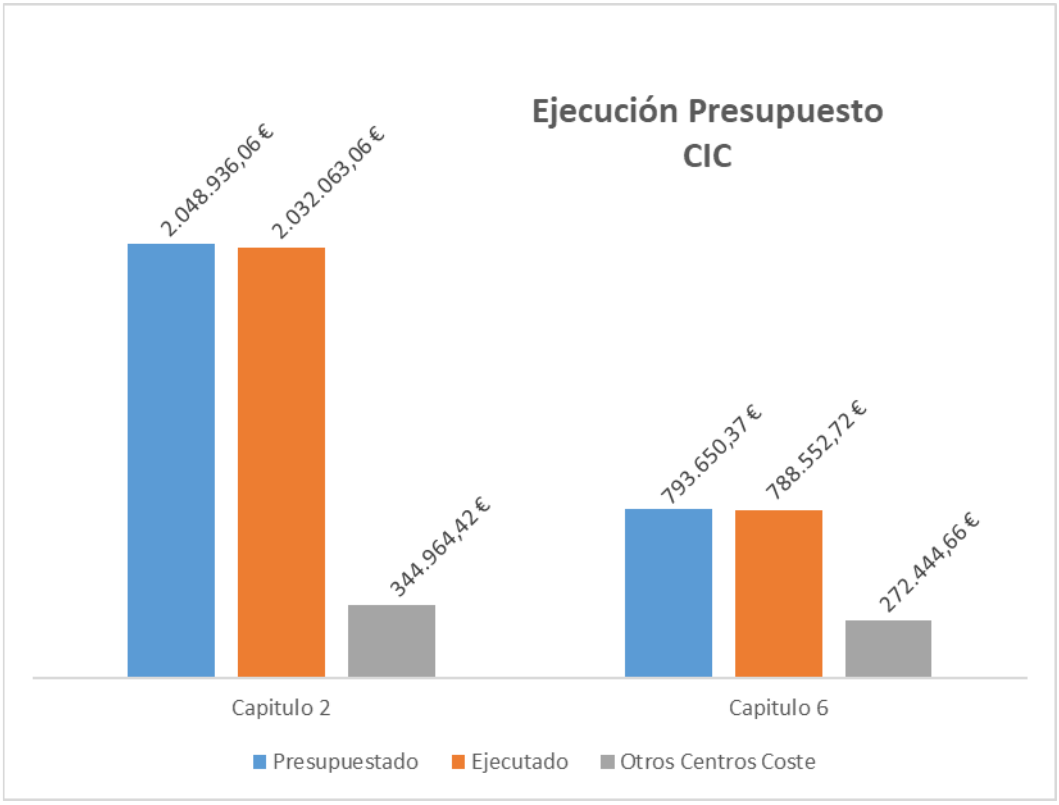
GESTIÓN ADMINISTRATIVA

Gestión Económica y Contratación

Durante el curso 2024/2025, la Oficina de Gestión Administrativa ha asumido una elevada carga de trabajo, derivada principalmente de los procesos de contratación de servicios y suministros vinculados al funcionamiento del Área TIC.

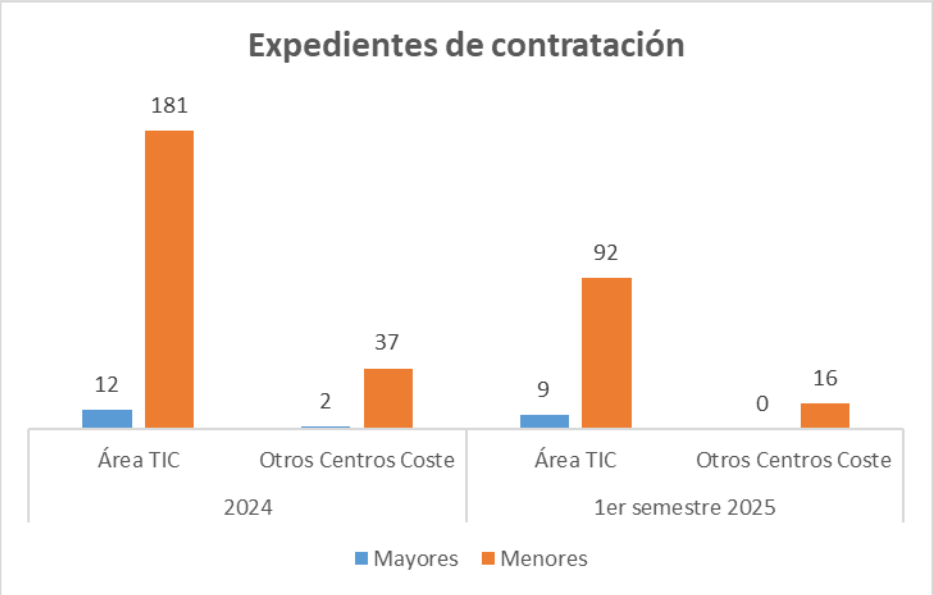
Para facilitar el seguimiento presupuestario, se ha desarrollado una hoja de cálculo que permite conocer en tiempo real el estado de tramitación de cada expediente, así como el grado de ejecución de cada partida y proyecto.

El siguiente gráfico muestra el grado de ejecución del presupuesto del ejercicio 2024.



De acuerdo con la normativa de contratación pública y las directrices de Gerencia, se han formalizado contratos mayores y menores, aplicándose en estos últimos, cuando procede, el mecanismo de adjudicación directa. Además, desde el Área se han tramitado solicitudes y valoraciones de ofertas correspondientes a servicios y suministros de otros Centros de Coste.

El siguiente gráfico muestra el número de expedientes de cada tipo tramitados a lo largo del año 2024 y el primer semestre de 2025.



En total, estos procedimientos han generado la emisión de 361 justificantes de gasto en 2024 y de 113 en el primer semestre de 2025.

En cuanto a inversiones con cargo al capítulo 6, se han tramitado 979 fichas de inventario en 2024 y 1.047 en el primer semestre de 2025, incluyendo asignaciones a unidades organizativas y bajas de equipos al final de su vida útil.

Trámites Administrativos Complementarios

A lo largo del curso se han emitido 10 informes de ejecución, a petición de proveedores, para su posterior certificación por parte de la Secretaría General.

Asimismo, se han gestionado 81 incidencias o solicitudes mediante la plataforma TIKA, y 32 expedientes electrónicos a través de G-TM. La herramienta Port@firmas ha sido utilizada en 1.187 ocasiones para la firma electrónica de documentos.

En relación con el equipamiento informático, se ha coordinado el préstamo de 178 ordenadores portátiles al PAS, incluyendo la entrega, recogida, intervención técnica y devolución a los/as usuarios/as.

FORMACIÓN Y DESARROLLO DEL PERSONAL

Formación especializada en Tecnologías de la información

Durante el curso 2024/2025, el personal del Área ha participado en un total de 28 actividades formativas específicas del ámbito TIC, no incluidas en el Plan de Formación anual del PTGAS. Estas acciones han estado directamente vinculadas a la implantación de nuevos servicios, proyectos o herramientas tecnológicas y han supuesto una actualización continua de las competencias del equipo.

De las 28 acciones formativas impartidas, 9 se desarrollaron en modalidad presencial y 19 en modalidad virtual, alcanzando una participación del 100 % del personal del CIC. El volumen total de horas de formación asciende a 198, con un coste asociado de 1.887,60 €.

Resumen de datos

- ✓ N.º de actividades formativas distintas: 28
- ✓ Modalidad de actividad formativa:
  - Presencial: 9
  - Virtual: 19
- ✓ % de participación de personal CIC: 100 % (28 de 28)
- ✓ N.º de horas formación TI 2024/2025: 198 horas
- ✓ Coste total: 1.887,60 €

Detalle actividades formativas TI realizadas

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Nuevas funcionalidades en gestión de aplicaciones UXXI	1,00	2
Formación solución Reyes CCN-CERT	3,00	1
Cómo hacer una buena identificación de los sistemas de información en el contexto del ENS	1,50	2
TIKA: Gestor de incidencias corporativo. Manejo de la nueva versión	2,00	27
Plataforma G-ONCE: Capa de interoperabilidad GUADALTEL	13,00	2
XIX Curso STIC - Seguridad en Aplicaciones Web (INAP)	50,00	1
Curso práctico sobre la aplicación Marco	3,00	2
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Planes de Estudio	3,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Actas I	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Actas II	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Expediente	3,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Gestión Económica I	3,00	3

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Gestión Económica II	3,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Gestión Económica III	3,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Horarios	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Matrícula I	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Matrícula II	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Recursos docentes I	2,00	3
Conocimiento del modelo de datos del núcleo de UNIVERSITAS XXI-ACADÉMICO. Recursos docentes II	2,00	3
Integración con portafirmas	6,00	4
Transformación Digital Segura: Uso y Normativa de Certificados Digitales	1,50	1
Elsa - Universidades	1,50	1
Formación aplicación EDUS (Evaluación Desempeño Universitario)	9,00	3
UDS Education 4.0	12,00	2
Construcción de sistemas de información utilizando servicios comunes	20,00	1
Uso e integración de APIs del sistema de administración electrónica G-ONCE	14,50	2
Formación técnica para administradores de la plataforma CONSEG	7,00	2
Oracle23. Oracle Restful Services. ORDS-0001	12,00	10
Formación para administradores-formadores de la plataforma CONSEG	12,00	2

Acciones formativas TI por participante

Participantes en 1 actividad formativa: 13
Participantes en 2 actividades formativas: 5
Participantes en 3 actividades formativas: 3
Participantes en 4 actividades formativas: 3
Participantes en 7 actividades formativas: 1
Participantes en 14 actividades formativas: 1
Participantes en 15 actividades formativas: 1
Participantes en 19 actividades formativas: 1
Personal que no participa en ninguna actividad formativa: 0

Formación transversal y Participación Institucional

Además de la formación técnica, el personal ha tomado parte en diversas actividades de carácter transversal, centradas en el desarrollo de competencias profesionales como el teletrabajo, la protección de datos, la actitud de servicio o la inteligencia emocional.

Nombre actividad formativa	Duración (horas)	N.º de participantes
Teletrabajo: Cómo prevenir riesgos laborales trabajando desde casa o a distancia	1,25	16
Creación y gestión de formularios web	6,00	4
Teletrabajo para managers	4,60	3
Cómo plantear objetivos según la metodología OKR	0,50	1
Como demostrar actitud de servicio en el sector público	1,25	2
Habilidades para el teletrabajo	1,25	12
Eficiencia y productividad diarias para personal público	1,25	2
Inteligencia Artificial	1,00	1
Lenguaje no verbal digital: Cómo conectar más allá de la pantalla	0,50	1
Primeros auxilios	3,00	1
Mindfulness para la reducción del estrés en el trabajo	1,50	1
Buenas prácticas en materia de transparencia y protección de datos personales	6,00	1
Conducción emocional: consciencia plena para una conducción segura	1,00	1
Cuidar para avanzar: Gestión del tiempo en el trabajo y el hogar	4,00	6
Curso práctico sobre la aplicación Marco	3,00	2

Asimismo, el Área ha tenido una participación activa en eventos y jornadas de interés institucional, las siguientes:

- Jornadas CRUE Digitalización 2024
- Experiencias con WAZUH, la plataforma de seguridad de código abierto47ª Jornadas CRUE Digitalización
- Ransomware detección y protección
- XVIII Jornadas STIC CCN-CERT
- Evento “Nuevo Modelo de Identidad Digital: telemática y segura”
- Presentación del portal de servicios en UXXI-RRHH
- Seminario Gestión Pública Universitaria. La Inteligencia Artificial aplicada a la Gestión Universitaria
- Servicios REST UXXI, integraciones y desarrollos satélite de UXXI
- Evento Transformación Digital CRUE-TIC
- Jornadas Certidigital
- Evento Identidad Digital
- Jornadas CRUE Digitalización 2025

Estas actuaciones refuerzan el compromiso del Área con la mejora continua, la adaptación a los nuevos retos tecnológicos y la implicación institucional en la transformación digital del entorno universitario.

SERVICIO DE REDES Y EQUIPAMIENTO

Redes, comunicaciones e infraestructura

Servicio de Red Inalámbrica WIFI

Mejora del Servicio

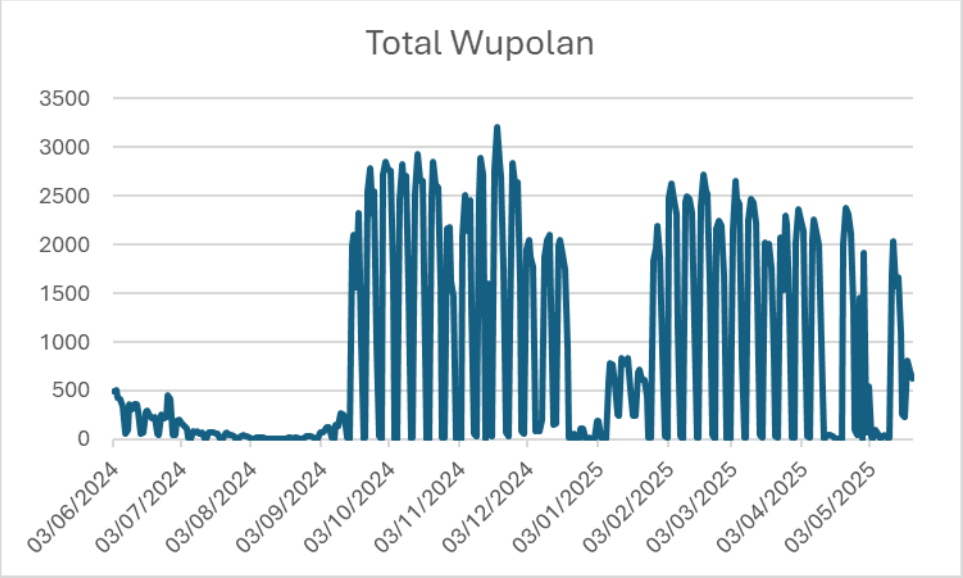
La red WiFi de la Universidad Pablo de Olavide se ha consolidado como un recurso fundamental para el desarrollo de las actividades docentes, investigadoras y administrativas. A través de ella se conectan desde ordenadores portátiles y dispositivos móviles personales hasta relojes inteligentes y pantallas digitales en aulas y zonas comunes. Por ello, el Centro de Informática y Comunicaciones (CIC) ha priorizado la ampliación de la cobertura y la mejora de la calidad de la conectividad, comenzando por las áreas con mayor densidad de uso.

Durante el presente curso académico se ha renovado íntegramente la infraestructura inalámbrica del Edificio 24, implantando tecnología WiFi 6. Esta actualización, iniciada el curso anterior en espacios como el Edificio de Rectorado, proporciona mayor ancho de banda, permite un mayor número de conexiones simultáneas por punto de acceso, optimiza el uso de dispositivos audiovisuales y mejora la gestión de la red, asegurando que cada persona usuaria esté conectada al punto con mejor rendimiento disponible.

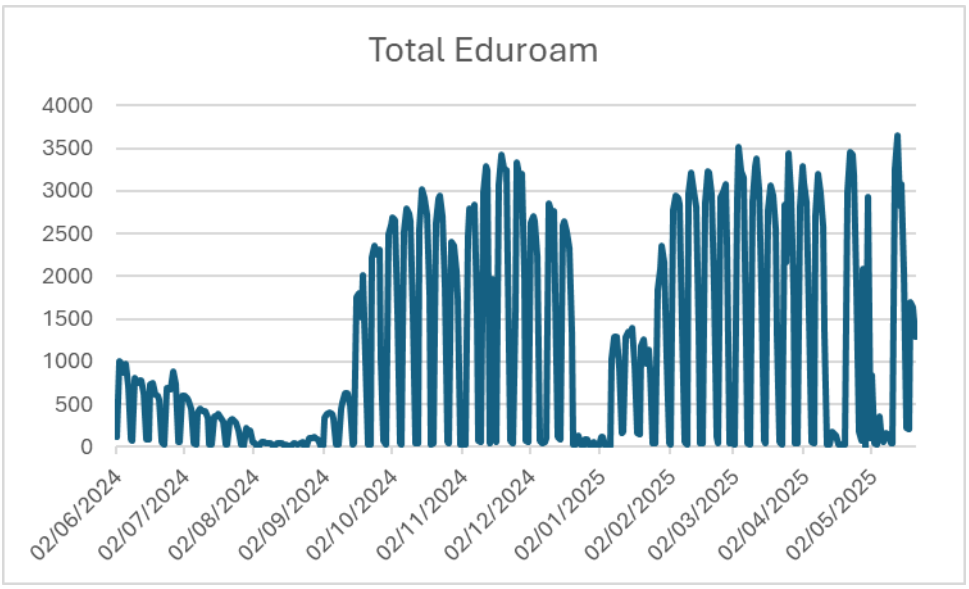
Conectividad

El uso de la red WiFi de la UPO ha experimentado un notable crecimiento, con un incremento del 66 % en el número de usuarios respecto al curso anterior. A continuación, se incluyen gráficos que muestran la evolución del volumen de conexiones en las distintas modalidades disponibles (WUPOLAN y EDUROAM).

CLIENTES WUPOLAN



CLIENTES EDUROAM



TELEFONÍA

La Universidad Pablo de Olavide ha avanzado significativamente en la modernización de su infraestructura de telecomunicaciones mediante la adjudicación del Lote 1 del contrato de Servicios Unificados de Comunicaciones de Voz y Datos a la empresa MasOrange. Esta iniciativa se enmarca en un plan estratégico de renovación tecnológica orientado a optimizar los servicios de voz fija y móvil, así como a reforzar la seguridad y la eficiencia en el acceso a datos en movilidad.

Actualmente se encuentra en curso la fase de implantación, que contempla estudios de cobertura destinados a eliminar zonas sin señal (“puntos de sombra”), así como un análisis pormenorizado de las extensiones existentes. Todo ello con el objetivo de garantizar una transición ordenada desde el proveedor anterior, Telefónica de España, minimizando el impacto sobre las personas usuarias y asegurando la continuidad del servicio.

Red de datos

En el marco del mismo contrato, el Lote 3 ha sido adjudicado a Telefónica de España. Este lote incluye actuaciones orientadas a mejorar la conectividad y la seguridad en las sedes externas de la Universidad Pablo de Olavide, concretamente en:

- **Carmona**
- **Pabellón de Marruecos** (anteriormente Sede de la Calle Laraña)
- **Complejo Universitario Flora Tristán**

Las principales acciones contempladas son:

- El aumento del caudal de conexión a Internet en estas localizaciones, con el fin de mejorar la experiencia de uso y garantizar la disponibilidad del servicio.
- La implantación de un sistema de cortafuegos (firewall) que refuerce la seguridad perimetral, protegiendo a las personas usuarias frente a amenazas externas.

En el momento de redactarse esta memoria, se están coordinando los trabajos con la empresa adjudicataria para ejecutar las mejoras previstas.

SEGURIDAD EN LAS COMUNICACIONES

La seguridad constituye un componente esencial en la gestión de las tecnologías de la información y las comunicaciones. Entre las medidas estratégicas adoptadas para reducir los riesgos asociados al tráfico de red destaca la segmentación de grupos de trabajo.

Uno de los segmentos más amplios dentro de la red institucional corresponde al estudiantado, que concentra una elevada diversidad de dispositivos conectados: ordenadores portátiles, tabletas, relojes inteligentes y equipos pertenecientes a personas invitadas, entre otros.

Con el objetivo de proteger la integridad del sistema, se ha desplegado un cortafuegos (firewall) que establece una separación tanto física como lógica entre este segmento y el resto de la red universitaria. Esta medida no solo restringe la interacción entre segmentos, sino que también proporciona un nivel adicional de protección frente a amenazas tanto externas como internas.

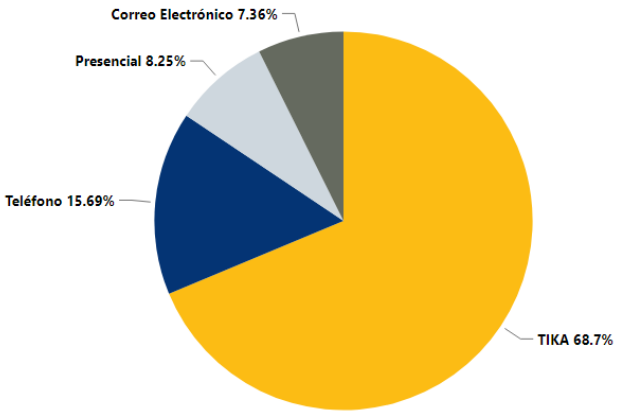
CENTRO DE SERVICIOS

El Centro de Servicio (CS) constituye un punto de atención consolidado dentro del Centro de Informática y Comunicaciones (CIC), proporcionando soporte personalizado a toda la comunidad universitaria.

A lo largo del periodo analizado, el CS ha gestionado un volumen significativo de solicitudes, siendo la plataforma TIKA la vía más utilizada por las personas usuarias, seguida por las llamadas telefónicas. Este servicio continúa siendo una pieza clave en la atención a incidencias, consultas y peticiones relacionadas con los servicios TIC de la Universidad.

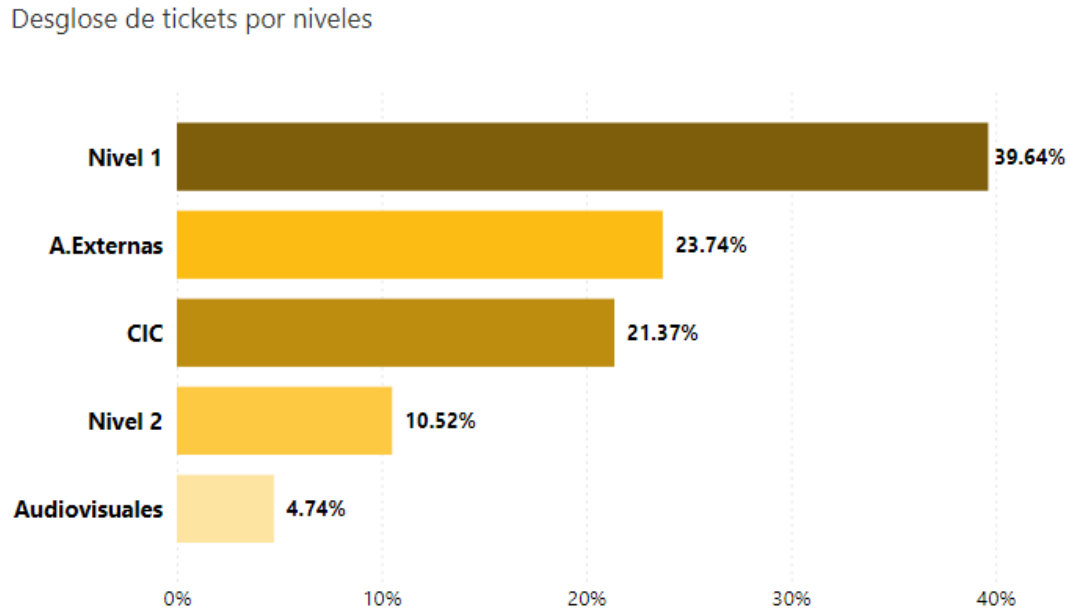
Periodo; junio 2024 a mayo 2025

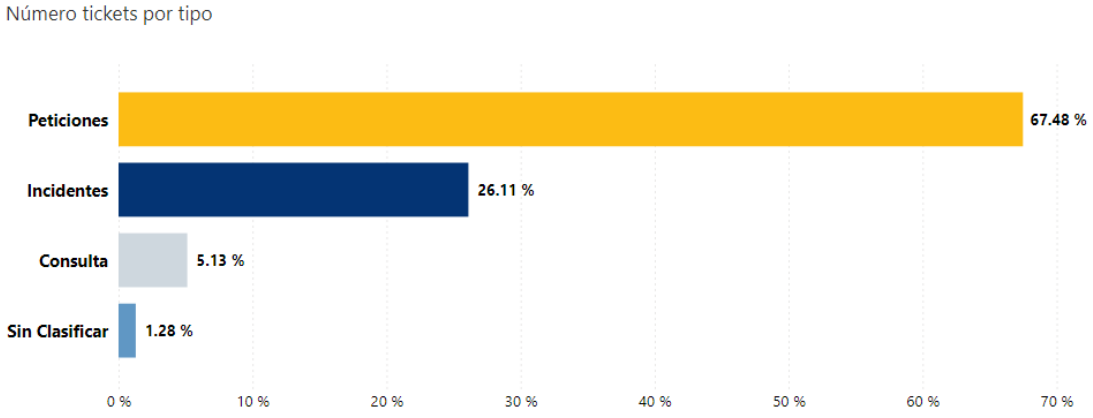
Número tickets por canal de entrada



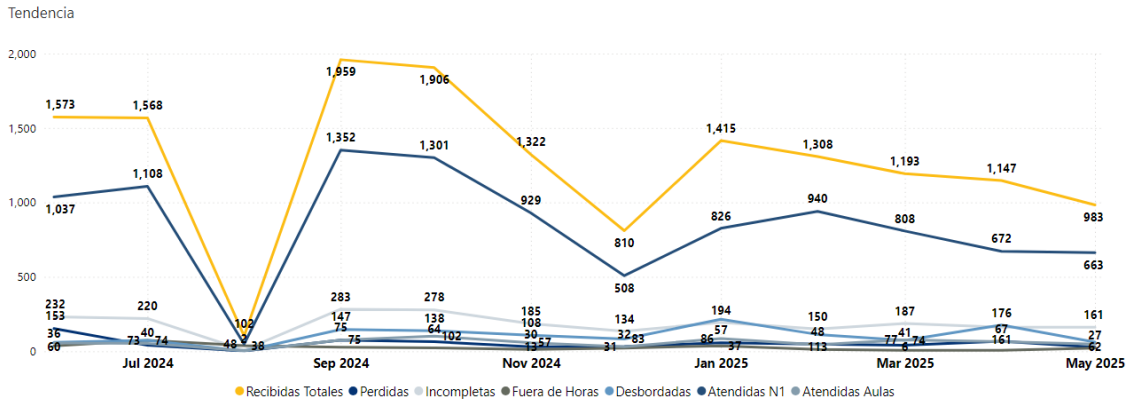
Tickets creados: Se observa una disminución importante, en los tickets creado con respecto al año anterior.

ATIC-023-2025

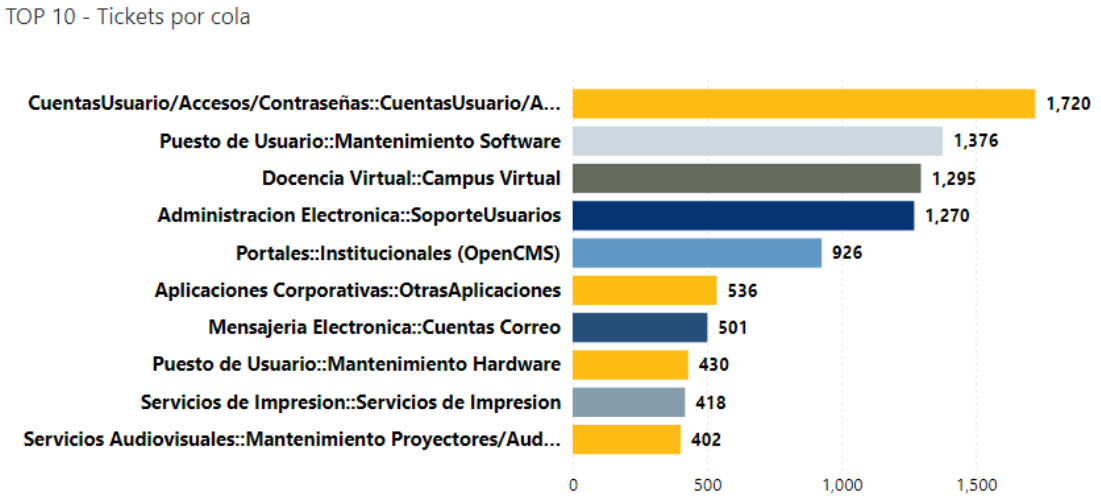




Atención telefónica: se observa en esta gráfica el elevado número de llamadas que recibe el Centro de Servicio, aunque se denota un decremento respecto al año anterior.



Top Ten de tickets por cola: una cola para el CS es el modo de agrupar las solicitudes de las personas usuarias. A continuación, se muestra un gráfico con las diez colas (temas) que más tickets generan.



ESPACIO MULTIMEDIA

La Universidad Pablo de Olavide impulsa su Transformación Digital con nuevas dotaciones audiovisuales

En sintonía con los avances tecnológicos que transforman el entorno académico, la Universidad Pablo de Olavide continúa dando pasos firmes hacia la transformación digital de sus espacios docentes y administrativos. A través del Centro de Informática y Comunicaciones, la institución ha acometido en los últimos años diversas mejoras en materia de asistencia y dotación audiovisual, con el objetivo de adaptar sus instalaciones a los nuevos escenarios educativos que demanda la Educación Superior.

Actualización de aulas y nuevos equipamientos

Desde la irrupción de la pandemia por la Covid-19, todas las aulas de docencia de la Universidad fueron equipadas con tecnología audiovisual para facilitar la enseñanza a distancia. Sin embargo, en el último año, se ha hecho un esfuerzo adicional hacia la Transformación Digital mediante la conversión progresiva de las aulas convencionales en aulas digitales interactivas. Estos espacios incorporan monitores digitales interactivos y botoneras programadas que simplifican el manejo de los equipos, mejorando significativamente la experiencia docente.

Actualmente, esta tecnología se encuentra instalada en el edificio 14 (aulas 4 y 5), edificio 24 (aula 1.11) y edificio 3 (aula 1). Asimismo, se encuentra en fase de adjudicación la implantación de estos sistemas en otras tres aulas: edificio 2 (aula 2), edificio 6 (aula 2) y edificio 7 (aula 1). Esta iniciativa busca fomentar una docencia más dinámica, participativa e intuitiva, apoyada en herramientas de última generación.

Aplicación tecnológica en espacios institucionales

El despliegue de esta infraestructura también ha alcanzado espacios de gestión institucional, mediante el aprovechamiento de equipamiento previamente disponible. Se han instalado monitores digitales interactivos en las salas de Gerencia, Vicerrectorado de Planificación Estratégica y Vicerrectorado de Transformación Digital, facilitando la celebración de reuniones tanto presenciales como virtuales, y mejorando la presentación de contenidos.

De igual modo, se han habilitado con sistemas similares las salas de reuniones de la Biblioteca y del propio Centro de Informática y Comunicaciones, reforzando así las capacidades tecnológicas en contextos no docentes, pero igualmente estratégicos.

Refuerzo de equipamiento audiovisual

Asimismo, el antiguo aula de idiomas del edificio 14, ahora reconvertida en aula de informática, ha sido equipada con un proyector de 3.200 lúmenes y un sistema de sonido con control de volumen mural, garantizando un entorno óptimo para la formación en competencias digitales.

Con el objetivo de reducir posibles incidencias técnicas y asegurar la continuidad de la actividad docente, se han adquirido además seis proyectores Epson EB-W49 de repuesto, que permitirán una respuesta rápida ante cualquier eventualidad técnica.

Nuevas posibilidades para la difusión del conocimiento

En el marco de esta estrategia de modernización, se ha reactivado la Sala de Grados 2 de la Biblioteca —anteriormente conocida como Sala CEI CAMBIO—, la cual ha sido equipada con un sistema de grabación y retransmisión en streaming, lo que la convierte en un espacio idóneo para la celebración de seminarios, presentaciones y actos académicos de interés para la comunidad universitaria.

Además, se ha habilitado la posibilidad de transmitir en directo los eventos celebrados en el Paraninfo de la Universidad a través de los monitores de Cartelería Digital distribuidos por el campus, lo que amplía significativamente el alcance y la visibilidad de los actos institucionales.

Finalmente, cabe destacar el notable incremento en la producción y difusión de contenidos audiovisuales a través de la plataforma UPOtv. Durante el último año, se han publicado 852 nuevos vídeos, de los cuales 417 son de acceso público y 437 de carácter privado. Desde su puesta en funcionamiento en 2010, UPOtv acumula un total de 6.197 vídeos disponibles, consolidándose como una herramienta estratégica para el apoyo a la docencia, la divulgación y la proyección institucional de la Universidad Pablo de Olavide.

MyAPPS

El servicio MyApps, que permite el acceso en la nube a las aplicaciones utilizadas en las aulas de informática, se ha consolidado como una herramienta clave para el desarrollo de prácticas académicas y la realización de exámenes.

Su accesibilidad a través de navegadores compatibles con HTML5 lo convierte en una solución universal, sin necesidad de instalaciones locales, lo que resulta especialmente útil para el estudiantado, independientemente del sistema operativo o dispositivo utilizado.

Como resultado de su madurez tecnológica y su adopción generalizada, el número de incidencias reportadas ha disminuido de forma significativa. Las solicitudes actuales se centran, en su mayoría, en peticiones del personal docente para la actualización de software o la incorporación de nuevas aplicaciones a la plataforma.

A continuación presentamos una serie gráfica de rendimiento de la plataforma.

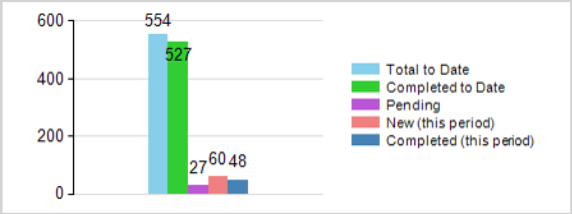
1. INCIDENCIAS

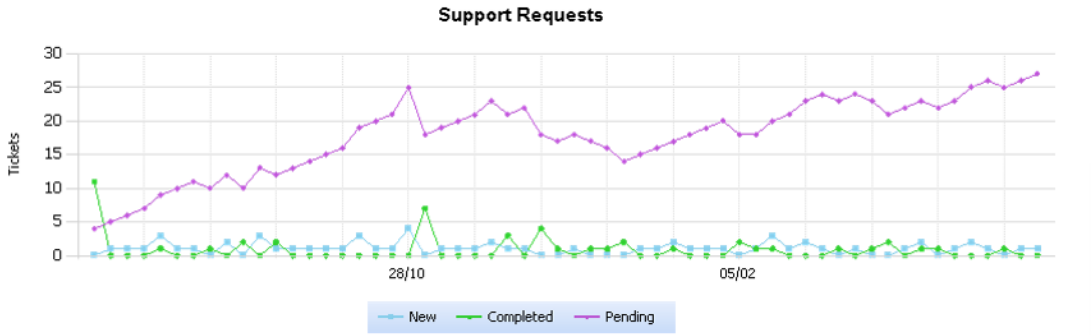
Support Service Summary

From Date: **26-May-2024**
To Date: **26-May-2025**

Total Requests this Period: **60**
Total Completed this Period: **48**
Total Requests to Date: **554**
Total Completed to Date: **527**
Pending: **27**

Total Different Users this Period: **6645**
Total Apps in Production: **272**





2. 12 APLICACIONES MÁS USADAS

Application Concurrency

From: **01-Jun-2024**
To: **31-May-2025**

Published Applications: **272**
Total Distinct Users during this Period: **6482**
Max Concurrency peak: **197** (on **14-May-2025 12:05**)

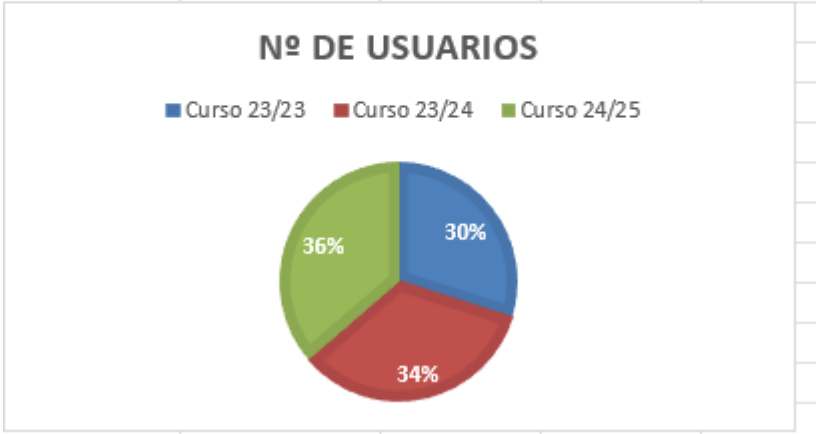
Application Concurrency

From: **01-Jun-2023**
To: **31-May-2024**

Published Applications: **254**
Total Distinct Users during this Period: **6117**
Max Concurrency peak: **213** (on **14-May-2024 18:05**)

3. N.º de usuarios/as por curso

Curso	Nº de Usuarios
Curso 23/23	5411
Curso 23/24	6118
Curso 24/25	6578



Application	Users
ibm spss statistics	2667
wolfram mathematica_v14	1288
adobe_reader	1203
microsoft excel	969
microsoft word	678
wolfram mathematica_eng_v14	626
microsoft excel 2019	560
adobe_acrobat	512
eviews_13	504
wolfram mathematica_v13	412
microsoft word 2019	412
eviews_14	354

Equipamiento, Aulas y Laboratorios

Puesto de Usuario

La Universidad Pablo de Olavide utiliza Microsoft Intune como plataforma de gestión centralizada de los puestos de usuario. Actualmente, se administran a través de este sistema un total de 2.812 equipos informáticos. Intune permite aplicar configuraciones de manera remota y desatendida en 41 perfiles diferentes, facilitando así tareas de actualización y mantenimiento sin necesidad de intervención técnica presencial.

El catálogo de aplicaciones disponibles en Intune incluye 91 títulos, que abarcan tanto las herramientas utilizadas habitualmente por el personal universitario como aquellas específicas para aulas de informática y docencia.

Programa PAROE 2024

Tras completar el proceso de transición iniciado con los programas Renove 2021 y 2022 —que supuso la adopción de Intune, la gestión de inventario mediante Microsoft Lists, Forms y Teams, y la utilización del Sistema Dinámico de Adquisiciones—, en 2024 se ha ejecutado íntegramente el PAROE (Procedimiento de Adquisición, Renovación y Optimización de Equipos Informáticos Corporativos).

En el marco de este programa se ha procedido a la renovación de 235 equipos destinados al Personal Docente e Investigador (PDI), distribuidos en 182 ordenadores de sobremesa y 53 portátiles.

Programa Renove 2023

Desde la entrada en vigor del PAROE, la denominación "Renove" queda reservada a la renovación de equipos informáticos en aulas docentes. En el marco del Renove 2023, se han sustituido un total de 139 equipos.

Los dispositivos retirados del PAROE y del programa Renove se reutilizan en contextos con menores requisitos técnicos —como laboratorios, seminarios, conserjerías, cartería o puntos de información—, prolongando su vida útil y extendiendo su periodo de amortización hasta un mínimo de ocho años.

Puesto de Usuario Móvil

Con el objetivo de ofrecer mayor flexibilidad, se ha implementado en diversas áreas del PTGAS el **modelo de Puesto de Usuario Móvil**, basado en la sustitución de los equipos de sobremesa por portátiles conectados a estaciones de acoplamiento. Esta configuración permite al personal mantener una experiencia de usuario equivalente, tanto en la oficina como en el domicilio, sin necesidad de equipos adicionales ni configuraciones específicas de acceso remoto.

Actualmente, **20 áreas** han adoptado este modelo, sumando un total de **162 puestos móviles**.

Base de Datos de Inventario

La base de datos de equipamiento informático ha sido consolidada en la plataforma **SharePoint**, donde se gestiona de forma centralizada y se exporta diariamente para su consulta por los distintos departamentos. Esta base de datos recoge datos de ubicación, estado y asignación de los siguientes recursos:

- PCs de sobremesa: 3.290
- Portátiles: 844
- Dock Stations: 200
- Monitores: 249

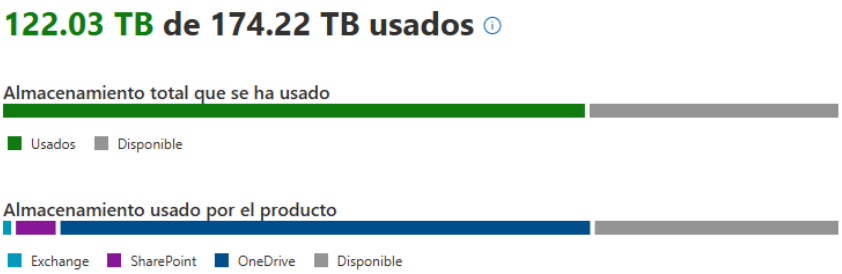
Almacenamiento de Archivos: Samba – SharePoint – OneDrive

El sistema de compartición de archivos Samba, empleado principalmente por el PAS, mantiene una utilización estable:

- Espacio ocupado: 4,1 TB
- Grupos activos: 134
- Usuarios: 607

Dado el carácter obsoleto de este sistema, las áreas que migran al modelo de Puesto Móvil están trasladando sus datos a **SharePoint**, lo que permite un acceso más ágil y seguro a la información, así como mejores opciones de recuperación de datos.

Además, se está impulsando el uso de **OneDrive** como solución de almacenamiento personal para el conjunto de usuarios/as.



Plataforma BSCW

La herramienta colaborativa **BSCW** es utilizada por personal docente, de administración y estudiantes de postgrado. Cuenta actualmente con:

- Usuarios/as registrados/as: 8.788
- Volumen de datos: 3,5 TB

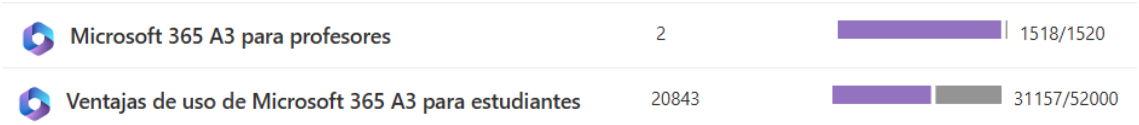
Dado que la versión actual ha sido discontinuada y su nueva versión pasa a modelo de pago en la nube, se contempla su **sustitución por SharePoint**, más alineado con el ecosistema Microsoft implantado.

Licencias Campus

La Universidad ha adquirido licencias Campus para los siguientes programas:

- **Matlab**
- **ArcGIS Pro**
- **ArcGIS Online**

En cuanto al entorno Microsoft 365 (anteriormente Office 365), se cuenta con **22.694 usuarios activos**, a los que se han asignado las correspondientes licencias de uso institucional.



Aulas

En el marco del *Renove 2024*, se han actualizado **149 equipos de aula** al sistema operativo **Windows 11**. Asimismo, se sigue avanzando en la transición a este sistema en todos los equipos compatibles.

Actualmente, el parque informático de las aulas se distribuye de la siguiente forma:

- **Windows 10**: 21 aulas – 365 equipos
- **Windows 11**: 16 aulas – 262 equipos

Aplicaciones Virtuales UDS

El sistema de aplicaciones virtualizadas mediante la plataforma **UDS** está orientado principalmente al personal del PTGAS, aunque también es utilizado por usuarios con equipos Mac o Linux para acceder a servicios que requieren tecnologías específicas, como **Internet Explorer**, necesario para determinadas aplicaciones institucionales.

GESTIÓN DE SEGURIDAD

Descripción de tareas seguridad de la información

Política, normas, procedimientos e informes

La actual Política de Seguridad de la Información de la UPO se aprobó en 2019. Se hace necesaria la adaptación de dicha política a las modificaciones en la normativa vigente, Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, aprobado por el Consejo de Ministros de 3 de mayo de 2022, y a la guía CCN-STIC 881A Perfil Cumplimiento Específico Universidades.

La aprobación de la nueva política requiere tratamiento conjunto en materia de protección de datos y el impulso desde la Comisión de Seguridad de la Información quien debe proponer y revisar la Política de Seguridad de la Información.

La falta de revisión y una mayor difusión de la Política se ha puesto de manifiesto tanto en el informe anual de INES, en el análisis de riesgo y en la declaración de aplicabilidad con evaluación de medidas de madurez, así como en la auditoría de GAP – ENS y la auditoría de la Cámara de Cuentas (ver apartado específico).

Se mantienen en fase de borrador a la espera de revisión y aprobación las siguientes normativas y procedimientos internos:

- Procedimiento de actuación en caso de llegada de spam.
- Normativa y procedimiento de Gestión de incidentes.
- Normativa y procedimiento de acceso a áreas seguras TIC.
- Normativa de buen uso de áreas seguras.
- Procedimiento de extracción de datos de equipos corporativos.

- Procedimiento de registro de accesos a servicios expuestos al exterior.
- Procedimiento de solicitud y uso de llave electrónica genérica.

La auditoría GAP-ENS propondrá en su informe de resultados la normativa y procedimientos de desarrollo que deberán abordarse para el cumplimiento del ENS.

Se han generado los siguientes informes:

- INF_CIC-16_swlabccee_v01r01.docx Informe software de Laboratorios
- INF_CIC-16_ENS_Subred_v01r03
- Pro_CIC-16_Vulnerabilidades_v01r01
- INF_CIC-16_Informe Análisis de Seguridad CONSIGNA-PRE
- INF_CIC-16_Análisis_EDR_v.2r0.docx
- INF_CIC-16_Informe Análisis de Seguridad PORTAFIRMAS_v.1.0
- INF_CIC-16_auditoria_aplicaciones_v.1.0
- PRO_CIC-certificados_v.1.0
- INF_CIC-Sello_v1r1.docx
- INF_CIC-Anexo_Sello_v1r1.docx
- INF_CIC-16_ENS_contratacion_modelos_v.1.0 .docx
- INF_CIC-16_ENS_contratacion_clausulas.v.2.0.docx

Comisión de Seguridad de la Información y Protección de Datos

Durante el curso 2024/2025 no se ha reunido la Comisión de Seguridad y Protección de Datos.

Análisis de riesgos e indicadores

Se ha realizado la revisión del Análisis de Riesgo sobre los sistemas bajo el alcance del ENS. Se ha realizado con la Herramienta PILAR RM 2024.3.4 (6.9.2024), dando continuidad a los criterios establecido en análisis anteriores e incorporando la nueva tabla de medidas del ANEXO II del nuevo ENS.

El proceso de revisión actualiza los valores de indicadores a:

- Riesgo potencial máximo (si no se aplicaran salvaguardas): 5,0 (escala 0-10) – MUY ALTO.
- Riesgo presente máximo (con las salvaguardas aplicadas actualmente): 3,5 (escala 0-10) – ALTO.

Se genera la siguiente documentación:

- Informe ejecutivo INF_CIC-16_analisis_de_riesgo_2025.doc.
- SOA_Declaración de Aplicabilidad de Medidas del ENS_2025.
- Fichero de análisis de riesgo 2025.

Se genera también el valor del indicador de gestión de la seguridad establecido en marco con un valor de 2,06. Se elabora el informe con el valor y el procedimiento de cálculo.

Los niveles de riesgo deberán ser aprobados en la siguiente reunión de la Comisión de Seguridad de la Información y Protección de Datos.

Los valores del riesgo apenas se modifican respecto a años anteriores, ya que, aunque se apliquen progresivamente mejoras en la seguridad, existen áreas con riesgos altos (como el control de acceso y gestión de identidades) que determinan el valor de estos indicadores.

Gestión de incidencias de seguridad

Se realiza el análisis anual de la gestión de incidentes sobre el año anterior. Se han producido un total de 333 incidentes de seguridad.

	Origen	Número	%
Externo			
Andalucía CERT	ACERT	0	0
INCIBE-CERT	INCIBE	2	0,60
CCN-CERT	CNN-CERT	0	0
Proveedores con sistemas externos	PRO	2	0,60
Proveedores con sistemas en la UPO	PRU	0	0
Ciudadanos	CIU	0	0
Auditorías	AUD	0	0
Interno - Sistemas detección automática			
Servicio Antivirus	VIR	4	1,20
Sonda SAT-INET	SAT	82	24,62
Servicio Antispam	SPA	29	8,71
Otros servicios de monitorización	MON	16	4,80
Interno - Personal UPO			
Responsables UPO	RPS	1	0,30
Personal upo	USR	195	58,56
Interno - Personal CIC			
Jefe de gestión de seguridad	JGS	0	0
Dirección del CIC	DIR	1	0,30
Administradores de sistemas CIC	ADM	1	0,30
Otros	OTR	0	0

Se produce un cambio de tendencia con respecto a los años anteriores y suben los incidentes de seguridad. Mientras que desde 2020 hasta 2023 la tendencia ha sido la caída del número de incidentes que se registran en la Universidad, en el año 2024 se ha incrementado este valor en un 24.71% con respecto al año anterior. Este incremento se debe a un importante aumento de los incidentes relacionados con las categorías de código dañino, disponibilidad y fraude.

El cambio en la tendencia en el número total de incidentes atiende a:

- El incremento de incidentes detectado por la sonda SAT-INET.
- El incremento de registro de solicitudes de restauración de información motivadas por el borrado de datos accidental en las unidades compartidas.
- Aumento de identificación de incidentes de falta de disponibilidad como incidentes de seguridad.
- Debido al éxito de las campañas de educación en Ciberseguridad realizadas, se han cuadruplicado las notificaciones de la comunidad universitaria de correos sospechosos que han llegado.
- Incorporación de nuevas herramientas y capacidades de detección.

Además de la resolución de cada uno de los incidentes individuales, los análisis de las incidencias detectadas han permitido otras actuaciones encaminadas a la mejora de la gestión de la seguridad:

- Se ha procedido a informar y concienciar a usuarios/as cuyos equipos se han visto implicados en algún incidente de seguridad.
- Se han detectado situaciones de riesgo como la cuenta del rector en relación a los ataques dirigidos y se ha dado una formación específica a sus gestores.
- Mejora en la configuración de sistemas de detección a detección de cuentas de correo comprometidas, antes de realizar un ataque con impacto.
- Incremento en el número de equipos protegidos por antivirus profesional.
- Separar la gestión de incidentes de la gestión de vulnerabilidades para poder dar un tratamiento más adecuado a cada tipo de registro y realizar informes más específicos.

Deber de notificación de incidentes

Durante 2024 no se ha procedido a la notificación oficial al CCN-CERT ya que no se han registrado incidentes de nivel alto o superior.

Durante el periodo que abarca la presente memoria se ha producido dos incidentes de relevacia, el apagón general del 28 de abril y el incidente de seguridad del 12 de junio que tuvo una afectación total sobre los sistemas informáticos (ver apartado siguiente).

El apagón general de 28 de abril tuvo una causa externa y los servicios de la Universidad no se vieron afectados significativamente gracias a que los sistemas alternativos de energía funcionaron correctamente. La afectación general de las comunicaciones y la parada de servicios no críticos para optimizar el consumo energético, matuvieron los servicios inalcanzable durante el periodo que duró el incidente. Una vez recuperado el suministro energético se restableció el funcionamiento normal. No se notifica a los CERTs por no tratarse de un ciberincidente en nuestros sistemas y no afectarse la integridad de los mismos.

Comunicación de incidentes

La Universidad ha actuado de forma proactiva en la notificación de incidentes de seguridad a los Certs en relación con detecciones de incidentes:

- Denuncia a los sistemas antispam de correo spam no marcado como tal, para la mejora en los sistemas de detección antispam, con un total de 64 notificaciones.
- Denuncia a proveedores de aplicaciones y servicios de la Universidad de incidentes o vulnerabilidades críticas detectados en sus sistemas.

Gestión de vulnerabilidades

El creciente número de incidentes de seguridad y la automatización de los ataques exigen elevar el nivel de madurez en las medidas preventivas y correctivas que permitan evitar impacto en la organización.

El Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo) obliga a la implementación de una serie de medidas y a la adopción de principios que permitan mitigar los riesgos de sufrir un incidente de seguridad, y poder así garantizar una adecuada protección de los servicios públicos y la información que manejan las administraciones. En particular, en sus artículos 8, 10 y 21 exponen la necesidad de realizar acciones que permitan identificar y tratar vulnerabilidades del sistema.

Una vulnerabilidad se define como una debilidad de un activo o de un control que puede ser explotada por una o más amenazas. [UNE-ISO/IEC 27000:2014]. Las vulnerabilidades son las debilidades presentes en el sistema que pueden permitir a un atacante realizar un ataque exitoso.

Se hace necesario mejorar el modelo de gestión de vulnerabilidades para aumentar la madurez de los procedimientos y medidas de control relacionadas. En consonancia con la necesidad detectada se ha trasladado al sistema de gestión de calidad, MARCO, en forma de riesgo en la matriz de riesgos /oportunidades con identificador 2024-408-R-2. Este riesgo está vinculado al compromiso de desempeño del área “Mejora en el procedimiento de detección y tratamiento de vulnerabilidades” desde donde se evaluará el grado de avance.

Asociado a este compromiso de desempeño se han realizado las siguientes acciones:

- Creación de borrador procedimiento de gestión de vulnerabilidades.
- Mejora en la base de datos de registro de vulnerabilidades.
- Generación de nuevo documento de informe anual específico para vulnerabilidades.
- Creación de indicadores.
- Control de equipos servidores fuera de ciclo de vida.
- Creación del laboratorio de seguridad para auditorías técnicas. Creación de plantilla de informe de auditoría. Realización de piloto de auditoría técnica y puesta en funcionamiento.
- Herramientas de monitorización de superficie de exposición.
- Planificación de auditorías internar periódicas de detección de vulnerabilidades y revisión de procedimientos.

El nuevo informe de gestión de vulnerabilidades pone de manifiesto, dando seguimiento a años anteriores, a la necesidad de madurar los controles de vigilancia sobre la detección proactiva de vulnerabilidades y reducción de superficie de exposición.

Se han desarrollado labores de gestión de vulnerabilidades en activos críticos, estableciendo una mayor procedimentación y registro de actualizaciones críticas. Se ha puesto especial atención a las vulnerabilidades que afectan a servicios expuestos a Internet o con accesos externos y se han desplegado parches ante vulnerabilidades críticas. Esta actividad se está realizando a partir de las notificaciones de aviso del CCN-CERT o AndaluciaCERT.

Se ha redefinido una vulnerabilidad a efectos del informe y los indicadores, como una debilidad que se presenta en un sistema concreto. Con esta nueva definición, se han gestionado un total de 162 vulnerabilidades, muchas en relación con tecnologías de publicaciones de páginas web o de virtualización. De especial impacto ha sido la que afectaba a un componente (openssh) de los sistemas Linux que ha tenido

hallazgo en muchas máquinas desplegadas.

Se ha observado una dificultad en el seguimiento de las vulnerabilidades cuya mitigación requiere acciones a medio o largo plazo, como sustitución de sistema, retirada o reinstalación completa.

EDR/MDR

El Perfil de cumplimiento específico para universidades (CCN-STIC 881A) modifica el nivel de cumplimiento básico de la medida [op.exp.6] del Anexo II del ENS para incorporar el refuerzo R4 como obligatorio donde contempla el uso herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - Endpoint Detection and Response).

Durante el curso académico 2024/2025 se mantiene la herramienta EDR en los equipos del CIC, CSU y alianzas externas, así como en el conjunto de servidores administrados por el CIC que dan soporte a los servicios de la Universidad y que se encuentran en producción.

El EDR ofrece capacidad de respuesta y búsqueda proactiva para detectar y aislar amenazas avanzadas mediante procesos de Threat Hunting.

Durante este periodo NO se han detectado incidente en equipos críticos, aunque se han detectado errores de procedimiento relacionado con la descarga e instalación de software.

Concienciación

Acciones formativas

Se han realizado acciones formativas:

- Campaña de formación de paso a puesto móvil. El cambio a puesto de trabajo móvil en el PTGAS se ha acompañado con una sesión formativa presencial en cada área que se incorporaba a la nueva forma de trabajo. En estas sesiones participa la Coordinadora de Seguridad de la Información, explicando los aspectos de seguridad y riesgos que afectan a la nueva forma de trabajo.

- Charla de concienciación y ciberseguridad a equipos de gobiernos. Charla formativa de 2 horas de duración impartida por el CEO de SecureIT sobre el panorama actual del cibercrimen y las responsabilidades de los equipos de gobiernos de las organizaciones.
- Acción formativa al equipo del gabinete del Rector ante la detección de riesgo elevado de fraude en la lista de distribución rector@upo.es.

Se ha detectado necesidad de concienciación para el personal de apoyo a los departamentos, por tratarse de un colectivo que puede ser objeto de ataques dirigidos especialmente a ellos por la naturaleza de las funciones que desempeñan.

Concienciación vinculada a la gestión de incidentes

Se ha mantenido, como en años anteriores, una labor intensa de concienciación a través de correo electrónico desde la cuenta de seguridadti@upo.es, en respuesta a las consultas de los/as usuarios/as. Además, se han

enviado mensajes personalizados a todos/as aquellos/as usuarios/as que se han visto implicados en incidentes de seguridad, ofreciendo una información detallada del incidente e incluyendo recomendaciones de actuación. Se ha insistido en la cuenta de seguridadti@upo.es como punto de contacto único para incidentes de seguridad.

De igual forma se han atendido desde dicha cuenta, por la coordinadora de seguridad de la información, dudas en materia de seguridad que los/as usuarios/as han trasladado al CIC por algunos de sus cauces establecidos (TIKA, seguridadti@upo.es, de forma presencial, o por consulta telefónica).

Siguiendo con la tendencia detectada en años anteriores, se mantiene un importante número de denuncias de incidentes por parte de usuarios/as y consulta ante la llegada de correos sospechosos.

Se registran menor número de quejas que en años anteriores en relación a las molestias que genera la seguridad como, por ejemplo:

- Demoras en algunos procedimientos para cumplir con los requisitos de seguridad.
- Implantación de medidas de seguridad que pueden resultar molestas como el cierre de sesión tras tiempo de inactividad, o el doble factor de autenticación en el acceso remoto.

Proyecto CONSEG de UNIDIGITAL

El proyecto CONSEG Enel marco de los proyectos contemplados en el plan estratégico de transformación digital, ha completado su ejecución. El proyecto comprende:

- Lote 1: plataforma de diseño y gestión de campañas de concienciación. Plataforma de formación para acceso de los usuarios participantes en las campañas.
- Lote 2: materiales multimedia para campañas de formación específicos para el ámbito de las universidades.

Se ha procedido al despliegue on-premise de las herramientas del lote 1 integrándolas con el SSO corporativo y se han realizado los cursos de formación para administradores del sistema y administradores de campañas.

Seminario de Gestión Pública

En el marco del Seminario sobre gestión pública universitaria 2025 “La Inteligencia Artificial aplicada a la Gestión Universitaria” se han abordado diferentes aspectos del uso de la inteligencia artificial, haciendo referencia a los nuevos retos, nuevas formas de trabajo y los nuevos riesgos de seguridad del uso de herramientas que incorporan IA.

Sello C3!Cyber de MetaRed

MetaRed TIC es un proyecto para fomentar la colaboración entre universidades iberoamericanas en materias de transformación digital; su objetivo es compartir buenas prácticas, casos de éxito y realizar desarrollos tecnológicos conjuntos. Surgida del IV Encuentro Internacional de Rectores/as Universia, entre sus iniciativas se encuentran los Reconocimientos C3!Cyber, que otorga con el fin de reconocer el esfuerzo realizado en la difusión, la divulgación y la concienciación sobre la importancia de la ciberseguridad.

La Universidad Pablo de Olavide ha llevado a cabo durante el curso 2024/2025 sendas campañas formativas y de concienciación dirigidas al PTGAS y PDI, así como talleres y cursos de formación dirigidos tanto a la comunidad universitaria como a entidades y al público general de su entorno.

Todas estas iniciativas junto con la participación en el proyecto CONSEG, así como la implicación de la ciberseguridad en los planes estratégicos de transformación digital, han valido para obtener esta distinción que viene a reconocer el compromiso de la universidad con la formación y concienciación en materia de ciberseguridad.

Responsabilidades de seguridad y buenas prácticas

En los nuevos procedimientos en los que se detectan riesgos relevantes en materia de seguridad, se están incorporando anexos con responsabilidades en materia de seguridad y buenas prácticas para evitar que se produzcan incidentes con impacto en la organización. Ejemplo de estos procedimientos:

- Incorporación de nuevos sistemas de información en la infraestructura tecnológica de la UPO.
- Uso del Certificado de Representante de la Universidad.
- Uso de la firma en nombre de la universidad de copias auténticas, de exportaciones, de solicitudes de sellado de tiempo y de la autenticación en la PLACSP (Plataforma de Contratación del Sector Público).

Auditoría

En el marco de mejora en las tareas proactivas de mejora de la seguridad se está trabajando en la planificación de tareas de auditoría interna periódicas que permitan detectar riesgos y vulnerabilidades técnicas y organizativas. En este sentido se han realizado las siguientes auditorías internas:

- Auditoria de uso de la subred 1
- Auditoría de despliegue de herramienta EDR
- Auditoría de despliegue de mi9croclaudia en equipos servidores y personal del CIC
- Auditoria técnica CONSIGNA
- Auditoría técnica Portafirmas
- Auditoría de aplicaciones equipos clientes CIC
- Auditoría técnica MARCO

Para cada auditoría se han generado registros con las vulnerabilidades detectadas, procediendo a su tratamiento y mitigación.

Herramientas y servicios CCN-CERT/redIRIS

ELSA

Tras la participación en el piloto de la herramienta ELSA (descubrimiento de Exposición Local y Superficie de Ataque) la herramienta se ha puesto en producción, realizando además un cambio importante en el interfaz y la inclusión de nuevas funcionalidades.

En el ámbito de mejora en la actividad proactiva de minimización de la superficie de detección y mitigación de vulnerabilidades se está tratando de incorporar la información de esta herramienta, no obstante, estamos encontrando dificultades para la gestión de la información y la identificación exacta de los riesgos mostrados.

Se está en comunicación con el personal al cargo del servicio comunicando errores en la plataforma y solicitando información para poder interpretar correctamente los resultados.

Servicio SAT-INET

El Sistema de Alerta Temprana (SAT) de Internet es un servicio desarrollado e implantado por el Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT) para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna del Organismo adscrito e Internet. Su misión es detectar patrones de distintos tipos de ataque y amenazas mediante el análisis del tráfico y sus flujos.

Durante el periodo que se contempla en la memoria se han resuelto un número de 82 incidentes notificados por la sonda, elevándose el número de incidentes con respecto a periodos similares anteriores.

La mejora en las configuraciones de log de equipos DNS y proxy, nos permiten ahora localizar equipos con mayor efectividad, y por tanto gestionar las alertas con soluciones óptimas. No obstante, la mayoría de los dispositivos localizados son equipos BYOD conectados a la wifi, sobre los que existe poca capacidad de actuación.

EGIDA

El servicio EGIDA de RedIRIS para la protección frente a ataque DDoS se ha consolidado estableciendo los procedimientos formales de comunicación de incidentes. Durante el periodo que comprende esta memoria se han registrado 5 incidentes que han sido parados en tiempo real sin causar impacto significativo en la organización.

LAVADORA

Lavadora es el servicio de protección del correo electrónico, realizando tareas de detección y respuesta ante la llegada de correo malicioso.

Este servicio va mejorándose continuamente y en este periodo ha incluido nuevas funcionalidades:

- Informe mensual de buzones de correo que reciben una cantidad de spam muy por encima de la media.
- Correos de notificación a los destinatarios de correos que no han sido entregados por haberse retenido como correo con adjunto infectados.
- Reporte de análisis de correos maliciosos que superan las barreras y que son entregados a los buzones de correo de los usuarios que lo denuncian y lo reportamos al servicio para que puedan mejorar las capacidades de detección.

IRIS-CERT

Los organismos públicos tenemos obligación de notificación de incidentes de seguridad al CCN-CERt. No obstante tenemos un cert de referencia para la notificación de incidentes y consultas en materia de seguridad. Las universidades hemos tenido como cert de referente el INCIBE-CERT, habiéndose modificado recientemente esta condición y pasando ahora a depender de IRIS-CERT.

El IRIS-CERT funciona mediante la herramienta de comunicación LUCIA en su versión nube, por lo que nos

hemos tenido que dar de alta en este servicio, que aunará las notificaciones del IRIS-CERT y de la sonda SAT-INET.

Certificados electrónicos

Durante el curso 2023/2024 se puso de manifiesto, como así se recogió en la memoria anterior, que el creciente uso de los trámites telemáticos ha obligado al uso de certificados digitales para la identificación de las partes. Ciertos trámites incluidos en procedimientos de gestión requieren el uso de los certificados de representantes de la organización, en particular el certificado del Rector.

Una vez implementada la fase de piloto de la herramienta redtrust para el uso y gestión del certificado de representante se ha acordado un procedimiento de actuación con Gerencia que determina la capacidad de autorización a la Secretaría General.

El gabinete del Rector junto con la Secretaría General, han iniciado una ronda de reuniones con las áreas implicadas del PTGAS para poder procedimentar el uso del certificado electrónico de representante y los procedimientos de recepción de notificaciones legales dentro de la Universidad.

El CIC está asistiendo, tanto a la coordinadora de administración electrónica como a la coordinadora de seguridad de la información, para poder resolver cuestiones técnicas y evaluar posibles riesgos derivados de los acuerdos que se determinen.

Mientras se establece un nuevo procedimiento, si procede, seguirá aplicando el validado por la vicegerencia económica para la autorización en la instalación del certificado de representante.

Se detecta y así se informa a la dirección que se está alcanzando el número máximo de 15 usuarios/as con acceso al certificado de representante del rector y así se informa a la dirección del CIC. Se detecta también un número creciente de trámites en los que se necesita el certificado de representante ya que se está haciendo necesario su uso en las plataformas de gestión de otros organismos, frente al uso de certificados personales.

Formación

El equipo de Seguridad ha asistido a las siguientes acciones formativas:

- Workshop Certidigital para equipo de gobierno
- Workshop Certidigital para equipo técnico (API)
- V Jornadas Digitales Certidigital. Ampliando Horizontes
- Workshop Certidigital para equipo técnico (Arquitectura)
- Webinar Zero-trust: Una visión 360° desde el punto de vista de la identidad
- Herramienta RedTrust
- Gestión de la regulación (NIS2, DORA, ENS)
- Desayuno tecnológico Secure&IT - Sevilla
- Formación solución Reyes CCN-CERT
- Cómo hacer una buena identificación sistemas de información en el contexto del ENS
- Experiencias con WAZUH, la plataforma de seguridad de código abierto
- Webinar: metaOLVIDO: Gestión y tratamiento automático de metadatos
- Webinar: API de LUCIA e integración
- STIC Amazon Web Service (AWS) en el ENS
- Curso de Certificados Digitales

- Curso básico STIC - Seguridad en entornos Windows
- Requisitos de seguridad exigibles a proveedores. ENS y RGPD
- Riesgos y responsabilidad en la IA
- Curso de Trazabilidad del Dato
- Acceso seguro a dispositivos de almacenamiento externo USB Confirmación
- Sesión de concienciación sobre ciberseguridad
- Ransomware detección y protección
- Cómo hacer una buena identificación sistemas de información en el contexto del ENS
- Buenas prácticas en materia de transparencia y protección de datos personales
- XIX Curso STIC - Seguridad en Aplicaciones Web (INAP)
- XVIII Jornadas STIC CCN-CERT

Informe anual INES - ENS

Se ha realizado el informe anual de estado de la seguridad exigido que establece como obligatorio en el ENS. Dicho informe se realiza en la herramienta INES que el CCN-CERT pone a disposición de las organizaciones para cumplir con dicho requisito.

El informe arroja los siguientes indicadores que suponen una leve mejora sobre los de años anteriores. Los niveles para los sistemas MEDIOS son:

- Indicador del cumplimiento del ENS 32.31 %.
- Indicador de mejora continua 67.69 %.

No aparecen datos referidos a 2024 sobre nivel de madurez y organización de la seguridad, ya que el nuevo cuadro de mando no los facilita si no se alcanza un nivel de cumplimiento de más del 90% (actualmente somos capaces de cumplimentar el 87,8%).

Se genera la siguiente documentación:

- Informe ejecutivo del Informe INES.
- Informe con el contenido detallado del contenido del informe.

Metared, informe IMC 2024

MetaRed es un proyecto colaborativo que conforma una red de redes de responsables de Tecnologías de la Información y la Comunicación (TICs) de IES Iberoamericanas, tanto públicas como privadas, con el objetivo de compartir mejores prácticas, casos de éxito y realizar desarrollos tecnológicos colaborativos.

En un mundo cada vez más interconectado y dependiente de la tecnología digital, la ciberseguridad se ha convertido en una preocupación central para todas las instituciones, incluidas las universidades.

En este marco, el proyecto del Índice de Madurez en Ciberseguridad de las Universidades e Instituciones de Educación Superior (IES) Iberoamericanas (IMC 2024) surge como una iniciativa crucial para abordar esta preocupación. Este índice no solo busca evaluar el estado actual de la ciberseguridad en las universidades e IES de la región, sino también establecer un marco de referencia para mejorar y fortalecer sus capacidades en este ámbito esencial. Al ofrecer una visión detallada y específica del nivel de madurez en ciberseguridad de

estas instituciones y habilitar la comparación con entidades de similar naturaleza, el proyecto aspira a ser una herramienta valiosa para la toma de decisiones estratégicas y la asignación de recursos en la lucha contra las amenazas cibernéticas.

La Universidad Pablo de Olavide ha participado en esta iniciativa tal y como se comentó en la memoria anterior. En noviembre de 2024 se han presentado los informes de resultados de los datos recogidos de 247 organizaciones de 10 países. Se han facilitado un informe general y un informe específico a las organizaciones participantes:

- MC - Metared_UPO.pdf
- IMC_2024.pdf

El IMC Iberoamericano global, calculado según el promedio de todas las IES participantes de los diferentes países, es 1.37, lo que sitúa al sector de la educación superior iberoamericana en un nivel de madurez básico (L1), de los cuatro niveles de madurez disponibles (L0, L1, L2 y L3). En España el IMC se sitúa en 1,73. La Universidad Pablo de Olavide obtiene un IMC particular de 1,22, por debajo de la media conjunta y la media por país. Se observa una valoración especialmente baja, 0.78 en el subdominio de valoración relacionado con la identidad. La identificación de todos los activos, de los procedimientos y los actores que intervienen que forman parte de los sistemas de información.

En el siguiente ejercicio se va a repetir la participación cumplimentando de nuevo los cuestionarios de recogida de información.

Cámara de Cuentas

Ejerciendo el derecho de abordar temas transversales en los que encuentren interés relevante, en este ejercicio la Cámara de Cuentas ha incluido en su auditoría aspectos relacionados con la Ciberseguridad y el cumplimiento normativo. Ha solicitado que se cumplimenten una serie de cuestiones, principalmente relacionadas con el aspecto de gobernanza de la ciberseguridad y las medidas obligatorias contempladas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)

Las cuestiones están muy relacionadas con los aspectos recogidos en el modelo de política de seguridad de la información, recogido en el perfil de cumplimiento específico del ENS para universidades.

En este sentido, la Universidad posee una Política de Seguridad de la Información alineada con el ENS pero anterior a la publicación de las modificaciones en 2022 del ENS y de la publicación del perfil de cumplimiento específico. Se pone de manifiesto que, si bien cumplimos con la medida, se requiere una actualización de dicha política que incluya las novedades normativas y se adecue al perfil de cumplimiento en la medida en que la valoración de nuestros sistemas y la naturaleza de nuestras actividades así lo exijan.

En la reunión mantenida en junio de 2025 con los/as auditores/as de la Cámara de Cuentas, se informa que el cumplimiento de los datos es correcto, pero que se va a requerir algo más de información acerca de la causa de aquellos aspectos de gobernanza que no cumplimos. En cualquier caso, al no tratarse de una auditoría de seguridad, las recomendaciones que puedan derivarse en ningún caso supondrán una salvedad en el informe de auditoría de la Cámara de Cuentas.

Auditoria ENS

Impulsado por la atención prestada por la Cámara de Cuentas al estado de algunos aspectos de seguridad en las Universidades, se ha aprobado la iniciativa de una auditoría para conocer el estado de la seguridad respecto a la madurez del sistema y al cumplimiento normativos. No se trata de una auditoría de certificación sino de un GAP, una auditoría que permita conocer la situación actual en relación con la situación deseada, los riesgos más críticos y una propuesta de plan de seguridad que permita la mitigación de estos riesgos.

La auditoría la está llevando a cabo la empresa S2 grupo y está finalizando la fase de entrevistas para conocer el funcionamiento y organización de la seguridad. En los siguientes meses se espera obtener el informe, los indicadores y el plan de mejora de la seguridad.

Contratación a proveedores

Detectado como oportunidad de mejora y vinculado a un compromiso de desempeño del área, se ha puesto en marcha un grupo de trabajo en relación a los requisitos exigibles a los proveedores en diferentes materias. Entre estas materias está la seguridad de la información. Como resultado de este trabajo se han elaborado dos informes, uno que recopila los requisitos exigidos por la normativa vigente y otro con ejemplos de implementación de estos requisitos.

- INF_CIC-16_ENS_contratacion_requisitos_seguridad_v.1.0.docx → Especificación de requisitos de seguridad obligatorios por ley a la hora de contratar productos TIC.
- INF_CIC-16_ENS_contratacion_clausulas.v.2.0.docx → Ejemplo de clausulado clasificado según requisitos legal.

Se ha encontrado dificultad en procedimentar qué requisitos y cómo deben exigirse en cada contrato, ya que depende la criticidad del sistema, la naturaleza del contrato y las condiciones de contratación.

Otras mejoras

- Automatización de copias de seguridad offline
- Actualización del sistema SSO para incluir 2FA

SERVICIO DE APLICACIONES Y SISTEMAS

Administración Electrónica

La sociedad contemporánea es muy dinámica y evoluciona a un ritmo exponencial, dirigiendo incesantemente nuevos requerimientos a las Administraciones Públicas, y más en concreto, a las Universidades, propiciando nuevas fórmulas de generar, gestionar y transmitir el conocimiento, la cultura y el saber. En consecuencia, la Universidad Pablo de Olavide debe asimismo evolucionar continuamente y adaptar sus normas y medios de actuación para adaptarse a los avances sociales, y aún más, convertirse en impulsoras del cambio y la innovación. Debe emplear las tecnologías de la información y las comunicaciones (TIC) como soporte del entorno de enseñanza-aprendizaje y de las relaciones con su personal usuario directo (Personal Docente e Investigador, Estudiantes y Personal Técnico, de Gestión y de Administración y Servicios) y con la sociedad en general.

Una de las demandas que con mayor intensidad viene dirigiendo la ciudadanía a la Universidad es la simplificación de los procedimientos administrativos. La ciudadanía percibe en la regulación excesivas cargas administrativas, que lastran tanto la actividad económica como el ejercicio de los derechos. En paralelo, la administración electrónica se constata como otro de los instrumentos básicos de simplificación administrativa, en la medida que su adecuada implementación representa un importante ahorro de costes y un motor para el desarrollo.

Las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, representan un enérgico respaldo a las medidas de simplificación administrativa y a la generalización de la administración electrónica, hasta el punto de que constituyen los dos ejes sobre los que se articulan sus principales novedades.

Administración Electrónica

En este curso académico se ha seguido con la renovación de la infraestructura de administración electrónica de la Universidad que comenzó el curso académico anterior, ya que la que se había venido usando desde hace más de diez años se había quedado obsoleta en cuanto a temas de accesibilidad, seguridad y tenía problemas de actualización e integración con otros sistemas.

Se describen a continuación las distintas infraestructuras y aplicaciones que dan soporte a las plataformas de Administración Electrónica que se han seguido manteniendo y las nuevas que se han implementado durante este curso académico.

Sede electrónica

La nueva Sede Electrónica de la Universidad Pablo de Olavide ha estado disponible desde el 2 de abril de 2024 en la dirección web https://sede.upo.es. La creación de la misma fue publicada en el BOJA nº 57 de 21 de marzo de 2024, que recogía la “Resolución Rectoral de 15 de marzo de 2024, por la que se suprime la actual Sede Electrónica y crea la nueva Sede Electrónica de la Universidad Pablo de Olavide, de Sevilla”.

La Sede Electrónica es accesible a través de la página web institucional de la Universidad (www.upo.es), que constituye el punto de acceso general electrónico de la misma. El ámbito de aplicación de la Sede Electrónica de la Universidad Pablo de Olavide, de Sevilla, será el de todos sus órganos y en todas las actuaciones y trámites referidos a procedimientos o a servicios que requieran la identificación de la Universidad como Administración Pública y, en su caso, la identificación o firma electrónica de las personas interesadas, tanto miembros de la comunidad universitaria como el resto de la ciudadanía que se relacione con ésta, así como aquellos otros respecto a los que se decida su inclusión en la Sede por razones de eficacia y calidad en la prestación de servicios.

Se acaba de renovar el certificado de la Sede emitido por la autoridad de certificación GEANT Vereniging, vigente hasta abril de 2026. GEANT es un prestador reconocido para la emisión de certificados digitales de sede electrónica que cumple con las exigencias marcadas en el Artículo 18 del Real Decreto 1671/2009 y han sido desarrollados en base a los perfiles propuestos por el grupo de Autenticación y Firma del Consejo Superior de Administración electrónica y el Esquema Nacional de Seguridad.

Dicho prestador se encuentra instalado por defecto en los navegadores de uso habitual, por lo que no es necesario por parte de la persona que accede a la Sede configurar que se confía en los certificados expedidos por éste.

La Sede Electrónica da cobertura a los requisitos legales requeridos desde el Esquema Nacional de Interoperabilidad (ENI) y Esquema Nacional de Seguridad (ENS).

Antigua oficina virtual (Solicit@)

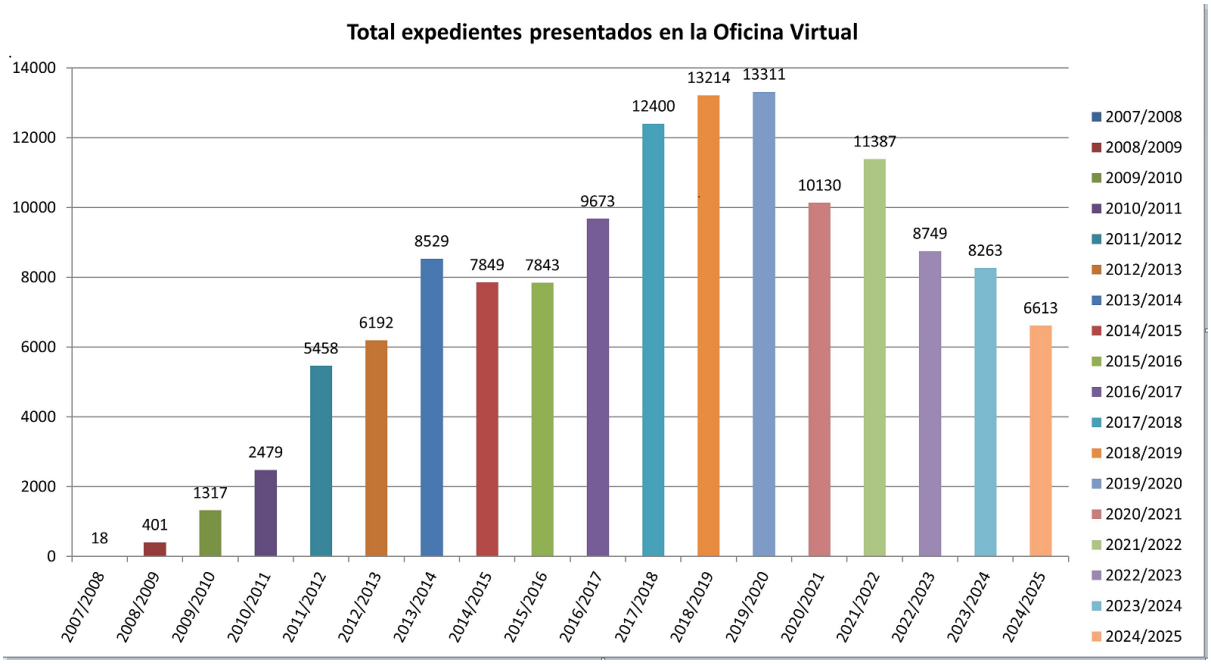
Este es el aplicativo de presentación de solicitudes telemáticas que se ha venido utilizando desde que se comenzó a implantar la Administración Electrónica en la Universidad. El sistema está basado en la aplicación Solicit@, cuyo módulo principal es la Oficina Virtual. Desde este portal web la ciudadanía realiza la cumplimentación, firma y presentación telemática de los trámites publicados por la Universidad. Cada vez son menos los trámites que se inician por esta vía, ya que se está trabajando activamente en migrarlos a la nueva Sede Electrónica. Los trámites que quedan aún por migrar son:

- Solicitud de Comisiones de Servicio PTGAS.
- Solicitud de Comisiones de Servicio PDI.
- Solicitud de Comisiones de Servicio Personal Apoyo a la Investigación.
- Solicitud de Licencias a efectos de Docencia e Investigación.
- Solicitud Título Universitario Oficial de Graduado-a.

Se espera que durante 2025 o principios del 2026 se pueda suprimir este aplicativo definitivamente, dando así respuesta a una demanda de toda la comunidad universitaria, ya que presenta muchos inconvenientes técnicos en su acceso (es una plataforma que se ha quedado obsoleta y de la que no hay mantenimiento oficial).

Trámites presentados a través de la Oficina Virtual Antigua

Evolución por curso académico de las solicitudes con presentadas en la Oficina Virtual antigua:

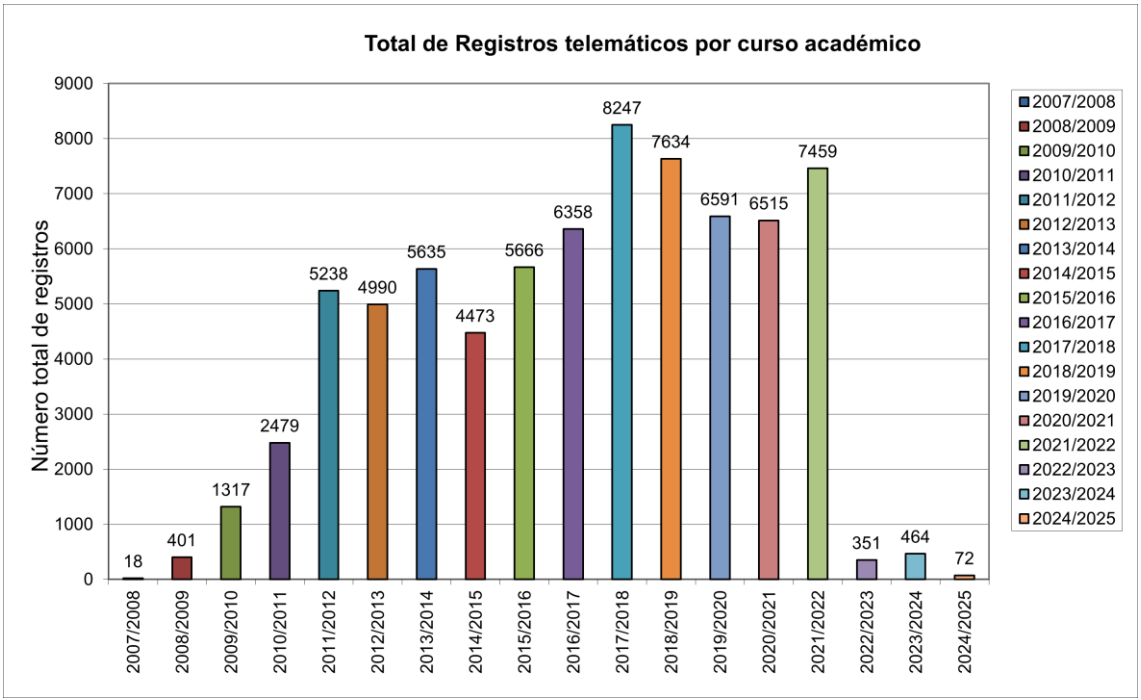


Se continúa con la tendencia descendente en las solicitudes presentadas durante este último curso académico a través de la Oficina Virtual antigua. Esto se debe al proceso de migración de los procedimientos electrónicos existentes a la nueva plataforma de administración electrónica o a aplicativos específicamente diseñados.

Durante este curso 2024-25 se han migrado procedimientos como:

- Solicitud de Acuerdos de Colaboración.
- Solicitud de Certificado Académico Personal.
- Solicitud de Publicación en el Tablón Electrónico Oficial (se ha creado aplicativo propio).
- Solicitud de Reconocimiento de Créditos (se ha creado aplicativo propio).

Evolución por curso académico de solicitudes presentadas a través de la Oficina Virtual antigua con registro telemático:



El único procedimiento que queda vigente aún en la Oficina Virtual antigua y que tiene registro telemático es la Solicitud de Licencias a Efecto de Docencia e Investigación, de ahí el bajo número de solicitudes que se ve en el gráfico anterior.

@Firma

En la Universidad Pablo de Olavide se dispone de servicio de autenticación y firma propio, instalado y administrado sobre hardware de la UPO. Este servicio se viene proporcionando a través del aplicativo @FIRMA, desde el año 2007. @FIRMA es la plataforma corporativa de la Junta de Andalucía para autenticación y firma electrónica es de libre uso y se distribuye para cualquier Consejería, Organismo de la Junta de Andalucía o Administración pública que lo solicite.

Gracias a @FIRMA, las aplicaciones que la utilicen pueden incorporar procesos de autenticación y firma digital mediante el uso de certificados digitales, independientemente del entorno de desarrollo en que hayan sido programadas.

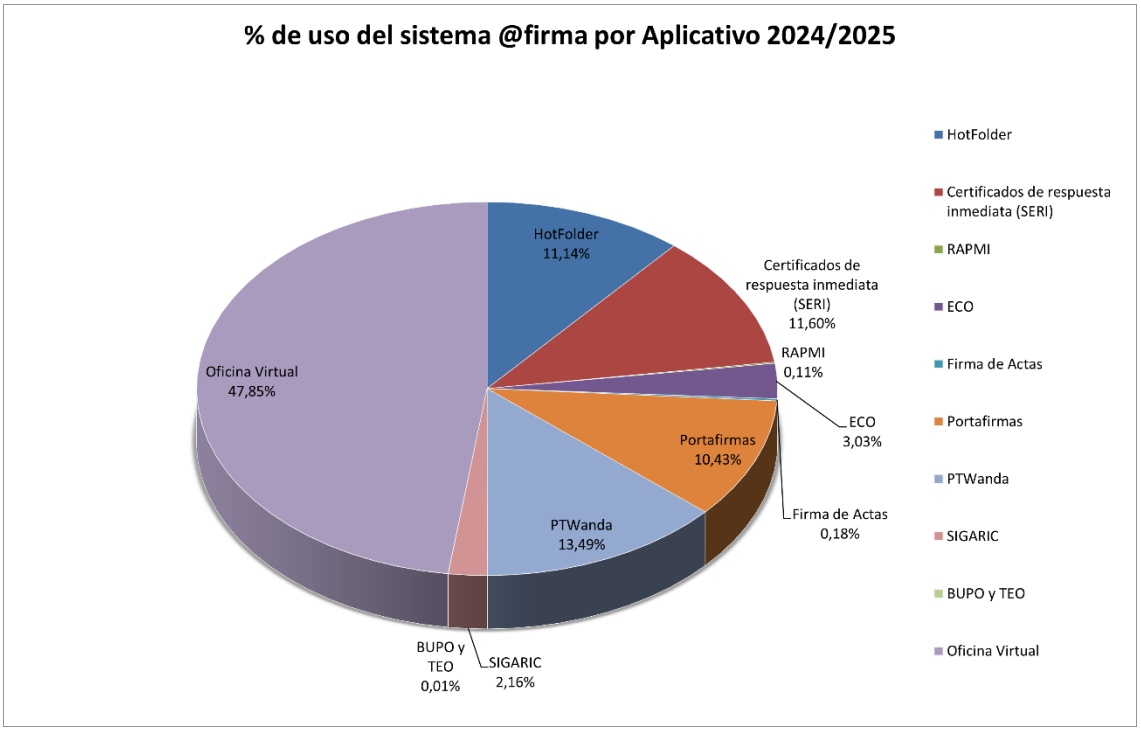
@FIRMA está sujeta a continuas actualizaciones de la "Política de validación", que consiste en una serie de criterios configurados en una implantación de @firma que permiten validar certificados y mapear sus atributos, por parte de la Junta de Andalucía, las cuales se distribuyen a los distintos organismos que tienen una instalación propia de este aplicativo. Periódicamente es necesario actualizar en nuestra implantación.

Funcionalidades relacionadas con las políticas de validación de certificados en @firma:

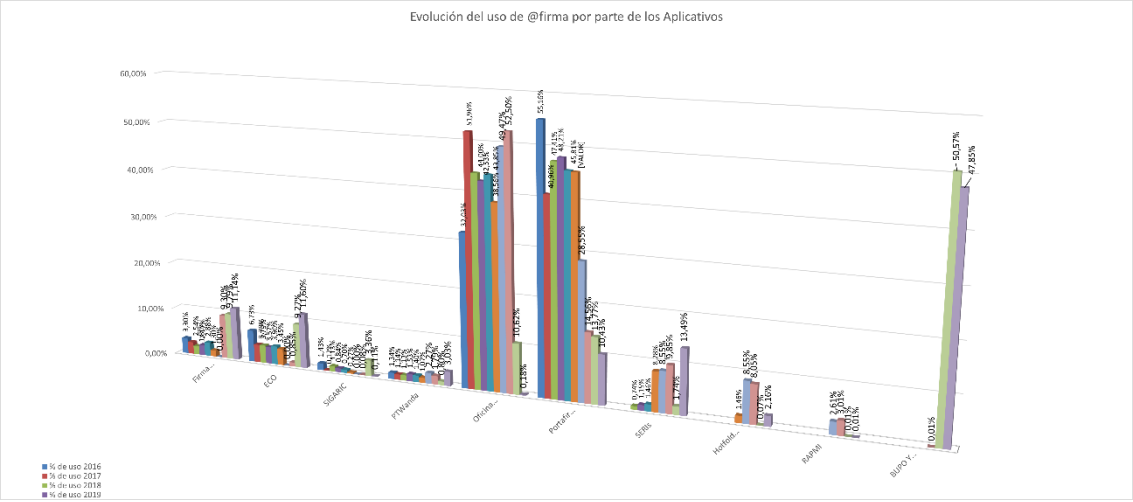
- Autenticación: Proceso que permite autenticar o identificar de forma fehaciente a una entidad basándose en la comprobación de su certificado digital.

- Validación de firmas: Proceso que permite determinar si una firma es válida o no. Se comprueba tanto la validez de la firma (formato y atributos) como la validez de los certificados contenidos en el momento de la firma (si hay referencia temporal) o en el momento de la validación (si no hay referencia temporal).
- Validación de certificados: Proceso que permite determinar si un certificado es válido (en estado no caducado ni revocado ni suspendido). Requiere el tratamiento de los datos contenidos en el certificado y su presentación a las aplicaciones de forma homogénea.

En el siguiente gráfico se muestra el uso del sistema @firma por aplicativo:



En el anterior gráfico podemos ver que las aplicaciones a través de las cuales se realizan mayor cantidad de interacciones con la plataforma de @firma son la Oficina Virtual antigua y la emisión de Certificados de Respuesta Inmediata (SERIs).
Desde la entrada en funcionamiento del nuevo Portafirmas versión 3, estas interacciones se realizan directamente con la plataforma de firma del Ministerio y no están contabilizadas aquí.



Portafirmas

La aplicación Portafirmas es una herramienta destinada a facilitar a sus usuarios el uso de la firma electrónica reconocida en documentos procedentes de distintos sistemas de información, con el objetivo de agilizar la actividad administrativa y disminuir el soporte papel. Realiza las funciones de autenticación, firma de documentos, seguimiento de las firmas realizadas y verificación de estas. Dicho sistema se puso en marcha el 21 de Octubre de 2008 a partir de la publicación en el BOJA núm.. 209, del 21 de octubre de 2008, de la Resolución Rectoral de 26 de septiembre de 2008, de la Universidad Pablo de Olavide, de Sevilla.

Para poder acceder es necesario cumplir los requisitos especificados en la Instrucción v/2014 de la Secretaría General sobre el uso del Portafirmas en la Universidad pablo de Olavide.

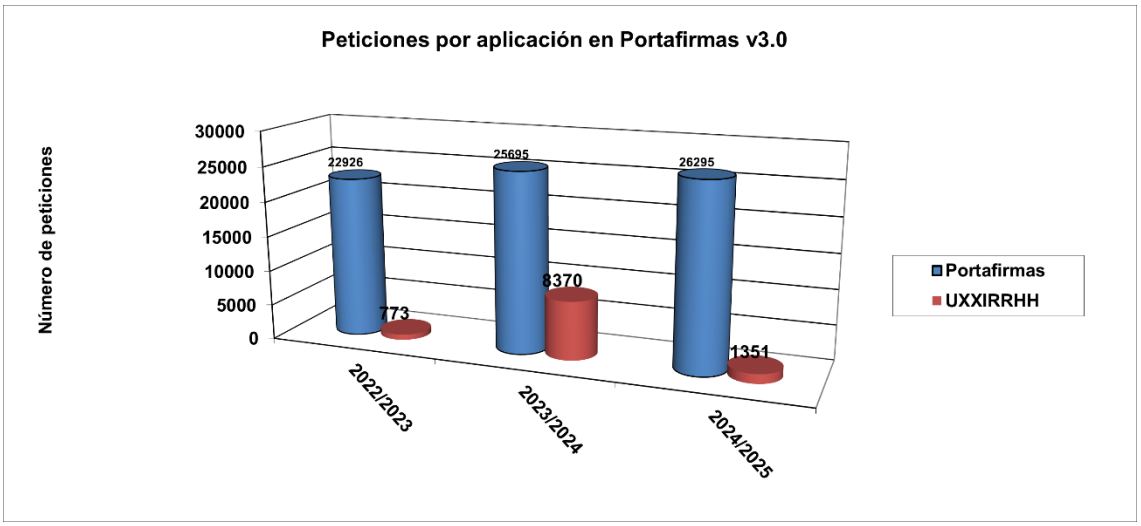
El 24 de febrero de 2022 se puso en marcha la versión 3.5.2.2 de este aplicativo, que, entre otras cosas, llevaba como mejora que la autenticación y firma se hace a través de la herramienta Autofirma, aplicación de firma electrónica desarrollada por el Ministerio de Asuntos Económicos y Transformación Digital que accede a la plataforma de firma del Ministerio.

En diciembre de 2024 se realizó la actualización de la versión 3.5.2.2 a la 3.7.5, que incluía correcciones y mejoras sobre todo en la gestión del personal usuario, en la gestión de firmantes invitados y en la seguridad.

Aparte del uso que actualmente tiene como aplicativo de firma digital de documentos, está siendo utilizada por:

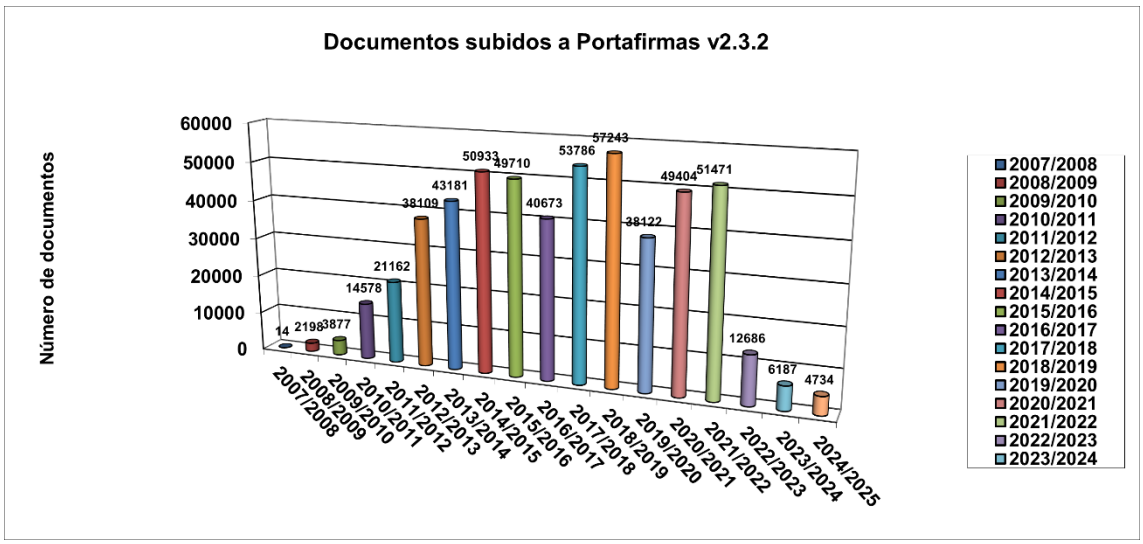
- El aplicativo Anot@ RCP (Registro Central de Personal), que ya está implantado en la Universidad.
- La plataforma de tramitación G-ONCE, que empezó a funcionar el 2 de abril de 2024 con los procedimientos de Instancia Genérica y Solicitud de Copias Electrónicas Auténticas y que ha seguido implementando procedimientos durante el cuso académico 2024-25. La firma de los documentos generados durante la tramitación de las solicitudes de estos procedimientos se lleva a cabo a través del aplicativo Portafirmas v3.7.5

En el siguiente gráfico se puede ver el número de peticiones enviadas a Portafirmas v3.7.5 por tipo de aplicación (Portafirmas v3.7.5 engloba tanto las peticiones enviadas desde la plataforma G-ONCE como las realizadas desde la propia aplicación Portafirmas):

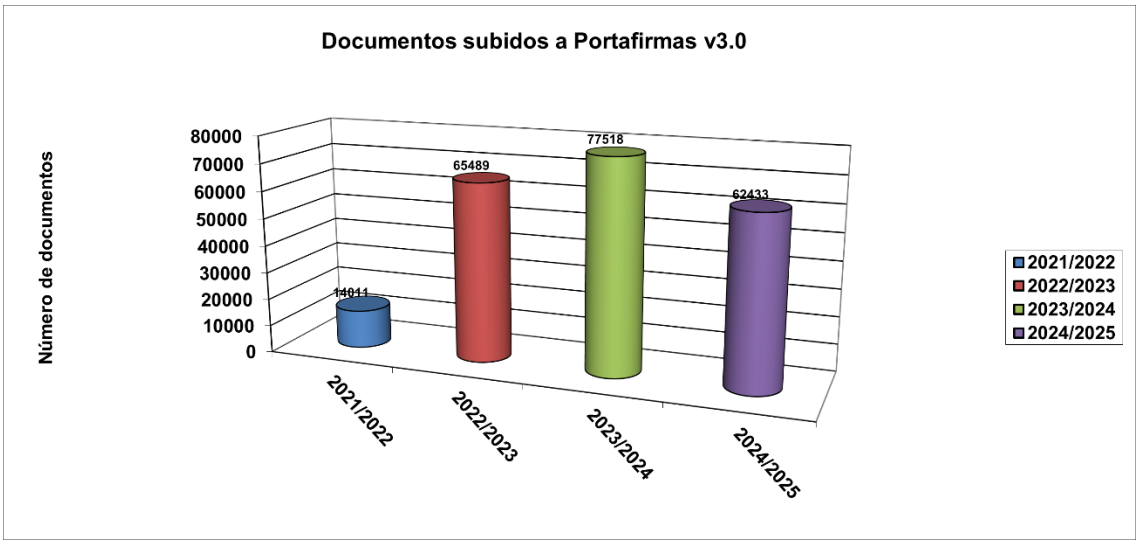


El antiguo Portafirmas v2.3.2 se ha utilizado durante este curso académico solo para firma de documentos enviados a través de la aplicación eCO (Comunicaciones Interiores) y la antigua plataforma de tramitación, pero se está en trámites de su eliminación definitiva. De hecho, el aplicativo eCO fue sustituida en julio de 2024 por un procedimiento interno integrado en la plataforma de tramitación G-TM.

En el gráfico podemos ver cómo se sigue reduciendo el número total de documentos subidos a Portafirmas v.2.3.2:



Y la evolución del número total de documentos subidos a Portafimas v.3.7.5 desde su entrada en producción el 24 de febrero de 2022.



Antigua plataforma de tramitación de expedientes administrativos (PTW@nda)

La plataforma de tramitación de expedientes administrativos, que se ha venido usando en la Universidad desde el año 2009, está basada en el aplicativo PTW@nda de la Junta de Andalucía y a su vez se basa en el motor de tramitación Trew@. Es usada por las diferentes áreas de la Universidad para llevar a cabo la tramitación electrónica de distintos procedimientos, mediante la cumplimentación de tareas y fases y la elaboración de documentos. Estos procedimientos son:

- Solicitud de Comisiones de Servicio del PTGAS, PDI y Personal Investigador.
- Solicitud de Título Oficial de Graduado/a.
- Solicitud de Licencias a Efectos de Docencia e Investigación.
- Solicitud de Publicación en BUPO.

Actualmente todos estos procedimientos están siendo analizados y rediseñados por las distintas áreas con objeto de su racionalización y simplificación y su migración a la nueva plataforma de tramitación de expedientes administrativos, G-TM, que es un módulo dentro de la suite G-ONCE. Cuando estas actuaciones hayan finalizado, PTW@nda desaparecerá.

De hecho, en este período se han migrado los siguientes trámites:

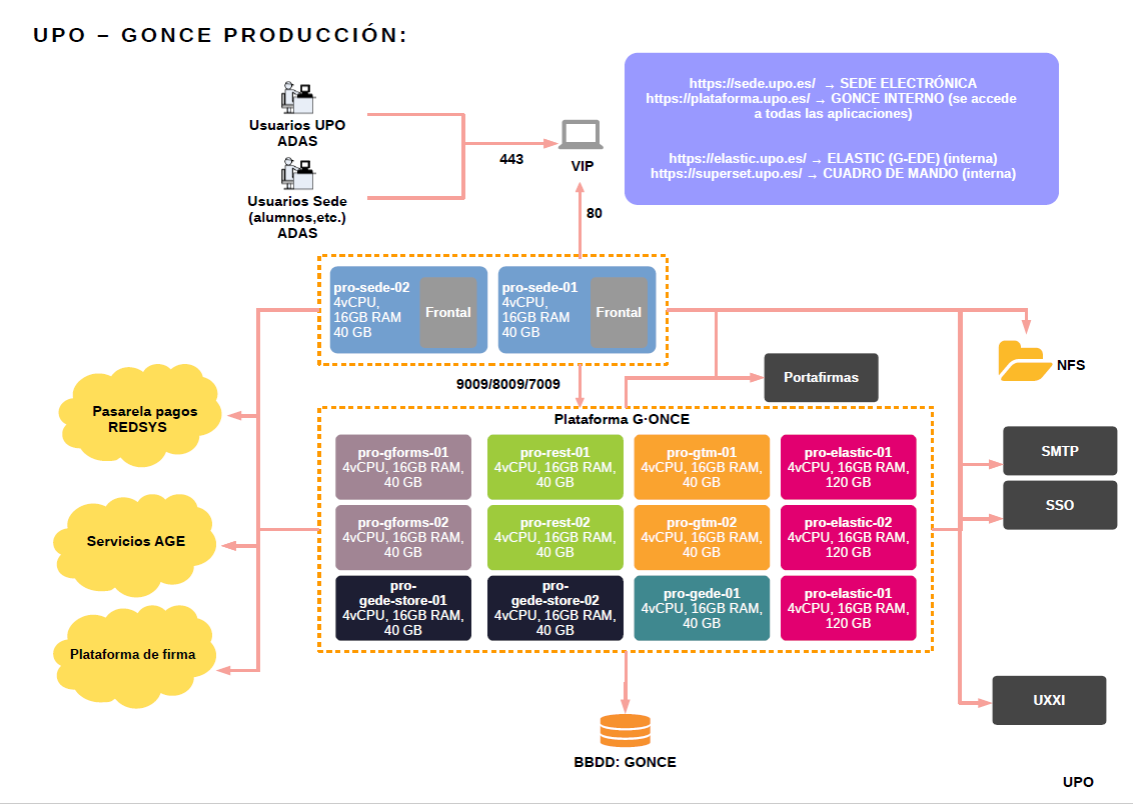
- Solicitud de Traslado de Expediente (se ha creado aplicativo propio).
- Solicitud de Reconocimiento de Créditos ((se ha creado aplicativo propio).
- Solicitud de Acuerdos de Colaboración.
- Solicitud de Certificado Académico Personal.
- Solicitud de Publicación en el Tablón Electrónico Oficial (se ha creado aplicativo propio).

Suite G-ONCE

G-ONCE es una solución única e integrada para que los organismos públicos puedan adecuarse a los requisitos que imponen 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. Se ha licitado y contratado dentro del marco de un proyecto interuniversitario del cual la Universidad Pablo de Olavide forma parte.

Es un conjunto de módulos y aplicativos a través de los cuales se pretende dar respuesta a todo lo que la Universidad Pablo de Olavide necesita en materia de administración electrónica: presentación de solicitudes telemáticas, tramitación de expedientes de forma electrónica, servicio de archivo electrónico, notificaciones fehacientes, etc.

Para dar soporte a todo esto se crearon dos entornos, tanto de pruebas como de producción, con multitud de servidores e instalaciones, como se puede ver en la imagen adjunta.



De todos los componentes que conforman la plataforma de administración electrónica G-ONCE, en la UPO se implementaron los siguientes:

- Portal de la ciudadanía:
  - Sede Electrónica /Oficina Virtual.
  - Gestión de notificaciones.
  - Portafirmas.
  - Verificador de firmas.
  - Tablón Electrónico Oficial.

- Portal de personal empleado público
  - Motor de tramitación (G-TM).
  - Gestor documental y archivo definitivo (G-EDE).
  - Administración (G-Settings).
  - Definición de procedimientos (Model@).
  - Generador de formularios (G-Forms).
  - Cuadro de mandos

- Interoperabilidad e integraciones:
  - AGE.
  - GEISER .
  - Notific@.
  - Plataforma de Intermediación de Datos (PID).
  - Identidad corporativa: ADAS.
  - Pasarela de pagos: Redsys.
  - Plataforma de correo electrónico.
  - Componentes ERP: UXXI.
  - Portafirmas v3.
  - Sistema de Información Administrativa (SIA).

Actualmente se encuentran operativos 13 procedimientos cuya tramitación se realiza completamente a través del motor de tramitación G-TM, mas 23 procedimientos de actuación administrativa automatizada (AAA) o servicios de respuesta inmediata (SERIs).

- Procedimientos con tramitación completa en G-TM:
  - Ayudas de Acción Social.
  - Anulación de Matricula.
  - Aportación de Documentación para la Matrícula.
  - Certificado Académico Personal.
  - Copias Electrónicas Auténticas.
  - Acuerdos de Colaboración.
  - Comunicaciones Internas.
  - Recursos Administrativos.
  - Instancia Genérica.
  - Procedimiento Administrativo Común.
  - Reconocimiento de Servicios Previos.
  - Permisos y licencias para PDI.
  - Permisos y Licencias de Personal Investigador.

  De estos 13 procedimientos, 11 han sido puestos en funcionamiento durante el curso 2024-25.

- Procedimientos de actuación administrativa automatizada (AAA)
  - Certificado de Asignaturas/Conceptos Matriculados Doctorado.
  - Certificado Asignaturas Matriculadas Título Propio.
  - Certificado Asignaturas Matriculadas en Grado.
  - Certificado Asignaturas Matriculadas en Máster.
  - Informe de aprovechamiento curso "Comp.Dig.Grado".
  - Informe de aprovechamiento curso "Comp.Dig.Máster".
  - Informe de Colaboración en el Curso Competencia Digital Grado.

- Informe Uso de la Plataforma de Aula Virtual.
- Certificado de desempeño de la actividad docente.
- Certificación Supletoria Provisional Título Máster Oficial.
- Certificación Supletoria Provisional Título Grado.
- Certificado de Dirección de Tesis Doctorales Curso Actual.
- Certificado de Dirección de Tesis Doctorales Defendidas.
- Certificado de Dirección de Proyectos de Tesis No Defendidas.
- Certificado Tutorización/Co-Tutorización TFM.
- Certificado de Curso de Formación Doctoral.
- Certificado Horario y Lugar de Trabajo PDI.
- Certificados Méritos Docentes (Quinquenios).
- Certificado Méritos Investigación (Sexenios).
- Certificado Horario Trabajo PTGAS.
- Certificado Lugar de Trabajo PTGAS.
- Acreditación abono derechos al Título Grado.
- Certificado de Docencia.

De estos 23 procedimientos, 4 han sido puestos en funcionamiento durante el curso académico 2024-25.

Registro de funcionarios habilitados (RFH) y oficina de asistencia en materia de registro (OAMR)

La Orden HAP/7/2014, de 8 de enero, del Registro de Personal funcionario Habilitado (RFH) para la identificación y autenticación de la ciudadanía, en el ámbito de la Administración General del Estado y sus Organismos públicos vinculados o dependientes, estableció por primera vez la regulación de un registro del personal funcionario que pudieran asistir a las personas interesadas en la realización de determinados trámites electrónicos de identificación y autenticación en su nombre.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge y amplía esta figura. Se establece en su artículo 12 que cuando las personas interesadas, que no estén obligadas a relacionarse electrónicamente con las Administraciones Públicas, no dispongan de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por el personal funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello.

A estos efectos, se prevé que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantengan actualizado un registro u otro sistema equivalente, donde constará el personal funcionario habilitado para la identificación o firma y en el que se incluirán, al menos, aquellos que presten servicios en las Oficinas de Asistencia en Materia de Registros.

En la Orden PCM/1383/2021, de 9 de diciembre, es en la que se regula actualmente el RFH en el ámbito de la Administración General del Estado, sus Organismos Públicos y Entidades de Derecho Público.

Existe una oficina de asistencia en materia de registro (OAMR) ubicada en el Edificio 18, despacho 18.B.06, donde la ciudadanía encontrará a su disposición los equipos informáticos preparados para la presentación de trámites electrónicos relacionados con la Universidad en caso de no disponer de medios adecuados.

La persona interesada, previa acreditación de su identidad, deberá dar su consentimiento expreso para su identificación o firma por el personal funcionario habilitado para cada actuación administrativa que la requiera.

La relación actualizada de personal funcionario designados por la Universidad Pablo de Olavide para identificar y autenticar a personas físicas que no dispongan de mecanismos de identificación y autenticación para actuar electrónicamente ante su Sede Electrónica se encuentra publicado en el siguiente enlace:

Personal funcionario habilitado

También se dispone en dicho enlace de la relación del personal funcionario habilitado por la Universidad Pablo de Olavide para la expedición de copias auténticas electrónicas.

DIR3

El Directorio Común proporciona un Inventario unificado y común a toda la Administración de las unidades orgánicas / organismos públicos, sus oficinas asociadas y unidades de gestión económica - presupuestaria, facilitando el mantenimiento distribuido y corresponsable de la información. Se concibe como un inventario de información sobre la estructura orgánica de la Administración Pública, y sus oficinas de atención ciudadana. Es decir, es un catálogo de las unidades orgánicas, organismos públicos, y oficinas de registro y atención al ciudadano de la Administración. Queda soportado legalmente en el artículo 9 del Real Decreto 4/2010 (Esquema Nacional de Interoperabilidad).

En este sentido, la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica (DGMAPIAE) puso en marcha las medidas adecuadas para, con una capa de servicios, asegurar la adecuada gestión del mismo, garantizando:

El acceso a la información, así como la actualización y mantenimiento de esta, es a través de un sistema de información dedicado donde puede consultarse y actualizarse. Este sistema reside en la DGMAPIAE, que se responsabiliza de su gestión y mantenimiento.

Cada Administración colaboradora será proveedora de los datos de su ámbito de competencias, siendo responsable de su actualización, calidad, y veracidad. Asimismo, podrá consumir todos los datos de las Administraciones restantes, garantizando así los requisitos de interoperabilidad establecidos en el Real Decreto.

La ciudadanía, a través de los portales públicos (por ejemplo, 060), podrán consultar la información del Directorio, de acuerdo con las condiciones que se establezcan con las Administraciones proveedoras.

Durante este tiempo se han llevado a cabo tareas de mantenimiento del catálogo DIR3 de la UPO, adaptando la información mostrada a las nuevas realidades de la Universidad. La versión actual de las Unidades Orgánicas, Oficinas Asociadas y Unidades de Gestión Presupuestaria de la Universidad Pablo de Olavide está vigente desde el **30 de abril de 2025** y se puede consultar en DIR3

GEISER (Gestión Integrada de Servicios de Registro)

GEISER es una solución integral de registro que funciona en modo nube para prestar el servicio para cualquier organismo público, que cubre tanto la gestión de sus oficinas de registro de entrada/salida como la recepción y envío de registros en las unidades tramitadoras destinatarias de la documentación.

El servicio de registro GEISER es la pieza principal del Servicio Compartido de Gestión de Registro.

La aplicación permite la digitalización de la documentación presentada por el ciudadano en las oficinas, y al contar con certificación SICRES 3.0 posibilita el intercambio de registros en formato electrónico con otros organismos conectados a la plataforma SIR.

GEISER quedó completamente operativo en el mes de mayo de 2022 en la UPO, siendo un organismo más conectado a SIR, lo que ha provocado una mejora en cuanto a la facilidad de recepción y envío de documentación con otras Administraciones Públicas.
Durante este curso académico se han contabilizado **13000 asientos** en el libro de registro electrónico de entrada y **2803 asientos** en el libro de registro electrónico de salida.

Despliegue de servicios SCSP (Supresión Certificado Soporte Papel)

El objetivo de este protocolo es la utilización de la transmisión de datos como medio estándar de sustitución de certificados en papel mediante la definición del formato de información tanto requerida como suministrada de manera general, y en la parte correspondiente a cada servicio de manera específica, entre AAPPs para cumplir con la normativa vigente en la que no se puede pedir documentación a los ciudadanos que ya se encuentre en poder de las AAPPs, tal y como se recoge en el artículo 28.2 de la Ley 39/2015, de Procedimiento Administrativo Común.

Ya se está utilizando el Cliente Ligero, que es una herramienta proporcionada por el Portal de Administración Electrónica (PAe) utilizada para consumir servicios SCSP. Para usar el Cliente Ligero no es necesario instalar nada, ya que todo se hace a través de una plataforma web.

Entre los servicios que tenemos actualmente autorizados se encuentran:

- (CCAA) Consulta de los datos de discapacidad
- (CCAA) Consulta de los datos de familia numerosa
- (CRUE) Consulta de datos de matrículas universitarias
- (DGP) Consulta de datos de identidad
- (DGP) Verificación de datos de identidad
- (Educación) Consulta de la condición de becado
- (Educación) Consulta de los datos de un título no universitario
- (Educación) Consulta de los datos de un título universitario
- (Educación) Consulta de títulos no universitarios por datos de filiación
- (Educación) Consulta de títulos no universitarios por documentación
- (Educación) Consulta de títulos universitarios por datos de filiación
- (Educación) Consulta de títulos universitarios por documentación
- (IMSERSO) Consulta del nivel y grado de dependencia
- (INSS) Consulta de las prestaciones del Registro de Prestaciones Sociales Públicas (RPSP), incapacidad temporal y maternidad
- (Justicia) Consulta de inexistencia de delitos sexuales por datos de filiación
- (Justicia) Consulta de inexistencia de delitos sexuales por documentación
- (TGSS) Estar al corriente de pago con la Seguridad Social

También se está empezando a utilizar la opción de Recubrimiento, que es la consulta a través de servicios web normalmente desde dentro de gestores o plataformas de tramitación. La suite G-ONCE ha comenzado a implementarla en aquellos procedimientos que necesitan hacer uso de estos servicios, como la Solicitud de Certificado Académico Personal.

Aplicaciones Corporativas y Sistemas

Portales Web

Los despliegues basados en contenedores, tanto para WordPress como para aplicaciones transversales, siguen ofreciendo buenos resultados. Se ha llevado a cabo una actualización completa de la plataforma orientada a aplicaciones, como paso previo a la futura renovación de la plataforma WordPress.

Asimismo, se está evaluando la idoneidad de trasladar el enfoque de virtualización de aplicaciones a las plataformas basadas en Laravel, con el objetivo de simplificar su despliegue y facilitar el mantenimiento de entornos con dependencias complejas.

Seguimos trabajando con la plataforma de pruebas basada en Kubernetes, que incluye herramientas de despliegue y actualización. Se están probando e incorporando nuevos servicios con la intención de construir una plataforma generalista, fácil de configurar y mantener, capaz de dar soporte a distintas clases de aplicaciones (inicialmente WordPress).

El clúster de UXXI continúa en funcionamiento sin incidencias.

También seguimos retirando algunos de los servidores más antiguos basados en la pila LAMP, como parte del proceso de modernización de la infraestructura web. El proxy corporativo HAProxy continúa operando con normalidad.

En cuanto a los CMS corporativos basados en OpenCms, se continúa con su operación y mantenimiento habitual, sin que se hayan producido incidencias destacables durante el periodo.

Correo electrónico

El sistema de correo electrónico de la Universidad Pablo de Olavide se apoya en soluciones de software libre y ha sido diseñado para responder a las necesidades actuales en materia de usabilidad, capacidad, disponibilidad y seguridad.

Como en cursos anteriores, se han continuado los esfuerzos en la mejora continua y actualización del servicio, con especial atención al ámbito de la seguridad. En este sentido, se han reforzado los protocolos de actuación y se han implantado nuevas medidas destinadas a proteger la plataforma frente a amenazas cada vez más complejas. Cada incidente se considera una oportunidad para revisar, adaptar y robustecer nuestras defensas. Se mantiene el foco en la detección temprana y eficaz de ataques dirigidos a la captura de credenciales, consiguiendo neutralizarlos con rapidez y efectividad. Además, se colabora activamente con el Instituto Nacional de Ciberseguridad (INCIBE) para una mejor gestión y tratamiento de los incidentes de seguridad, así como para la aplicación de medidas de contención adecuadas. Por su parte, el sistema "Lavadora" de RedIRIS, al que la Universidad está adherida, continúa ofreciendo una protección efectiva frente a amenazas y correo no deseado, mediante un filtrado eficiente del correo entrante.

Complementariamente, se sigue trabajando en la generación automática de informes de actividad sospechosa y en la monitorización proactiva del sistema, lo que permite actuar con agilidad ante posibles intentos de suplantación o accesos indebidos.

Durante el presente curso, se ha avanzado significativamente en la renovación integral de la infraestructura del sistema de correo. Se han desplegado nuevas máquinas virtuales con sistemas operativos actualizados y se ha procedido a la reinstalación de todo el software con las versiones más recientes. Tras la renovación de las estafetas de correo externas situadas en la DMZ durante el curso anterior, este año se ha abordado la actualización de las estafetas internas, los servidores proxy POP/IMAP, el servicio de correo web y el servicio de agenda vinculado al correo electrónico. También se ha avanzado en la implementación del nuevo sistema de listas de distribución y en el gestor de buzones.

En paralelo, se ha consolidado la implantación de las firmas DKIM (DomainKeys Identified Mail) y de las políticas DMARC (Domain-based Message Authentication, Reporting and Conformance), lo cual refuerza la autenticidad y fiabilidad del correo saliente y protege a la Universidad frente a intentos de suplantación de identidad.

Finalmente, se ha continuado con la depuración y gestión de cuentas de correo obsoletas o en desuso. Esta acción contribuye a liberar espacio para el resto de usuarios, mejorar el rendimiento general del sistema y reducir los riesgos asociados al uso indebido de cuentas inactivas. Esta gestión eficiente garantiza un entorno más seguro, estable y optimizado para toda la comunidad universitaria.

Gestión de identidades

El Servicio de Gestión de Identidades de la Universidad Pablo de Olavide constituye un componente esencial en la infraestructura tecnológica de la institución, proporcionando múltiples opciones de autenticación para el acceso seguro a los recursos universitarios. Entre los métodos disponibles se incluyen credenciales tradicionales (usuario y contraseña), tarjeta inteligente y DNI electrónico.

Este servicio facilita la entrada al Sistema de Identidad Federado de las Universidades Españolas (SIR), así como a una amplia gama de servicios internos, como el Aula Virtual, la Oficina Virtual, la Firma Automatizada, el Repositorio Seguro, la Formación del Plan Docente, los Laboratorios Virtuales y el Servicio de Biblioteca. Asimismo, actúa como punto de integración con el sistema de Identidad Electrónica para las Administraciones Públicas (Cl@ve), ampliando el acceso a usuarios externos.

Durante el curso 2024–2025, se ha llevado a cabo una renovación integral de la infraestructura de autenticación única (SSO), basada en el sistema adAS. Esta actualización ha incluido:

- La instalación de nuevos servidores con mayor capacidad y sistemas operativos actualizados.
- La adopción de la última versión disponible del software adAS.
- La mejora global del rendimiento, la seguridad y la disponibilidad del servicio.

En paralelo, se continúa con un ambicioso proyecto de modernización del Servicio de Gestión de Identidades. Este plan estratégico tiene como finalidad redefinir y optimizar los procesos actuales de gestión de identidades y accesos, integrándolos en un modelo más robusto, escalable y alineado con las mejores prácticas.

Entre las iniciativas más destacadas se encuentran:

- Implantación futura de adAS User, que permitirá habilitar el acceso mediante doble factor de autenticación (2FA) a todos los servicios integrados con nuestro sistema SSO, fortaleciendo así los mecanismos de seguridad frente a accesos no autorizados.
- Integración del sistema OpenAthens, con el objetivo de ampliar las capacidades de federación de identidades y facilitar el acceso a recursos electrónicos externos mediante credenciales institucionales.
- Actualización y mejora del directorio corporativo, iniciativa que busca reforzar la seguridad, estabilidad y eficiencia del servicio, asegurando un soporte sólido para todos los sistemas dependientes.

Todas estas acciones reafirman el compromiso de la Universidad con una gestión de identidades moderna, segura y centrada en el usuario, que permita ofrecer una experiencia de acceso ágil y fiable a toda la comunidad universitaria.

Infraestructuras Tecnológicas

Durante el último período, se han llevado a cabo importantes avances en la infraestructura tecnológica de nuestra institución, con el objetivo de mejorar la eficiencia, seguridad y disponibilidad de los recursos. A continuación, se detallan las principales actuaciones realizadas en cada área.

Se ha implementado un sistema de almacenamiento moderno y de alto rendimiento, diseñado para garantizar la seguridad y alta disponibilidad de los datos. Este sistema está replicado en múltiples Centros de Procesamiento de Datos (CPD), lo que asegura el acceso continuo incluso en caso de incidencias. Entre sus características destacan:

- Protección avanzada contra ransomware.
- Mayor velocidad y capacidad de respuesta.
- Sustitución e instalación de nuevas cabinas de almacenamiento, culminadas durante este curso.

El entorno de virtualización ha sido objeto de una profunda actualización, tanto en hardware como en software:

- Sustitución de equipos obsoletos por nuevos servidores físicos, mejorando el rendimiento y la flexibilidad del sistema.
- Actualización a las últimas versiones de software compatibles, garantizando un entorno seguro y optimizado.
- Implementación de mejoras derivadas de los estudios realizados el curso anterior, reforzando la robustez y alineación con estándares actuales.

Gracias al análisis exhaustivo realizado previamente, se han aplicado mejoras significativas en el sistema de respaldo:

- Reducción en los tiempos de ejecución de backups.

- Optimización del espacio de almacenamiento utilizado.
- Mejoras en la seguridad y el rendimiento general del servicio.

Migración a un nuevo proveedor de Certificados Digitales, Harica, para garantizar mayor fiabilidad y seguridad.

Actualización de la infraestructura de DNS para mejorar la resolución y disponibilidad de los servicios.

Renovación de la arquitectura del servicio de Proxy, incorporando alta disponibilidad y mejorando su eficiencia.

Aplicaciones Corporativas de Gestión

Además del mantenimiento y evolución relacionados con las aplicaciones corporativas de gestión, se han incorporado las siguientes funcionalidades y/o servicios:

Se han desarrollado nuevos aplicativos cómo:

- Continua el piloto de una nueva aplicación de generación y gestión de horarios de la empresa Bullet: Bullet Calendar y Bullet.
- Se ha implantado la nueva Automatrícula para las Pruebas de Acceso a la Universidad.
- Se implanta un nuevo aplicativo para las Compras con proveedores.
- Se han implantado la automatización de procesos mediante tecnología Automatización Robótica de Procesos (RPA) de seis procesos:
    - Alta Profesorado Externo.
    - Acreditación de Idiomas.
    - Expedición de Hojas de Servicio.
    - Diligencias de Actas.
    - Justificaciones al Auditor.
    - Comunicación de Ingresos.
- Nuevo SERI de Certificación de Actividad Docente del Profesorado.
- Nuevo SERI de Certificado Asignaturas Matriculadas Título Propio.
- Nuevo SERI de Informe de Colaboración en el Curso Competencia Digital Grado.
- Nuevo SERI de Acreditación abono derechos al Título Grado.
- Se pone en marcha la nueva aplicación para la solicitud de publicación en el Tablón Electrónico Oficial.
- Nueva web de Máster.
- Nueva Web de Doctorado.

- Nueva web de SDUPO.
- Nueva web del Vicerrectorado de Deportes.
- Se crea un nuevo aplicativo para la gestión de Censos para los procesos electorales, así como una nueva consulta web personalizada por usuario.
- Nueva aplicación para la Gestión de Traslados de Expedientes y de Reconocimientos de Créditos.
- Nueva aplicación para la Baremación del PDI.
- Nueva aplicación para las Propuestas para el POD.
- Se sustituye el sistema SAGE por una solución basada en Microsoft Access.
- Se implanta la nueva Aplicación Móvil UPO.
- Se implanta la nueva Tarjeta Universitaria Virtual.

Actualizaciones de infraestructura, seguridad y evoluciones en las aplicaciones corporativas siguientes:

- Etempo: actualización de versión, parches de seguridad, actualización de base de datos, evoluciones, mejoras, etc.
- Gescontrata: Se actualiza la aplicación y se cambia una infraestructura virtual.
- Se comienza la actualización de la infraestructura de ODA a la versión 19.24.
- Se ha actualizado los aplicativos desarrollados en versión php 7 a php 8.
- Se está migrando el Buzón IRPF de base de datos Mysql a base de datos Oracle.

Se están desarrollando también los siguientes aplicativos:

- BUPO (Boletín oficial de la Universidad Pablo de Olavide). Sustituirá al anterior procedimiento electrónico, el cual tenía bastantes limitaciones. En fase de pruebas.
- Gestor de convocatorias de investigación. En fase de migración y pruebas.
- Nueva Gestión de Identidades.
- Aplicación de Servicio de Registro de Presencia.
- Nueva aplicación para la obtención de la fotografía de los usuarios/as para la tarjeta universitaria virtual.
- Se inicia la renovación el Acceso Personalizado para la comunidad universitaria.

Aula Virtual

El Aula Virtual es la plataforma de docencia virtual institucional a la que se puede acceder directamente desde https://campusvirtual.upo.es, desde los servicios personales o a través de los enlaces publicados en diferentes ubicaciones de la web de la Universidad.

En el curso académico 2024-25 se ha completado la implantación de la versión de Blackboard Ultra en el Aula Virtual. Esta implantación se ha realizado en dos fases dada la complejidad e impacto tanto técnico como funcional. En 2023 iniciamos la migración de la plataforma a la nueva versión Blackboard Learn Ultra, la cual supuso un salto tecnológico muy significativo en términos de eficiencia, seguridad y navegabilidad. La primera fase se completó el pasado curso y consistió en adoptar la Navegación Ultra, usándose con éxito en el curso 2023-2024. Esto supuso una sensible mejora de la interfaz de usuario de la herramienta, haciéndola más moderna, intuitiva, accesible y compatible con cualquier dispositivo, pero se mantuvieron los espacios virtuales con la misma organización. La segunda fase ha consistido en la adopción de los cursos en versión Ultra para todos los espacios virtuales del curso académico 2024-2025. Esta actualización de Blackboard ha supuesto un cambio sustancial respecto a la versión anterior, ya que no sólo cambia el aspecto gráfico de la herramienta, sino que implica una transformación completa de la organización de los cursos.

Para minimizar el impacto de este cambio se diseñó un Plan de Adopción para el PDI, que incluyó:

- Vídeos tutoriales del uso de los nuevos cursos, alojados en https://www.upo.es/docencia-virtual/aula-virtual/version-ultra/cursos-ultra
- Seminarios abiertos online síncronos diarios durante todo el mes de julio y septiembre, donde además de explicar cómo realizar la migración de contenido entre las dos versiones, se podía interactuar y resolver dudas sobre la nueva versión. Se realizaron un total de 60 seminarios.
- Jornadas de puertas abiertas un día a la semana, mañana y tarde, durante el mes de septiembre, realizándose un total de 8 sesiones.
- Asistencia personal presencial en días/horas concretas.

Enmarcado en el proyecto Unidigital de Docencia Híbrida CRUE-RedIRIS, el cual amplía las capacidades pedagógicas, promueve la interactividad y optimiza la gestión de recursos multimedia para enriquecer la experiencia de aprendizaje en entornos virtuales, se ha realizado la integración de la herramienta Genially en el Aula Virtual y se ha proporcionado licencia premium a los docentes que lo han solicitado. Genially es una herramienta que permite generar contenidos digitales interactivos sin necesidad de programar y sin tener conocimientos de diseño.

Al igual que en años anteriores, se han realizado labores propias de soporte y seguimiento en cuanto a la atención (personal, telefónica, etc.) a los/as usuarios/as y sus a correspondientes solicitudes de servicio.

Para la docencia del curso académico 2024-25, se crearon de oficio 2418 espacios virtuales correspondientes a los estudios de Grado, Máster y programas de Doctorado. A petición del CUI se han creado 150 espacios virtuales para el apoyo a la formación de los alumnos internacionales. Del mismo modo se han creado los espacios virtuales para la actividad docente de los cursos de Formación Permanente, formación de Doctorado y para el área de Formación e Innovación, todos ellos suman un total de 142. A diario se ha realizado un mantenimiento y actualización del acceso de docentes y estudiantes a estos espacios virtuales.

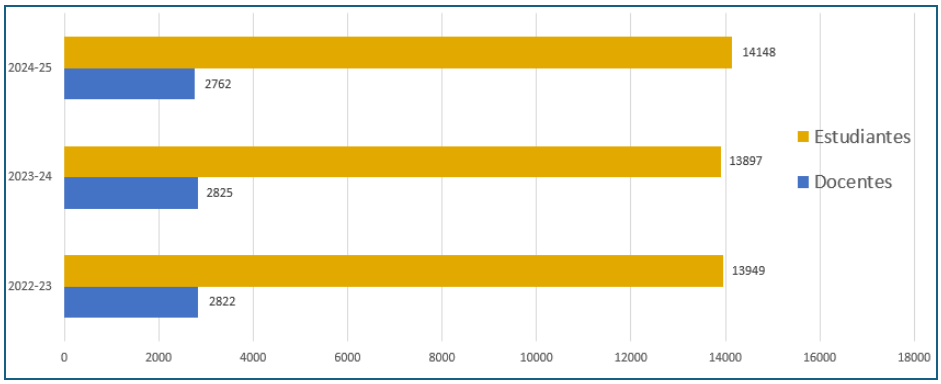
Se han eliminado del Aula Virtual los espacios virtuales del curso 2023-24, así como los usuarios sin espacios virtuales asignados: con ello se mejora el tiempo de respuesta de la plataforma, se minimiza el espacio de almacenamiento y se reducen los costes de mantenimiento.

Se ha proporcionado usuario supervisor de Collaborate, así como la formación y manuales creados especialmente para este acometido, a las áreas/unidades en las que se ha justificado la necesidad de crear y gestionar salas para la realización de reuniones, seminarios, jornadas, etc. También se han creado y configurado las salas virtuales de Collaborate que estaban fuera del alcance de las áreas/unidades con acceso administrador.

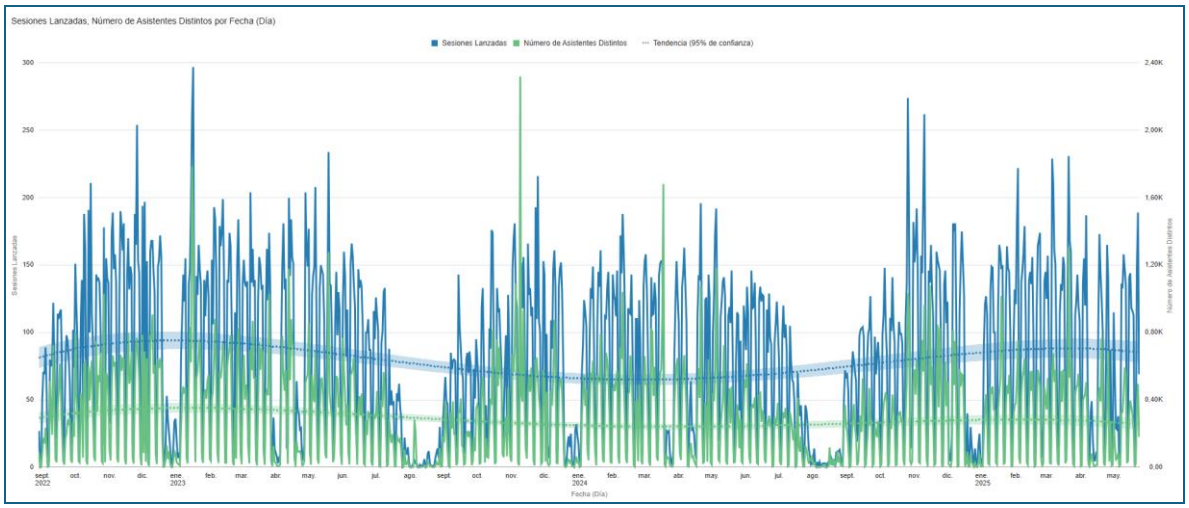
Se ha dado apoyo puntualmente en el uso de Collaborate en eventos organizados por Gerencia.

Datos estadísticos del Aula Virtual

La siguiente gráfica representa el total de usuarios agrupados por perfiles con acceso al Aula Virtual, se observa estabilidad en los últimos cursos académicos, tanto en el profesorado como en el estudiantado.



En relación con el uso de la herramienta de videoconferencia Collaborate Ultra, podemos observar en la gráfica como su uso es mayor al del curso pasado. La gráfica muestra los datos del total de sesiones realizadas por día (en azul) y el total de usuarios distintos conectados por día (en verde), de los últimos tres años académicos.



CONCLUSIÓN

El balance del curso 2024/2025 permite constatar un **avance sostenido en la consolidación y modernización de los servicios TIC de la Universidad Pablo de Olavide**. A lo largo del periodo, el Área ha abordado proyectos de gran envergadura, ha mejorado sus procesos internos y ha reforzado los mecanismos de atención, soporte y seguridad en un contexto tecnológico en permanente evolución.

En el plano de infraestructuras, se han acometido importantes mejoras en redes, equipamiento y comunicaciones, acompañadas de una atención permanente a la experiencia de usuario, especialmente en el entorno docente. La administración electrónica ha seguido consolidándose como eje vertebrador de la gestión universitaria, con nuevas integraciones y procedimientos completamente digitalizados.

En materia de seguridad, se ha continuado con la implantación y cumplimiento del Esquema Nacional de Seguridad, realizando análisis de riesgos, auditorías internas y una mejora sistemática en los procesos de detección, notificación y respuesta ante incidentes. El despliegue de soluciones como EDR y la participación en iniciativas como el proyecto CONSEG refuerzan este compromiso.

Cabe destacar también el **esfuerzo continuado en formación y actualización** del personal técnico, lo que garantiza la adaptabilidad del Área a nuevas herramientas, marcos regulatorios y necesidades institucionales. Esta apuesta por el desarrollo profesional se ha traducido en una mayor eficacia y calidad del servicio.

La colaboración con otras áreas, la implicación en proyectos interuniversitarios y la coordinación con organismos como CRUE-TIC o CCN-CERT permiten avanzar hacia un modelo de gestión más eficiente, seguro y orientado a resultados.

En definitiva, el Área TIC reafirma su papel como **motor de transformación digital en la Universidad Pablo de Olavide**, contribuyendo con solidez, rigor y capacidad técnica al cumplimiento de los objetivos estratégicos de la institución.