SERVICIO DE APLICACIONES Y SISTEMAS

Administración Electrónica y TIC

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 estado llevando a cabo una renovación de la infraestructura de administración electrónica de la Universidad, dado que la que se ha 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

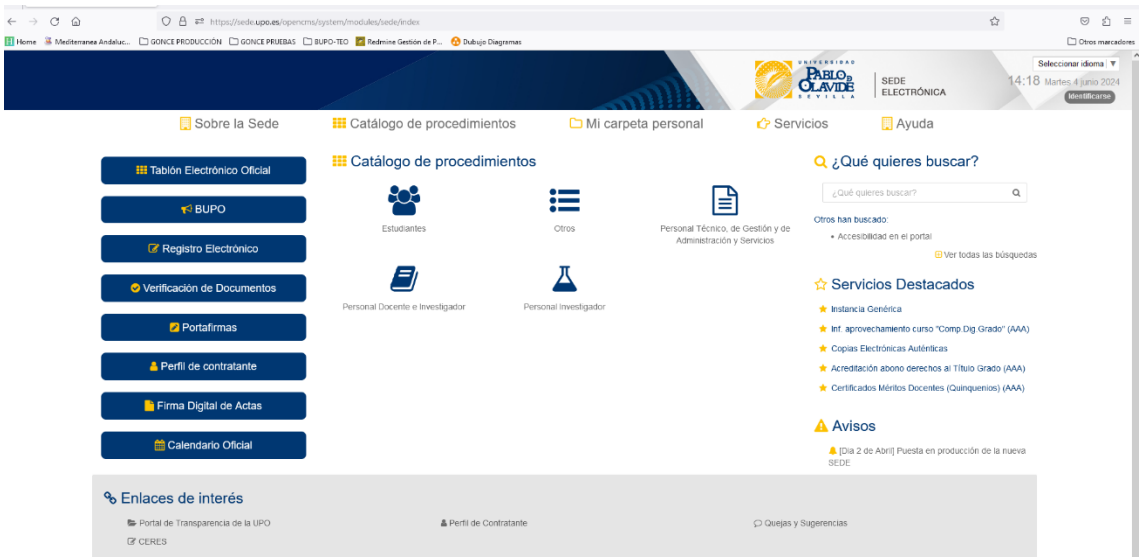
La sede electrónica de la Universidad Pablo de Olavide ha estado disponible en la dirección web https://upo.gob.es/ desde septiembre de 2011 hasta el 2 de abril de 2024, donde pasó a ser https://sede.upo.es. La supresión de la anterior sede y la creación de la nueva fue publicada en el BOJA nº 57 de 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 universitarias como el resto de la ciudadanía que se relacione con esta, 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 2025. 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@)

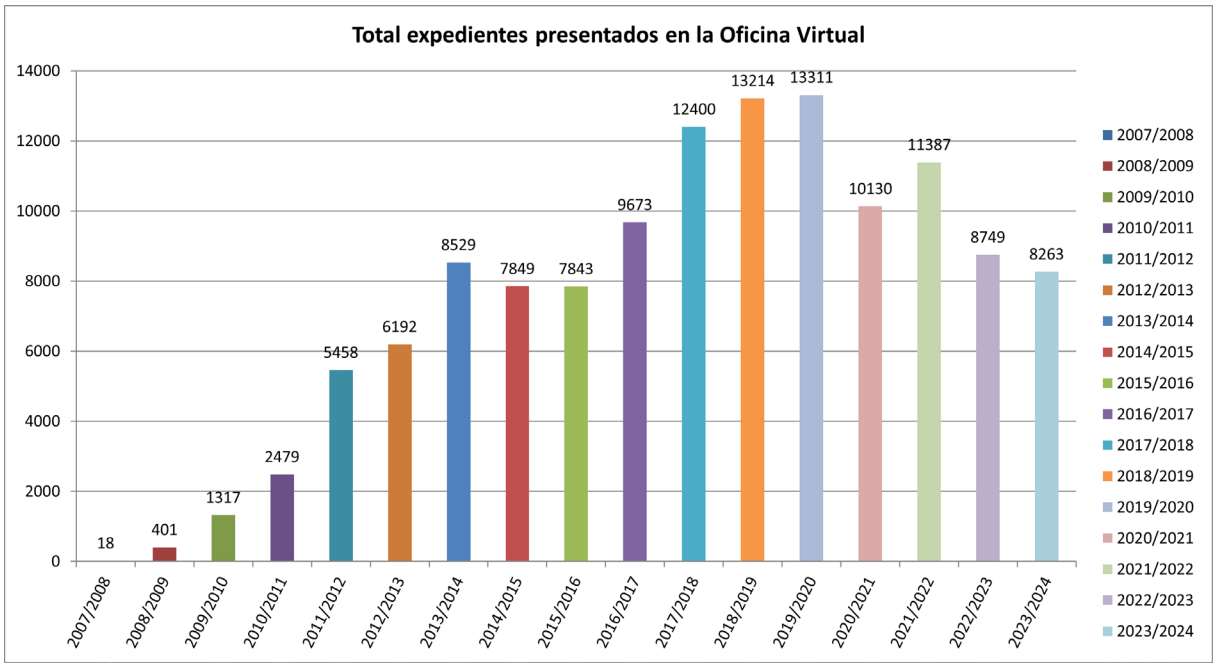
Este es el aplicativo de presentación de solicitudes telemáticas que se ha venido utilizando desde que se comenzó a implantar la Administración Electrónica en la Universidad. El sistema está basado en la aplicación Solicit@, cuyo módulo principal es la Oficina Virtual. Desde este portal web la ciudadanía realiza la

cumplimentación, firma y presentación telemática de los trámites publicados por la Universidad. También se puede realizar el pago telemático de aquellas solicitudes que lo lleven aparejado.

El acceso a dicha Oficina Virtual se puede realizar con certificado digital, con DNIe o mediante integración con adAS (sistema de Single Sign On). Este tipo de acceso permite todo el personal de la comunidad universitaria de la UPO (PTGAS, PDI y estudiantes) puedan utilizar sus credenciales de la Universidad, es decir el usuario y contraseña, que se le proporciona por ser parte de la Universidad, para acceder a la Oficina Virtual.

Trámites presentados a través de la Oficina Virtual

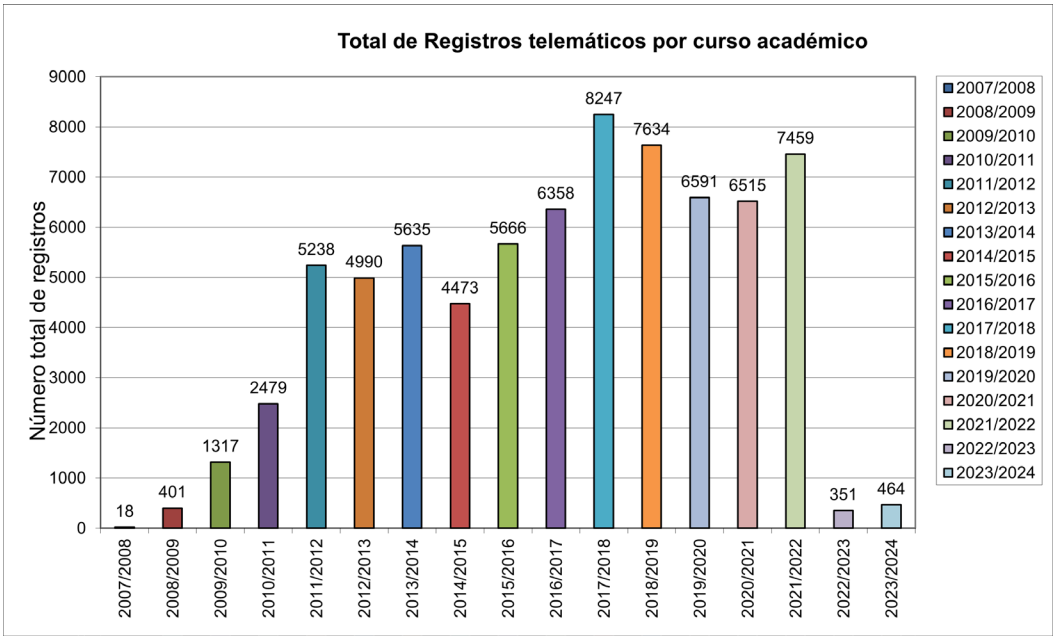
Evolución por curso académico de las solicitudes presentadas en la Oficina Virtual:



Se continúa con la tendencia descendente en las en las solicitudes presentadas durante este último curso académico. Esto se debe principalmente a dos factores:

- El procedimiento de Instancia Genérica ya se presenta directamente en el Registro General del Estado, no realizándose ya a través de nuestra Oficina Virtual.
- Las solicitudes de movilidad saliente para programas ERASMUS, SICUE, Atlanticus, etc., que antes se presentaban a través de la Oficina Virtual, ya se realizan a través de una aplicación desarrollada expresamente para ello.

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



Se constata un claro descenso en las solicitudes presentadas que llevan asiento en registro. Esto es debido a que, con la entrada en funcionamiento de GEISER (Gestión Integrada de Servicios de Registro, aplicación de registro en la nube ofertada por el Ministerio de Asuntos Económicos y Transformación Digital), se realizó un estudio por parte de la Secretaría General y las áreas propietarias de los procedimientos telemáticos para ver cuáles necesitaban ser registrados de forma imprescindible y cuáles no. Es por ello por lo que se eliminó esa dependencia del registro telemático de bastantes procedimientos.

MIGRACIÓN SOLICIT@

Mientras todos los procedimientos telemáticos que se encuentran activos son migrados a la plataforma nueva de Administración Electrónica (G-ONCE), se está desarrollando un paso intermedio que consiste en migrar la aplicación "Oficina Virtual" del servidor de aplicaciones JBoss 5.1.GA a WildFly 11.0. Este proceso se llevará a cabo en los entornos de desarrollo y explotación, asegurando que la aplicación se ejecute de manera óptima y segura en el nuevo entorno.

Con esto se logrará actualizar el servidor de aplicaciones a una versión más reciente y soportada, mejorando así el rendimiento y la seguridad de la aplicación y asegurando la compatibilidad con tecnologías modernas.

Esta propuesta cubre las siguientes actividades:

- Instalación y configuración de WildFly 11.0 en los entornos de desarrollo y explotación.
- Migración de la aplicación "Oficina Virtual" desde JBoss 5.1.GA a WildFly 11.0.
- Uso de miniapplet/Autoscript para la comunicación con Autofirma, versión de Escritorio.
- Pruebas de funcionalidad y rendimiento en ambos entornos

@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.

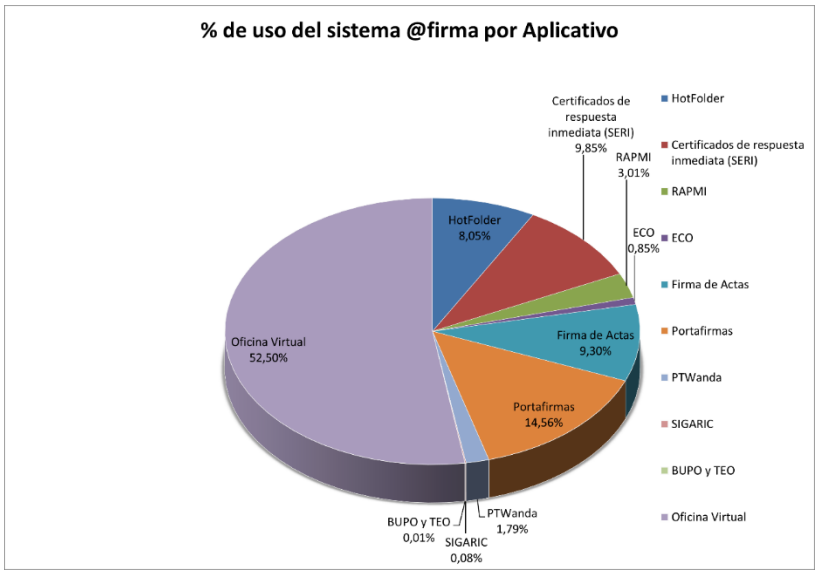
Gracias a @FIRMA, las aplicaciones que la utilicen pueden incorporar procesos de autenticación y firma digital mediante el uso de certificados digitales, independientemente del entorno de desarrollo en que hayan sido programadas.

@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. Y periódicamente es necesario actualizar en nuestra implantación.

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

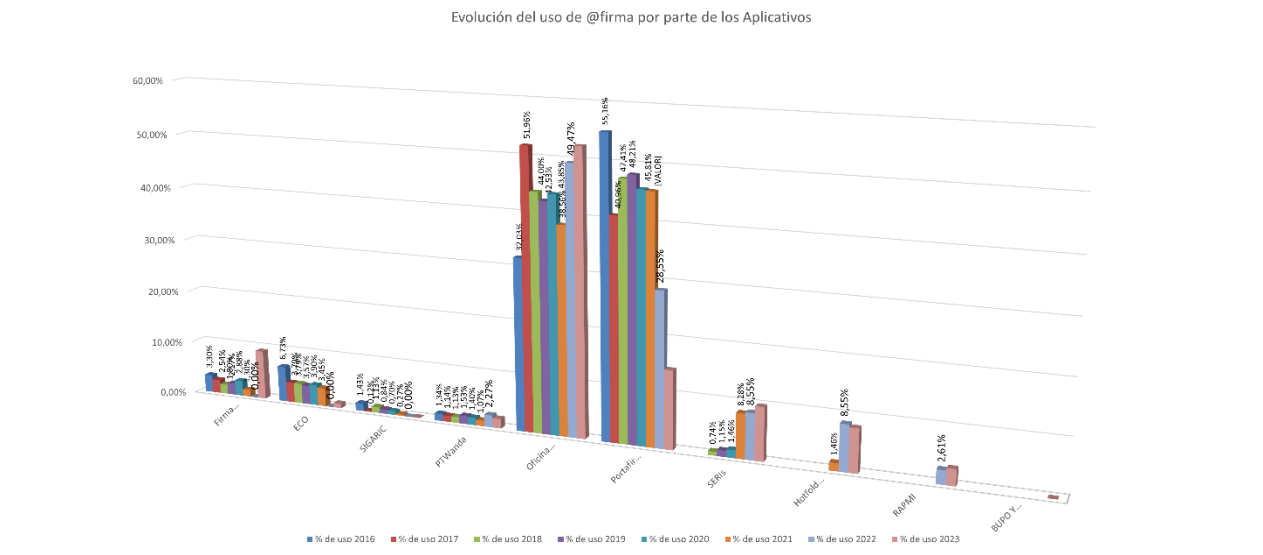
- Autenticación: Proceso que permite autenticar o identificar de forma fehaciente a una entidad basándose en la comprobación de su certificado digital.
- Validación de firmas: Proceso que permite determinar si una firma es válida o no. Se comprueba tanto la validez de la firma (formato y atributos) como 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 siguen siendo Portafirmas v2.3.2 y Oficina Virtual, aunque la Firma Digital de Actas y la emisión de Certificados de Respuesta Inmediata (SERIs) también han sido bastante utilizadas.

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.

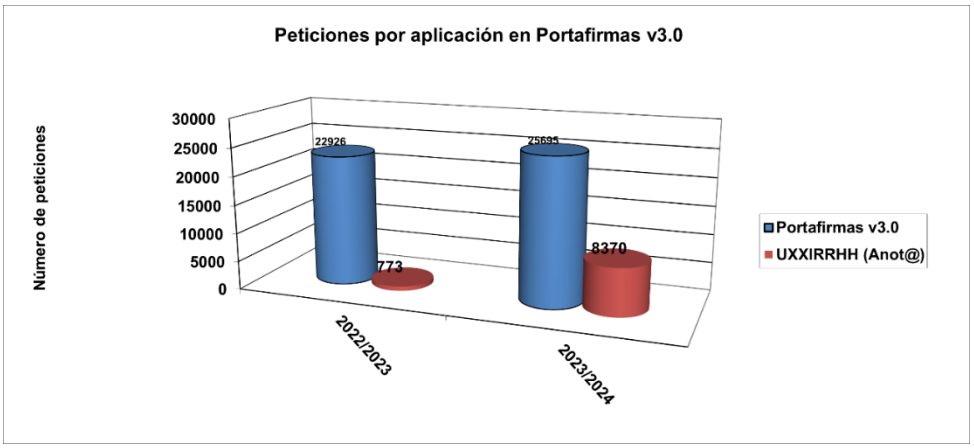
El 24 de febrero de 2022 se puso en marcha la versión 3.5.2.2 de este aplicativo, que, entre otras cosas, lleva como mejora que la autenticación y firma se hace a través de la herramienta Autofirma, aplicación de firma electrónica desarrollada por el Ministerio de Asuntos Económicos y Transformación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

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

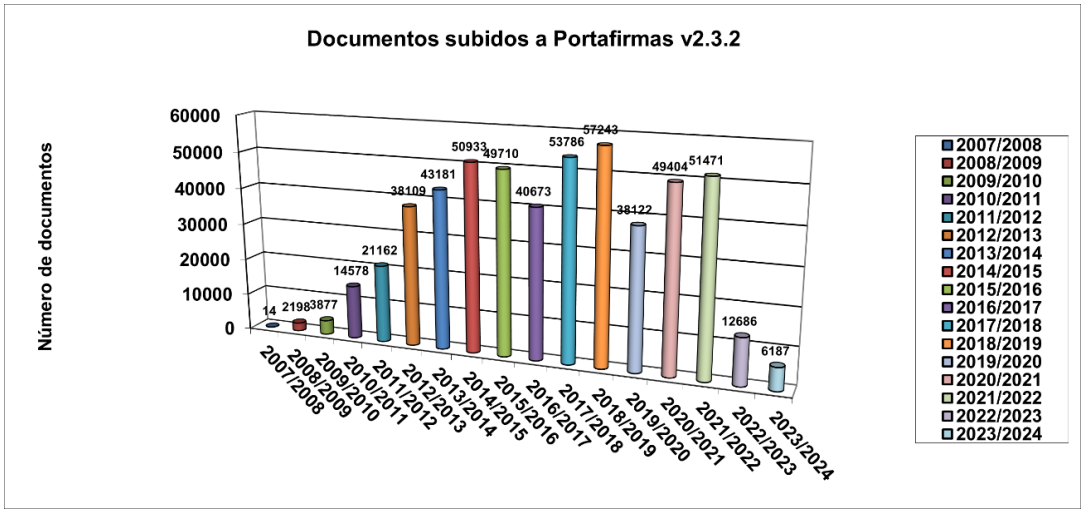
- El aplicativo Anot@ RCP (Registro Central de Personal), que ya está implantado en la Universidad.

- La nueva 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. La firma de los documentos generados durante la tramitación de las solicitudes de estos procedimientos se lleva a cabo a través del aplicativo Portafirmas v3.5.2.2.

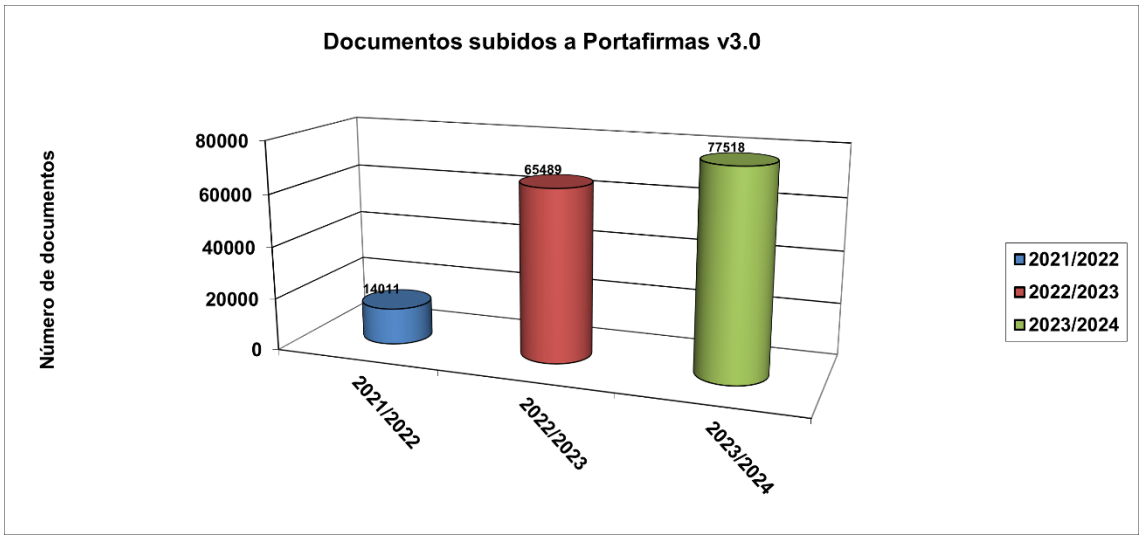
En el siguiente gráfico se puede ver el número de peticiones enviadas a Portafirmas v3.5.2.2 por tipo de aplicación (Portafirmas v3.5.2.2 engloba tanto las peticiones enviadas desde la plataforma G-ONCE como las realizadas desde la propia aplicación Portafirmas):



El antiguo Portafirmas v2.3.2 se utiliza actualmente solo para firma de documentos enviados a través de la aplicación eCO y la antigua plataforma de tramitación, pero se está en trámites de su eliminación definitiva.
En el gráfico podemos ver como se ha reducido a la mitad respecto al año pasado el número total de documentos subidos a Portafirmas v.2.3.2:



Y la evolución del número total de documentos subidos a Portafimas v.3.5.2.2 desde su entrada en producción el 24 de febrero de 2022. Como puede verse, su uso está cada día más generalizado en la Universidad.



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. Entre esos procedimientos, podemos destacar:

- Solicitud de comisiones de servicio del PTGAS, PDI y personal investigador.
- Solicitud de certificado académico personal.
- Solicitud de traslado de expediente.
- Solicitud de título oficial de graduado/a.
- Solicitud de publicación en el Tablón Electrónico Oficial.
- Etc.

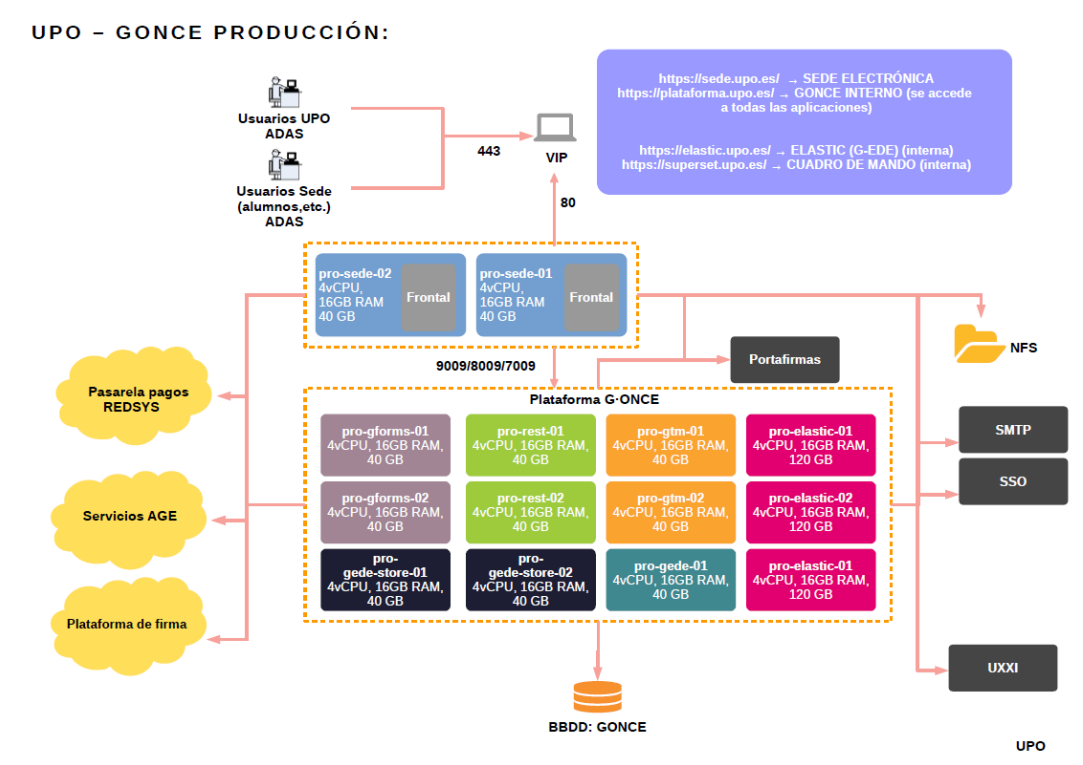
Actualmente todos estos procedimientos están siendo analizados y rediseñados por las distintas áreas con objeto de su racionalización y simplificación y su migración a la nueva plataforma de tramitación de expedientes administrativos, G-TM, que es un módulo dentro de la suite G-ONCE. Cuando estas actuaciones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

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 han creado 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 han implementado 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 los procedimientos de instancia genérica y copia electrónica auténtica, mas 19 procedimientos de actuación administrativa automatizada (AAA) o servicios de respuesta inmediata (SERIs).

La instancia genérica y la copia electrónica auténtica son procedimientos cuya tramitación completa se realza ya a través del motor de tramitación G-TM.

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 Habilitados (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, 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 28 de noviembre de 2023 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 9533 asientos en el libro de registro electrónico de entrada y 1165 asientos en el libro de registro electrónico de salida.

Proyectos en desarrollo

- Despliegue de servicios SCSP (Supresión Certificado Soporte Papel) en la infraestructura de la Universidad Pablo de Olavide.

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.

Se está probando 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 probando la opción de Recubrimiento, que es la consulta a través de servicios web normalmente desde dentro de gestores o plataformas de tramitación.

Aplicaciones Corporativas y Sistemas

Portales Web

Las plataformas basadas en contenedores han continuado su desarrollo y crecimiento. Hemos incorporado nuevos servicios y actualizado imágenes y herramientas administrativas.

Podemos ver cómo el sistema se adapta bien al ritmo de crecimiento y seguimos sin identificar problemas técnicos o de seguridad reseñables.

Como paso siguiente, hemos comenzado a ensayar una nueva plataforma basada en Kubernetes y todo su ecosistema de herramientas relacionadas. Se han implantado dos conjuntos de clústers: uno para experimentación propia y otro que proporciona servicios a UXXI. La idea sería valorar e incorporar herramientas de gestión útiles e ir familiarizándonos con los entornos k8s. Una propuesta de futuro consistiría en migrar los actuales hosts Docker a plataformas k8s.

Con respecto a los CMS corporativos basados en OpenCms, seguimos migrando contenidos a las plataformas más modernas. Se ha procedido a la remodelación de algunos de ellos, como el portal de Postgrado, se han incluido también pequeñas mejoras en el actual portal principal. De la misma forma, seguimos retirando los sistemas más antiguos basados en pila LAMP.

El proxy corporativo sigue operando sin novedad.

Finalmente, en el ámbito de la seguridad, se está realizado un importante esfuerzo en la corrección y actualización de varios problemas en el ámbito de una auditoría realizada recientemente.

Correo electrónico

El sistema de correo electrónico de la Universidad Pablo de Olavide está respaldado por software de código abierto y ha sido diseñado para satisfacer las exigencias actuales en términos de usabilidad, capacidad, disponibilidad y seguridad.

Nos dedicamos activamente a la mejora y actualización continua de este servicio, con el objetivo de mantenernos a la vanguardia tecnológica. En el contexto actual, subrayamos la importancia de intensificar nuestros esfuerzos en materia de seguridad. En este sentido, seguimos implementando mejoras constantes en los protocolos de actuación y en las medidas de seguridad que protegen el sistema de correo contra los

diversos y cada vez más sofisticados ataques. Cada incidente representa una oportunidad para adaptar y fortalecer aún más nuestras defensas.

Nuestro enfoque se centra en mantener la eficacia y rapidez en la detección de ataques dirigidos a la captura de credenciales, logrando detenerlos de manera pronta y eficiente. Además, colaboramos activamente con el Instituto Nacional de Ciberseguridad para mejorar la gestión y tratamiento de los distintos incidentes de seguridad, así como para implementar medidas adecuadas de contención. A su vez, el servicio "Lavadora" de RedIRIS, al cual estamos adheridos, continúa siendo eficaz. Este sistema filtra de manera eficiente el correo entrante a nuestra institución, protegiéndonos de una multitud de amenazas y correo no deseado. Para complementar esto, también estamos trabajando en la elaboración automática de informes de actividad sospechosa en el uso del servicio de correo electrónico, permitiéndonos actuar de manera proactiva en la detección de posibles capturas de credenciales e incidentes de seguridad en general.

Durante el presente curso, hemos estado trabajando y continuamos haciéndolo en la renovación completa de toda la infraestructura de correo electrónico. En este sentido, se han creado máquinas virtuales con sistemas operativos actualizados a la última versión disponible para alojar el nuevo software. También se ha procedido a reinstalar todo el software con las últimas versiones disponibles en dichos servidores. Hasta el momento, nos hemos centrado en la instalación de todas las estafetas de correo externas, tanto de correo entrante como saliente de la UPO, así como en la estafeta que aloja el servicio de antivirus. En cuanto al resto de elementos, seguimos trabajando en su actualización y esperamos finalizar estos trabajos el próximo curso.

Asimismo, estamos implementando medidas de seguridad adicionales, como DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting, and Conformance). DKIM permite al destinatario del correo verificar que el mensaje ha sido enviado por un dominio autorizado y que no ha sido alterado durante el tránsito. DMARC, por su parte, es un protocolo que, basado en los mecanismos SPF (Sender Policy Framework) y DKIM, permite a los propietarios de dominios proteger sus dominios contra el uso no autorizado, como el phishing y el correo electrónico fraudulento. Estas medidas contribuirán significativamente a mejorar la seguridad y confiabilidad de nuestro servicio de correo electrónico.

Adicionalmente, hemos estado trabajando en la mejora y gestión de la detección de cuentas de correo obsoletas y que ya no son necesarias. Esta iniciativa tiene como objetivo incrementar el espacio disponible para el resto de los usuarios, mejorar el rendimiento del sistema y reducir la posibilidad de uso fraudulento de dichas cuentas. Esta gestión eficiente de las cuentas de correo garantiza un entorno más seguro y optimizado para todos nuestros usuarios.

Gestión de identidades

El Servicio de Gestión de Identidades de nuestra institución desempeña un papel fundamental al proporcionar diversas opciones de acceso, tales como nombre de usuario y contraseña, tarjeta inteligente o DNI electrónico. Este servicio actúa como puerta de entrada tanto al Sistema de Identidad Federado de las Universidades Españolas (SIR) como a un creciente número de servicios ofrecidos por nuestra Universidad. Entre estos se encuentran servicios destacados como "Aula Virtual", "Oficina Virtual", "Firma Automatizada", "Repositorio Seguro", "Formación Plan Docente", "Laboratorios Virtuales" y "Servicio de Biblioteca". Además, funciona como punto de acceso a aplicaciones específicas gracias a la integración de nuestra plataforma de identidad con el sistema de Identidad Electrónica para las Administraciones conocido como "Cl@ve", facilitando así el acceso a usuarios externos a nuestra institución.

Hemos implementado las últimas actualizaciones disponibles en el software tanto de nuestro sistema de autenticación única (Single Sign-On, SSO) como de nuestro gestor de cambio de contraseñas para mejorar tanto la seguridad como las funcionalidades de este servicio. Reconocemos la importancia de establecer nuevos controles de seguridad para prevenir diversos ataques, especialmente aquellos de fuerza bruta. Estos controles han demostrado ser altamente efectivos, evitando numerosos intentos de ataques que son comunes en los servicios informáticos en general.

Asimismo, continuamos trabajando en un ambicioso proyecto de mejora integral del Servicio de Gestión de Identidades. Nuestro objetivo es evolucionar los procedimientos y sistemas actuales de gestión de identidades y accesos, integrándolos en un diseño global con objetivos ampliados y claramente definidos.

Se han realizado tareas de gestión y mantenimiento de cuentas, así como la reducción y detección de duplicados, con el fin de minimizar la posibilidad de uso fraudulento de cuentas obsoletas. También se han llevado a cabo tareas de actualización de los certificados del conector SAML2 (Security Assertion Markup Language 2.0) de nuestro SSO, lo que ha implicado una coordinación especial y actualizaciones en un gran número de servicios que podían verse afectados por esta razón. Toda esta labor se ha desarrollado de forma transparente y sin pérdida de servicio de ninguna clase.

Por otra parte, también se está trabajando en la actualización y renovación del servicio de Directorio corporativo. De esta forma se pretende mejorar la seguridad y el rendimiento del mismo.

En resumen, el Servicio de Gestión de Identidades sigue siendo una pieza clave en la infraestructura tecnológica de nuestra institución, mejorando continuamente para garantizar un acceso seguro y eficiente a todos nuestros recursos y servicios.

Infraestructuras

Se ha estado trabajando con el objetivo de mejorar la eficiencia, seguridad y disponibilidad de los recursos tecnológicos de nuestra institución.

En primer lugar, se ha trabajado intensamente en la mejora de la gestión del almacenamiento. Nuestro objetivo ha sido proporcionar a la Universidad un sistema de almacenamiento seguro, con alta disponibilidad, y replicado en varios Centros de Procesamiento de Datos (CPD) para garantizar el acceso continuo ante cualquier eventualidad. Este nuevo sistema de almacenamiento se caracteriza por ser moderno, rápido y contar con medidas de seguridad avanzadas contra ransomware, para evitar situaciones de pérdida de información y mejorar la seguridad de los datos de nuestra organización. Este esfuerzo ha resultado en la adquisición de nuevas cabinas de almacenamiento que serán instaladas próximamente, permitiendo disfrutar de todas estas ventajas a partir del próximo curso.

En cuanto a las infraestructuras de virtualización, se ha procedido a actualizar todo el entorno con las últimas versiones de software disponibles que nuestra infraestructura de servidores físicos puede soportar. Asimismo, se ha incrementado la memoria disponible al máximo, lo que nos permite alojar un mayor número de servidores virtuales en cada uno de nuestros nodos de virtualización. Este aumento de capacidad se traduce en una mayor flexibilidad y eficiencia en la gestión de nuestros recursos. Además, se han llevado a cabo estudios exhaustivos en toda nuestra infraestructura de virtualización que han sido fundamentales para detectar posibles mejoras, así como planificar el trabajo necesario para implementarlas en el futuro. Esta

revisión proactiva y análisis nos permite mantener un entorno de virtualización robusto y optimizado, alineado con las mejores prácticas y estándares actuales.

Con respecto a nuestro servicio de respaldo, se ha estado trabajando para actualizar el software a la última versión disponible y mejorar toda la infraestructura de respaldo (backup). Se ha realizado un estudio exhaustivo sobre toda nuestra infraestructura de backup para detectar posibles mejoras, lo cual nos ha proporcionado información valiosa que estamos implementando. Estas mejoras están dirigidas a reducir el tiempo necesario para realizar los backups, disminuir el tamaño de los mismos, así como mejorar la seguridad y el rendimiento general del servicio.

En resumen, las acciones realizadas en la gestión de infraestructuras han sido dirigidas a asegurar un entorno tecnológico seguro, eficiente y altamente disponible, que responda adecuadamente a las necesidades presentes y futuras de la Universidad. La adquisición de nuevas cabinas de almacenamiento, la actualización de nuestras infraestructuras de virtualización y las mejoras en el sistema de backup son pasos decisivos que nos posicionan favorablemente para enfrentar los retos tecnológicos y proporcionar un servicio de alta calidad a toda la comunidad universitaria.

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:

- Se amplía la funcionalidad de la aplicación de Horarios para postgrado, añadiendo nuevos controles de cara sobre todo al profesorado externo que impartirá docencia.
- Continua el piloto de una nueva aplicación de generación y gestión de horarios de la empresa Bullet: Bullet Calendar y Bullet
- Se inicia el piloto con Microsoft para la automatización de procesos que se hacen manualmente.
- Se finaliza el nuevo Cuadro de datos de estudiantes.
- Se desarrolla una nueva consulta de listas de clase por actividad.
- Nuevos SERIs de acreditaciones de curso impartidos por biblioteca y docencia virtual.
- Se incorpora de forma paulatina una nueva página de estilos para las consultas web del Servicio Personalizado.

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.
- I2aCronos: Se traslada el aplicativo a una infraestructura en la nube.
- Gescontrata: Se actualiza la aplicación y se cambia una infraestructura virtual
- RAPMI: Se incorporan nuevas funcionalidades.
- Actualización de la infraestructura de ODA a la versión 19.20

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.
- TEO (Tablón Electrónico 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.
- Se continua el desarrollo de un aplicativo para la gestión de censos.
- Nuevo aplicativo para la Gestión de los Traslados y Reconocimientos de Créditos. Sustituirá al anterior procedimiento electrónico, el cual tenía bastantes limitaciones. En fase de pruebas.
- Nuevo aplicativo de Baremación del PDI.
- Nuevo aplicativo de Elaboración del POD.
- En desarrollo un nuevo SERI de Actividad Docente del Profesorado
- Se está desarrollando una consulta de los datos históricos de la aplicación ECO, que será sustituida por un nuevo aplicativo.
- En fase de finalización de la nueva APP Crue

Aula Virtual

Al Aula Virtual, plataforma de docencia virtual institucional, 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.

El servicio de Aula Virtual ha trabajado intensamente este curso académico 2023-24 en la nueva versión ultra de la plataforma de Aula Virtual. Por un lado, se ha implantado en el entorno explotación la Navegación Ultra, ésta proporciona acceso directo a las herramientas principales con el contenido relativo a todos los espacios virtuales asignados, mejorando la accesibilidad y seguimiento de los cursos tanto por parte del profesorado como del alumnado; y por otro, se ha trabajado en la parte de los Cursos Ultra, configurándola y testeándola en un entorno controlado de pruebas, minimizando así el impacto a los usuarios cuando se realice su paso a explotación.

Como 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; mantenimiento y actualización diaria del acceso del profesorado y estudiantado al Aula Virtual

Para la docencia del curso académico 2023-24, se crearon de oficio todos los espacios virtuales de estudios de Grado, Máster y programas de Doctorado. A petición del CUI se han creado todos los espacios virtuales necesarios 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.

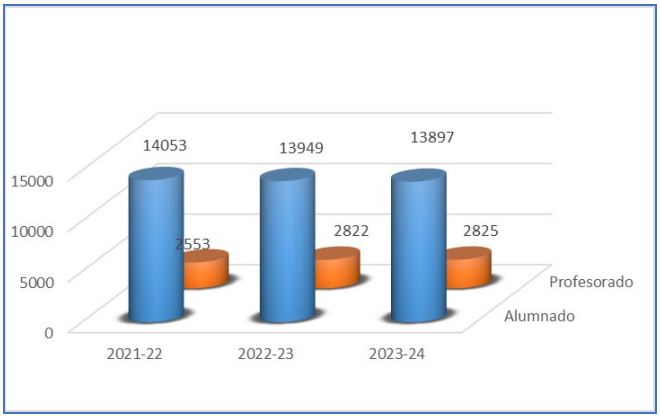
A continuación, se indica brevemente las tareas planificadas dirigidas a la mejora del rendimiento de la plataforma y a la satisfacción de los usuarios en este curso académico:

- Se ha implementado el servicio de respuesta inmediata para que el profesorado pueda obtener automáticamente el informe de uso de la plataforma de Aula Virtual de los últimos cinco años lectivos.

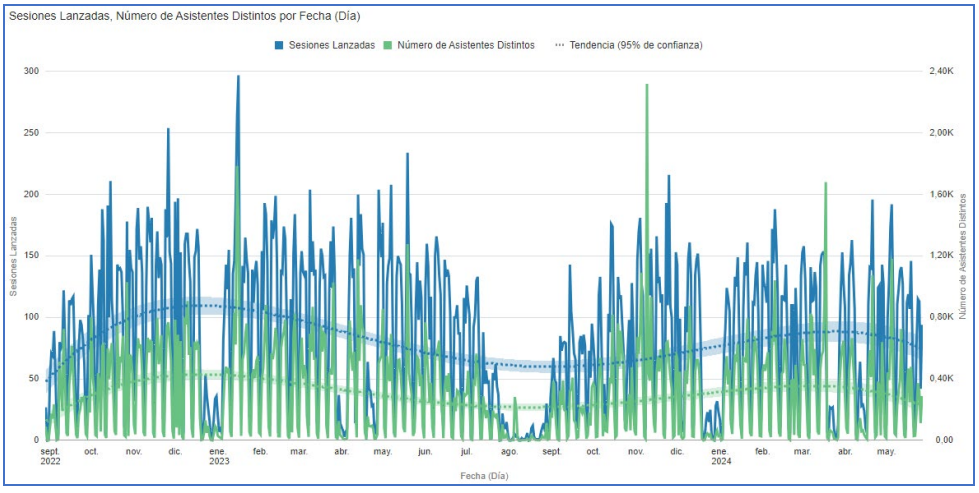
- Se ha proporcionado usuario supervisor de Collaborate, así como la formación y manuales creados especialmente para este cometido, a las áreas/unidades en las que se ha justificado la necesidad de crear y gestionar salas para la realización de reuniones, seminarios, jornadas, etc.
- Se han eliminado del Aula Virtual los espacios virtuales del curso 2022-23, así como los usuarios que no tenían ningún espacio virtual asignado en el curso 2023-24. Con ello mejoramos el tiempo de respuesta de la plataforma, minimizamos el espacio de almacenamiento y reducimos así costes de mantenimiento.
- 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 alumnado.



Con relación al uso de la herramienta de videoconferencia Collaborate Ultra, podemos observar en la gráfica como su uso es poquito menor 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).



El Servicio de Formación e Información, cuyo objetivo es facilitar toda la información y formación relativa al uso de las herramientas disponibles en la Universidad que sirvan de apoyo para el desarrollo de la docencia virtual, así como de cualquier otra herramienta que ayude a la innovación docente, ha venido trabajando durante todo el curso en la generación de videos tutoriales, especialmente basados en la nueva versión ultra de la plataforma de Aula Virtual. Todos ellos se han agrupado en una nueva serie en UPOTV, facilitando así su localización.

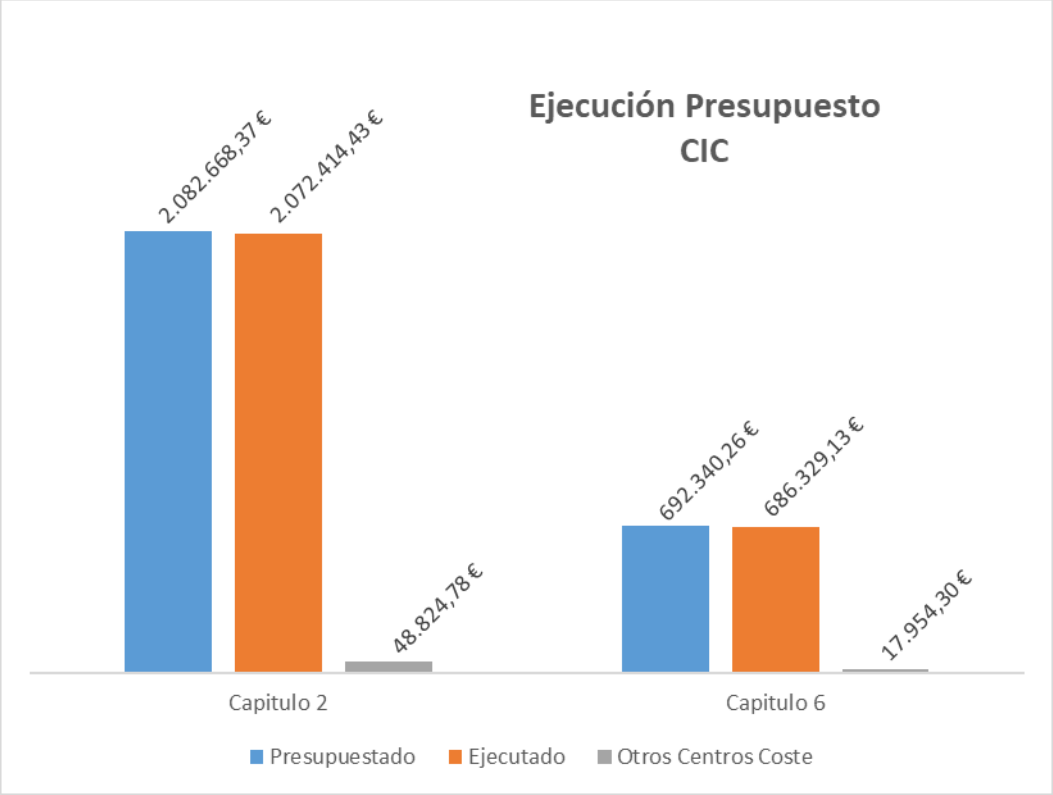
GESTIÓN ADMINISTRATIVA

Gestión Económica

Las tareas relacionadas con la contratación de servicios y suministros son las que suponen una mayor carga de trabajo para la Oficina de Gestión Administrativa.

Para disponer de la información inmediata sobre el estado de ejecución del presupuesto económico del Área, se ha desarrollado una hoja de cálculo que muestra el estado de tramitación de cada expediente, así como el acumulado por cada uno de las partidas presupuestarias y proyectos de actuación.

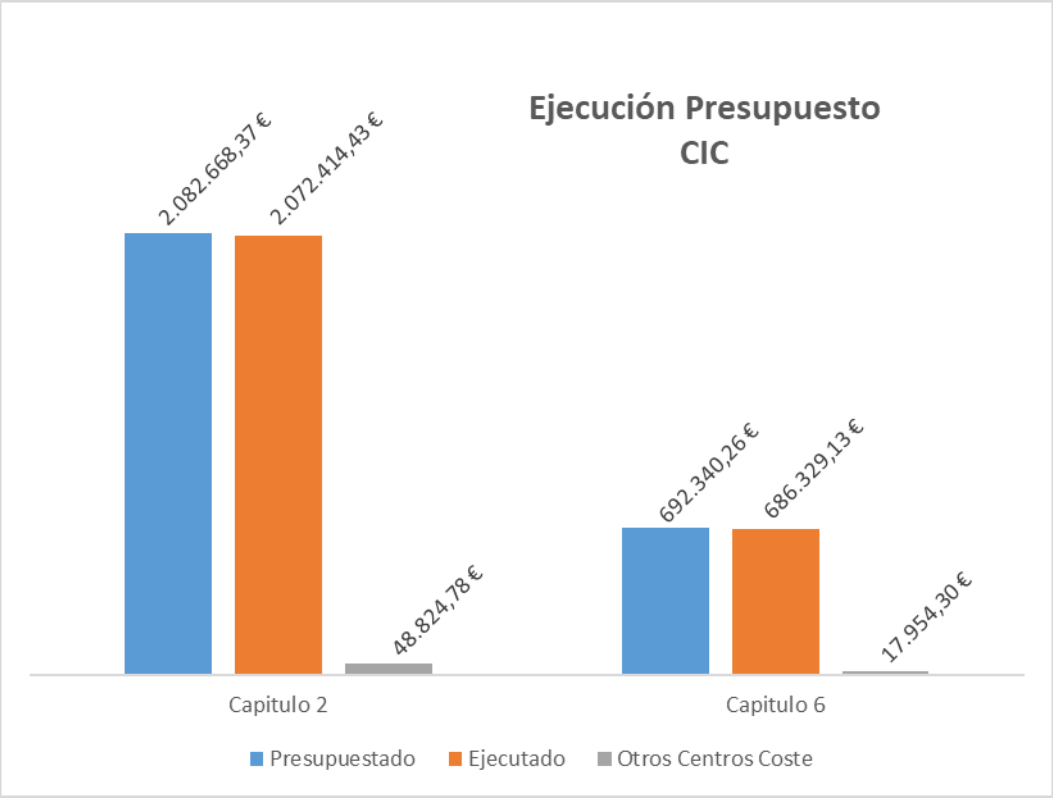
El siguiente gráfico muestra el grado de ejecución del presupuesto del ejercicio 2023.



Conforme con la normativa sobre contratación pública y las instrucciones específicas al respecto dictadas por la Gerencia, se realizan trámites para la formalización de contratos mayores o menores, permitiéndose para estos últimos y en determinadas circunstancias, la adjudicación directa sin la apertura del expediente.

Además de la gestión de servicios y suministros cuyo coste recae sobre el presupuesto del Área, desde ésta se realizan los trámites de solicitud y valoración de ofertas, así como, en su caso, la aceptación y recepción de los servicios y suministros relacionados con las TIC y cuyo importe debe ser soportado por otros Centros de Coste de la Universidad.

El siguiente gráfico muestra el número de expedientes de cada tipo tramitados a lo largo del año 2023 y el primer semestre de 2024.



Estos expedientes de contratación han generado la tramitación de 347 justificantes de gasto durante el ejercicio 2023 y de 129 durante el primer semestre de 2024.

Las contrataciones de inversiones con cargo al capítulo 6 y sus posteriores asignaciones a las unidades organizativas responsables del buen uso y custodia de los bienes, así como las bajas de estos al final de su vida útil, han supuesto la tramitación en el año 2023 de 842 fichas de inventario y de 547 en el primer semestre de 2024.

Otros trámites administrativos

A solicitud de los/as proveedores/as, se han emitido durante el curso 2023/2024 un total de 5 informes sobre la correcta ejecución de los servicios y/o suministros contratados para su posterior certificación por parte de la Secretaría General.

Por otro lado, se han presentado 54 solicitudes y/o incidencias a través de la plataforma TIKA destinadas a distintas áreas y servicios de la Universidad.

Desde la Oficina de Gestión Administrativa se ha gestionado la entrega en modalidad de préstamo de equipamiento portátil al Personal de Administración y Servicios. Se han entregado un total de 157 ordenadores portátiles.

Con posterioridad, y para la realización de actuaciones en dichos equipos, se ha gestionado su recogida, entrega al personal técnico y posterior devolución a los/as usuarios/as.

SERVICIO DE REDES Y EQUIPAMIENTO

Redes, comunicaciones e infraestructura

Servicio de Red Inalámbrica WIFI

Mejora del Servicio

La red WiFi de la UPO es una de las herramientas que más uso tiene en la universidad, puesto que se utiliza para tareas tan variopintas como realizar las prácticas de las asignaturas o chatear por Whatsapp; es igualmente utilizada por personas pertenecientes a la comunidad universitaria como por invitados, y el número de servicios disponible va aumentando, haciéndola más versátil.

Es sabido, sin embargo, que su infraestructura es precaria debido a la obsolescencia de sus sistemas de control. Para mejorar el estado de la red, en función de los presupuestos de los que se dispone, se realizan pequeños proyectos que ayudan a mejorar la calidad de la red inalámbrica y, por ende, la percepción de los receptores de los servicios que sobre ella se ofrecen. En esta línea, se han realizado las siguientes tareas de mejora:

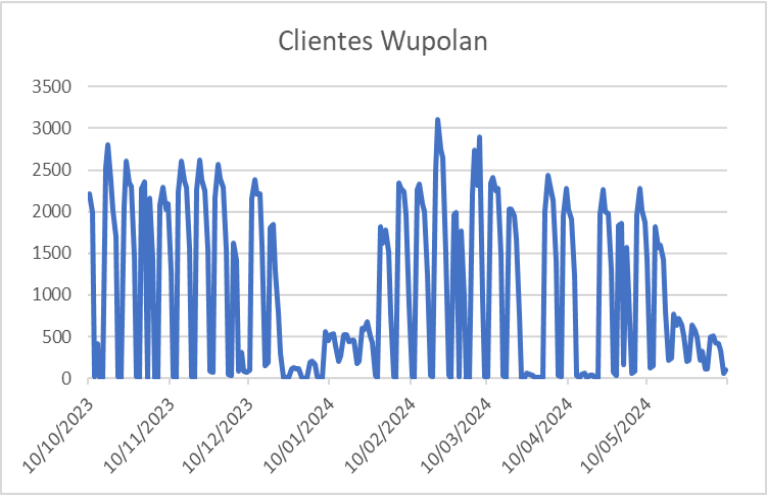
1. Actualización de los sistemas de autenticación y autorización de la red inalámbrica (RADIUS): tras detectar problemas de desconexión de usuarios de la red WiFi y de una investigación profunda, se llegó a la conclusión de que el fallo podía provenir del software actualmente utilizado para autenticar a los usuarios y autorizar el acceso a los diferentes perfiles. Una vez actualizado, se observa que el problema se elimina.
2. Actualización de los puntos de acceso (AP): dada la obsolescencia de muchos de los puntos de la red WiFi, se aprovechó una promoción de un fabricante de puntos de accesos de calidad (Juniper) para cambiar algunos de estos APs que podían dar problemas por unos nuevos más modernos de dicho fabricante, con tecnología 802.11ax, que da lo que se conoce como WiFi 6, un estándar mucho más avanzado, seguro, con mayor cobertura y mejor soporte de aplicaciones. Los edificios renovados son el 9, 21, 47, 31 y 32.

3. Siguiendo con la idea de mejora continua, se siguen realizando test de nuevos modelos de APs para analizar los resultados obtenidos en comparación con los actuales. Se está realizando uno prueba en el edificio 44, el cual tenía la cobertura inalámbrica muy limitada, realizando la prueba con un modelo de protocolo 802.11ax con Wifi 6, pero con diferentes capacidades de los anteriores.

Conexiones

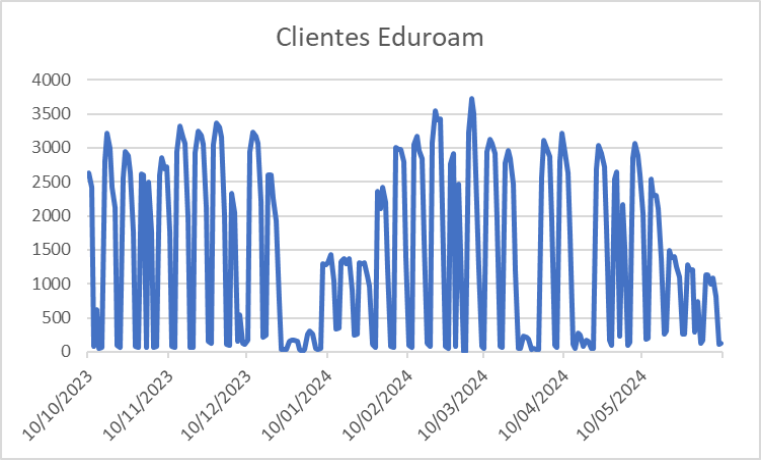
El uso y la conexión a la red WiFi de la UPO ha crecido en este curso un 66 % respecto al año anterior, en número de usuarios. A continuación, se muestran unas gráficas en las que pueden verse el elevado número de conexiones existentes en las diferentes modalidades (Eduroam encriptada y Wupolan abierta). Puede observarse como los máximos alcanzan valores considerables superiores a los 3.500 clientes al día.

CLIENTES WUPOLAN



-Máximo número de clientes conectados a Wupolan por día en los últimos 8 meses-

CLIENTES EDUROAM



-Máximo número de clientes conectados a Eduroam por día en los últimos 8 meses-

TELEFONÍA

En el Plan de Transformación Digital podemos encontrar la acción *1.5.1: Facilitar el Teletrabajo*. En relación a esta línea de trabajo, en el sector del CIC encargado de la telefonía corporativa se han realizado las siguientes acciones:

1. Para facilitar la movilidad al personal PTGAS que está en teletrabajo, se está realizando una migración del puesto de voz fijo al puesto de voz móvil. Al personal del PTGAS que está en este programa se le está facilitando un terminal móvil con una línea sólo voz que sustituye al terminal fijo actual, teniendo un número móvil que pasa a ser el número de localización de esas personas. El terminal fijo se elimina, teniendo el número fijo que tenían hasta entonces un desvio hacia el nuevo número móvil. Dicho desvío se elimina tras un tiempo prudencial que permite informar a la comunidad y publicar el nuevo número de contacto. Actualmente se ha realizado la migración de 73 personas pertenecientes al PTGAS que ya trabajan de forma definitiva con su número móvil.

2. Renovación de móviles: En la misma línea se ha procedido a renovar 88 de los 160 terminales móviles que existen en la actualidad en la UPO (sin contar con los descritos en el punto anterior). Estas renovaciones permiten tener la última tecnología con las medidas de seguridad actualizadas, lo que permite a los usuarios realizar trabajos desde el mismo dispositivo móvil, ya que con la renovación de equipos aumentan las capacidades de dichos terminales.

SEGURIDAD EN LAS COMUNICACIONES

Respecto a la seguridad en las comunicaciones, cabe destacar diferentes actuaciones para mantener la red de datos y su equipamiento en el estado más seguro posible, siendo estas algunas de dichas actuaciones:

- Actualizaciones de los cortafuegos.
- Actualización de los equipos de gestión y monitorización de red.
- Pilotos con diferentes sistemas de libre distribución para renovar los sistemas de monitorización de red (Cactis y oPUtils).
- Actualización del balanceador de carga para que permita intercambio de claves Diffie-Helman en perfiles SSL.
- Eliminación de los protocolos TLS1.1 y TLS 1.0 en los servicios publicados en el balanceador.
- Estudio de otras medidas sugeridas por la auditoría de seguridad.

Red de datos

En este apartado caben destacar dos actuaciones llevadas a cabo en este curso.

1. Instalación en el pabellón 27: la actuación realizada en el pabellón 27 ha consistido en la instalación específica para un equipamiento de investigación, con equipamiento independiente y configuración individualizada para su estudio.

2. Acceso a Internet en el Pabellón de Marruecos. Con motivo del traslado de la sede de la UPO en Sevilla al Pabellón de Marruecos se ha realizado la instalación de la conexión a Internet en dicho Pabellón. El acceso se mantiene con las mismas características tanto de ancho de banda como de seguridad, estando ya disponible desde abril.
3. Otras actuaciones: diversas tareas de instalaciones de nuevas tomas y reparaciones de las existentes son llevadas a cabo por el sector del CIC encargado de los cableados. A continuación, se muestra una gráfica del reparto de las actuaciones a nivel de instalación ocurridas en la red cableada en las instalaciones centrales de la UPO, distribuidas entre nuevas instalaciones de tomas de red y reparaciones de las tomas de red existentes.

Equipamiento de Red de datos

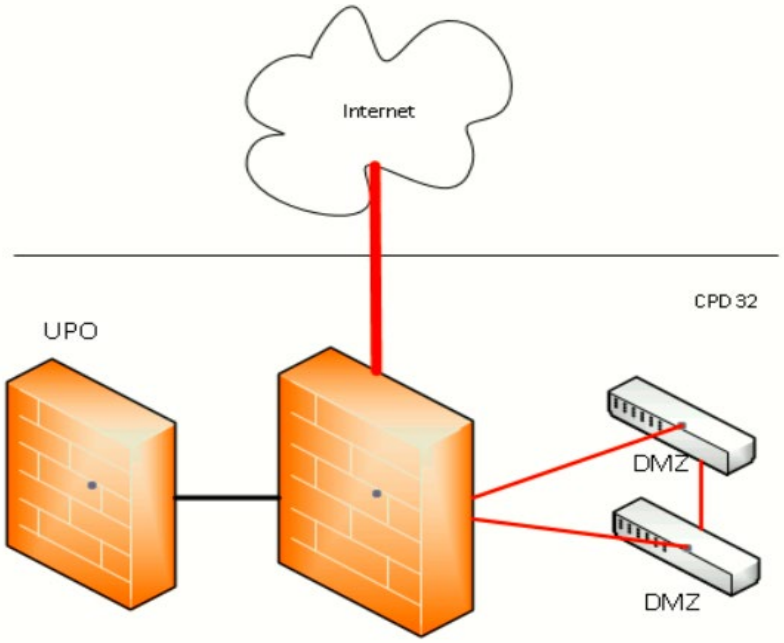
Dentro de los proyectos enmarcados en el Plan de Transformación Digital realizado por el Vicerrectorado de Transformación Digital se encuentran las dos acciones realizadas a nivel de red de datos de la UPO, que se ubican bajo la acción 1.2.3. Actualización/Optimización de infraestructuras tecnológicas.

1. <u>Renovación de la infraestructura de la red perimetral.</u>

Los trabajos realizados en esta acción han consistido en la realización de en la adquisición mediante concurso público de dos equipos de altas prestaciones para su uso como DMZ (Demilitarized Zone o Zona Demilitarizada). La DMZ se utiliza para ubicar allí servicios que son de uso tanto interno como externo a la UPO, así como aquellos otros servicios o equipos de investigadores que por su singularidad no deben estar ubicados dentro de la zona de red de datos protegida.

Este equipamiento, una vez adquirido, ha sido instalado en el CPD 32 de la UPO, realizándose su configuración adecuada a los requerimientos de los nuevos servidores que van a sustituir a los antiguos, de forma más segura, con alta disponibilidad y un ancho de banda mínimo de 10 GB por servidor.

El esquema es el siguiente:



2. Renovación de equipamiento de acceso.

La red de datos se encuentra siempre en constante renovación, procurando en la medida de las posibilidades presupuestarias renovar los equipos más antiguos para tener siempre una red lo más actualizada y segura posible. En este sentido, este curso se han cambiado 19 equipos a nivel de terminal que se ubica en las diferentes plantas de los edificios para que las personas usuarias puedan utilizar sus ordenadores. El cambio se realizó, como siempre, sin afectación al servicio.

A continuación, mostramos un cuadro con un resumen del estado de los equipos de acceso de la red de datos, donde se puede ver el año de instalación de los equipos.

Estado Actual de los dispositivos de acceso			
Marca	Modelo	Qty	Año instalación
H3C		17	2024
H3C		3	2024
3COM	4200	60	1998-2004
3COM	4210	1	2003
3COM	4500	1	2005
HP	1910	80	2005-2010
HP	1912	1	2005-2010
HP	1920	30	2010-2015
Juniper	4200	10	2007-2009
Huawey	S5720	25	2015
Extreme	X450 a	1	2001

Estado Actual de los dispositivos de acceso			
Marca	Modelo	Qty	Año instalación
Aruba	J9773A	2	2015
Cisco	2960	103	2015
Cisco	9200L	10	2020
Cisco	C3560	30	2010
Cisco	C3750	1	2015

Otros temas de interés

En este año se ha realizado un estudio para la mejora del rendimiento en términos energéticos de los CPDs que tiene la Universidad en la sede central, a saber:

- Centro de Datos principal, ubicado en el edificio 32 (CPD 32).
- Centro de Datos de respaldo, ubicado en el edificio 1 (CPD 1).
- Punto de Presencia de RedIRIS (PdP), ubicado también en el edificio 1.
- Sala de Housing de sistemas de cálculo científico.

Este estudio permite comprobar si podría optimizarse y mejorar su consumo, así como detectar posibles situaciones que puedan suponer riesgos ocultos.

A modo de resumen se muestra el DAFO aportado tras el estudio en el que se pueden ver el estado general de los CPDs, sobre el que habrá que ir trabajando para mejorar la eficiencia.

Fortalezas
- Concienciación del problema de la EE en el datacenter.
- Competencia técnica en monitorización de redes eléctricas.
- Sistema de captura de datos eléctricos maduro.

Debilidades
- No se capturan datos de IT.
- No se relacionan métricas de las infraestructuras con las propias de IT.
- A pesar de que existen muchos dispositivos de medida de parámetros eléctricos, no están estructurados para la monitorización de las métricas de datacenter.
- No se capturan datos de funcionamiento de los sistemas de refrigeración.

Oportunidades
- El PUE es muy malo, pero puede conseguirse una mejora significativa aplicando medidas sencillas y económicas.
- Puede aprovecharse a mejorar la eficiencia mediante economías de escala simplificando salas.
- Puede aprovecharse a crear una instalación eficiente y de alta densidad para CPD principal, respaldo, cálculo científico y PdP.

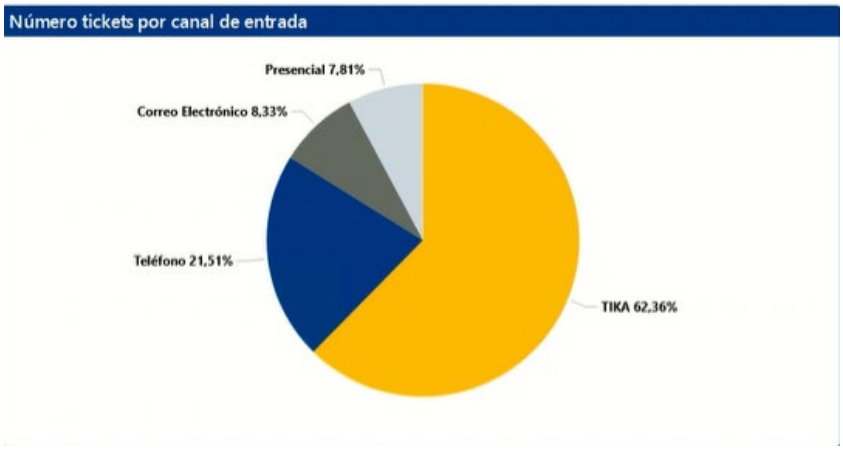
Amenazas
- La eficiencia es bajísima, lo que implica un riesgo desde el punto de vista regulatorio y reputacional.
- No existe un punto único de control para detectar y gestionar problemas en las infraestructuras del datacenter.

CENTRO DE SERVICIOS

Datos del servicio

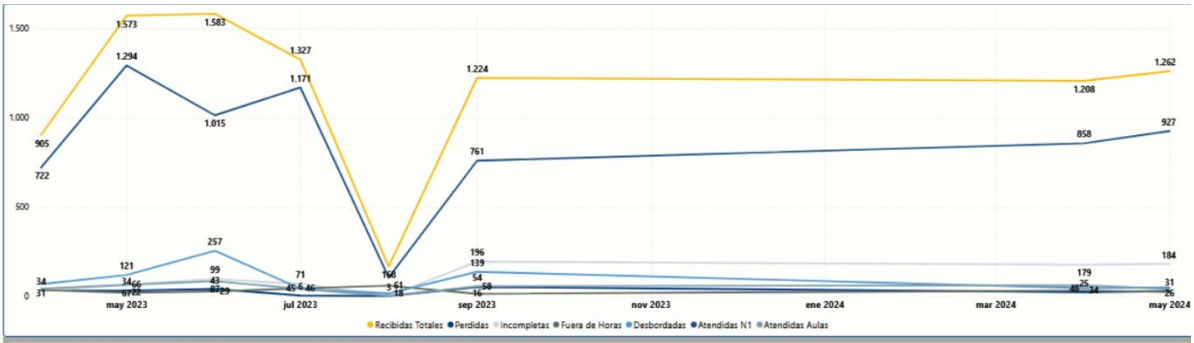
El Centro de Servicio (CS) ofrece una atención personalizada a la comunidad universitarias, siendo un servicio muy consolidado dentro del CIC. El pasado curso se produjeron cambios importantes en el personal adscrito al servicio, entre ellos el cambio del Service Manager.

El CS realiza un elevado número de actuaciones solicitadas por la comunidad universitaria, siendo la principal herramienta para realizar las solicitudes TIKA, seguido de las llamadas telefónicas.



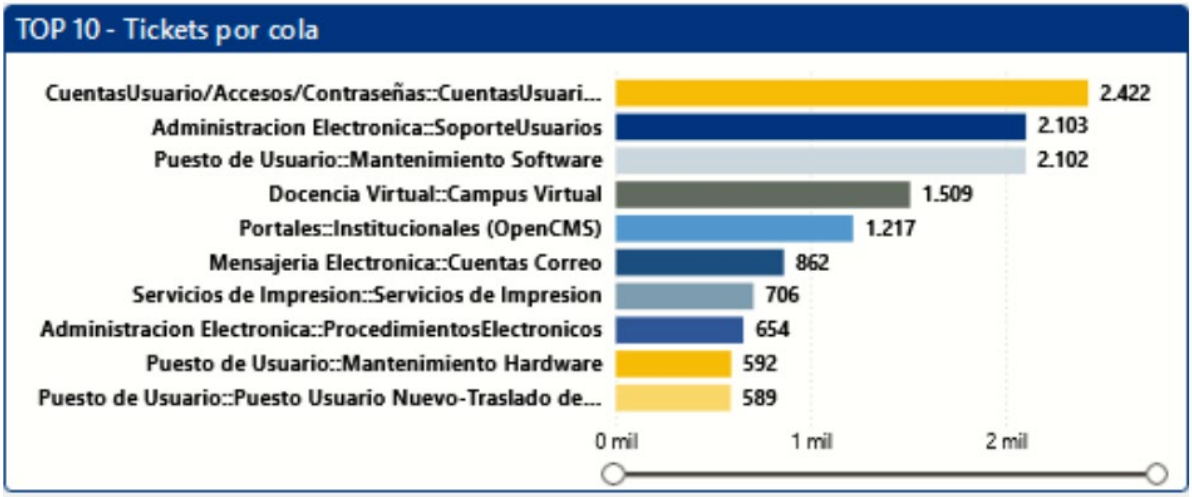
Tickets creados: Tras un ligero incremento de tickets en los meses anteriores respecto al curso pasado, debido entre otros factores, a la doble realización de PAROE (antiguo PLAN renove), se observa una disminución importante, fruto de la madurez del servicio tras los cambios del curso anterior.

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



Año, Mes	Recibidas Totales	Perdidas	Incompletas	Fuera de Horas	Desbordadas	Atendidas N1	Atendidas Aulas
2023, abril	905	34	31	37	70	722	45
2023, mayo	1.573	34	67	22	121	1.294	66
2023, junio	1.583	43	99	29	257	1.015	87
2023, julio	1.327	6	71	46	45	1.171	43
2023, agosto	168	3	3	61	18	107	5
2023, septiembre	1.224	54	196	16	139	761	58
2024, abril	1.208	25	179	34	48	858	64
2024, mayo	1.262	31	184	26	51	927	43

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

En este apartado se describen las actuaciones llevadas a cabo en el Espacio Multimedia del CIC. Este departamento gestiona:

- 7 salas de grado de la Universidad,
- 4 seminarios y salas de reuniones en Rectorado,
- 4 laboratorios de docencia avanzada,
- 118 aulas de docencia en su vertiente audiovisual,
- 2 aulas Digitales,
- 50 espacios de docencia adicionales (seminarios, laboratorios, etc.).

Las actividades llevadas a cabo este año se resumen en lo siguiente:

- La actividad práctica (EPD) de la asignatura "EQUIPAMIENTOS E INSTALACIONES DEPORTIVAS" del grado "GRADO EN CIENCIAS DE LA ACTIVIDAD FÍSICA Y DEL DEPORTE", supone la revisión de seguridad de entornos deportivos, tipo pabellones multiuso, pistas de futbol y baloncesto o estadios de futbol. Estas revisiones por parte de los alumnos se realiza de forma virtual mediante Gafas de Realidad Virtual (Meta Quest 2) y los entornos creados ad-hoc por la Universidad Católica de Murcia en el espacio virtual Spatial. El Centro de Informática apoya dicha práctica mediante un técnico que se encarga de preparar las gafas y activar los entornos virtuales, así como de "reflejar" lo visualizado por el alumno en otro dispositivo móvil para que un compañero de dicho alumno, pueda guiarle en los checks propuestos por el profesor a revisar. Se explica a cada alumno el funcionamiento de las gafas y de la experiencia Virtual y se atienden distintos problemas o dudas. Durante la sesión es necesaria la revisión continua del funcionamiento y de la carga de baterías de gafas, mandos y dispositivos móviles. Se disponen de 5 gafas y 5 dispositivos móviles en un entorno especial, la Sala de Aprendizaje Activo del Edificio 7, cuyo espacio y disposición es idóneo para este tipo de experiencias y prácticas, al disponer de tomas de carga y sistema WIFI dedicada. Las sesiones se dividieron por grupos de alumnos y sesiones según su curso. En total se asistieron a unos 100 alumnos divididos en grupos de 2 horas cada uno, a lo largo del día, mañana y tarde.

- Enmarcado en la línea 1.5. Digital Workplace del Plan de Transformación Digital, se ha realizado un piloto de Tecnificación de dos aulas de docencia en el edificio 14. Este proyecto ha consistido en la

instalación de dos pantallas interactivas digitales en conjunción con el departamento de IMEE, que ha realizado la mejora en otros aspectos del aula (comodidad, electrificación entre otras), y eliminación de la pizarra tradicional de tiza, quedando únicamente la pantalla interactiva como apoyo a los profesores, permitiendo también la realización de docencia dual como venia siendo hasta ahora.

- Para la continuación del proyecto anterior, se han realizado pruebas de conceptos de diferentes modelos de pantallas interactivas digitales, con diferentes fabricantes, para realizar evaluaciones de las actualizaciones que se van produciendo, al objeto de poder seleccionar las mejores en el avance de la nueva digitalización de las aulas.

- Se han realizado instalaciones para realizar videoconferencias en diversos despachos y salas de reuniones, con la instalación de pantallas y cámaras, complementándolos con dispositivos que facilitan el uso.

- Se ha realizado la desinstalación del material multimedia de la Sede Centro, quedando este material guardado a la espera de su instalación en la nueva sede del Pabellón de Marruecos.

- En este curso se ha dotado a las pantallas de cartelería existentes en la UPO la posibilidad de recibir streaming realizados desde el Paraninfo, pudiendo de esta forma proyectar en ellas los actos realizados desde allí para que puedan ser visualizados por la comunidad universitaria en general.

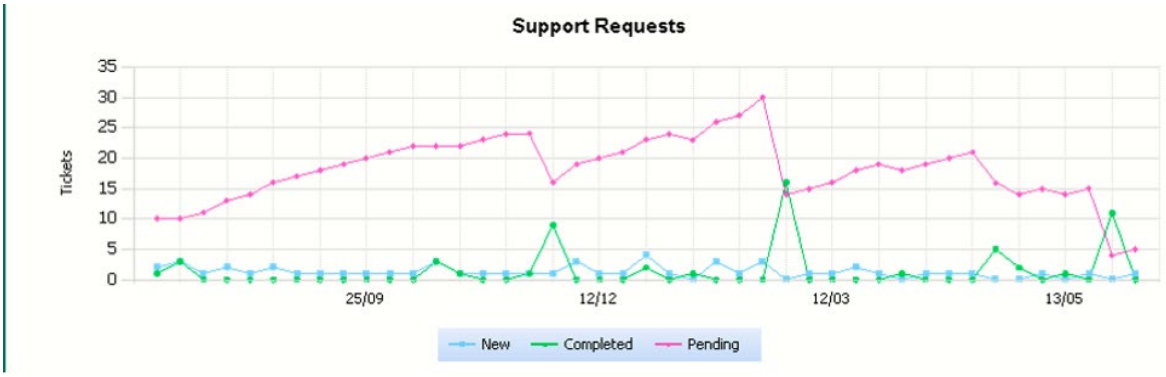
También desde este departamento se llevan temas diversos, como gestión de llaves y tarjetas de apertura inteligentes. En este sentido ha habido un total de 8 actuaciones.

MyAPPS

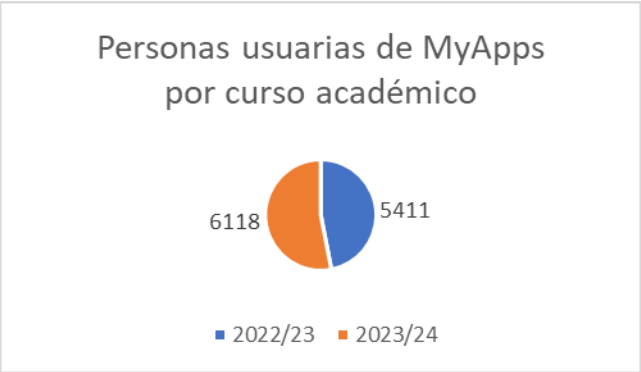
El servicio de aplicaciones de aulas de informática en la nube MyApps se ha consolidado como el servicio por excelencia para la realización de las prácticas del estudiantado y para la celebración de exámenes. Sigue un año más creciendo en uso como parte del entorno educativo de la UPO. Este servicio permite acceder a las aplicaciones y escritorios a través de un navegador, con la facilidad de HTML5 que permite su uso universal de forma sencilla y es ideal para el estudiantado, que no tiene que instalarse nada en sus dispositivos.

Las dos aplicaciones más utilizadas en MyApps siguen siendo, un año más, SPSS y Mathematica.

Al ser un servicio tan consolidado, cada vez es menor el número de incidencias reportadas al proveedor, siendo la mayoría de ellas requerimientos de actualizaciones del software existente o nuevas instalaciones solicitadas por el personal docente.



El número de personas usuarias en MyApps también ha crecido notablemente, como se puede apreciar en la siguiente gráfica:

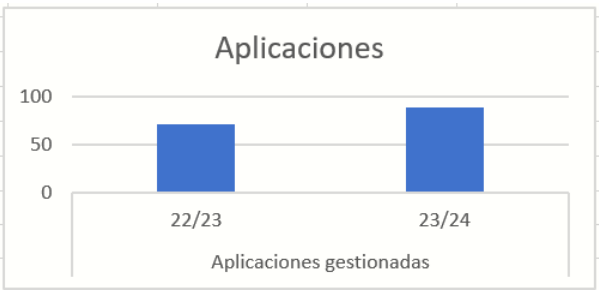


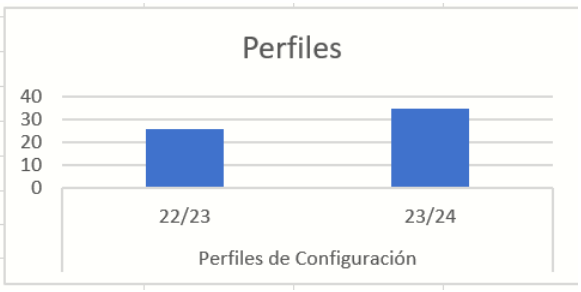
Equipamiento, Aulas y Laboratorios

*** Puesto de trabajo**

Como sistema de gestión del puesto de usuario se utiliza el producto Intune de Microsoft. Este sistema permite, de forma centralizada, la gestión y administración de puestos de trabajo, tanto equipos fijos como equipos móviles para teletrabajo.
El número de aplicaciones disponibles en Intune, incluyendo las utilizadas por personal de la Universidad y las instaladas de forma exclusiva en aulas de informática y docencia asciende a 89. Estas aplicaciones se distribuyen en remoto a través de Intune, facilitando la gestión y acortando el tiempo de instalación.

Los perfiles de configuración gestionados desde Intune son actualmente 35, esto permite realizar cambios de forma remota y desatendida en determinados equipos, sin necesidad de que un técnico tenga que configurar equipo a equipo de forma manual. Estos perfiles determinan las características de un determinado grupo de trabajo.





Intune es una suite de servicios compleja, por lo que la incorporación de Intune se ha ido realizando progresivamente, teniendo en la actualidad 1513 puestos de trabajo fijos y móviles gestionados con Intune.

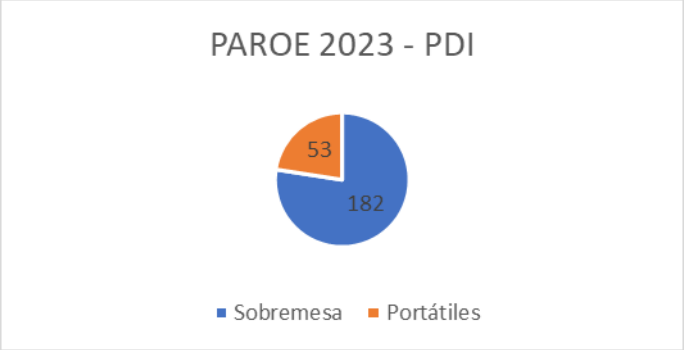
PAROE 2023

Tras el periodo de transición que significó el Renove 2021 y Renove 2022 (incorporación de Intune; gestión de inventario con Listas, Formularios y Teams; Sistema Dinámico de Adquisiciones), se ha terminado de ejecutar el PAROE 2023 (Procedimiento de Adquisición, Renovación y Optimización de Equipos Informáticos Corporativos).
Los dos cambios más significativos en este nuevo modelo son:

a) el CIC se encarga de asumir el coste íntegro de todo el equipamiento
b) todos los equipos se renuevan, los Departamentos solo tienen que indicar el docente al que va destinado cada equipo

Esto ha permitido eliminar del parque la práctica totalidad de equipos asignados a PDI con una antigüedad mayor de 5 años.

En el PAROE 2023 se han sustituido 235 ordenadores de PDI, 182 PCs de sobremesa y 53 portátiles. A continuación, se muestra una gráfica con el reparto de instalaciones del PAROE 2023 según el tipo de dispositivo.



Renove 2023

A partir de la entrada en vigor del PAROE, la denominación 'Renove' se utiliza solo para hacer referencia a la sustitución de equipos en Aulas.

En el Renove 2023 han sido sustituidos 99 equipos

Los equipos recuperados tanto del PAROE como del Renove, se destinan a actualizar los asignados a tareas que requieren menos prestaciones: Laboratorios, Seminarios, Conserjerías, Cartería, Puntos de Información, etc. De este modo, se logra extender el periodo de amortización como mínimo hasta los 8 años.

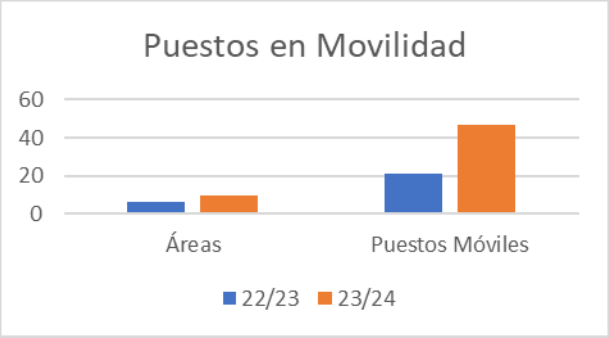
Puesto de Usuario/a Móvil

Continuando con las acciones llevadas a cabo en el Plan de Transformación Digital, encontramos la acción '1.5.1: Facilitar el teletrabajo', enmarcada en la línea '1.5. Digital Workplace'. En este sistema se crea el entorno de Puesto de Usuario/a Móvil, que se ha iniciado en diferentes áreas del PTGAS, consiste en sustituir el equipo local (normalmente sobremesa) por un equipo portátil y una pequeña dock a la que se conectará la pantalla, teclado y ratón, de modo que la experiencia de usuario/a no cambie respecto al uso del Pc de sobremesa.

Esta nueva configuración permite al usuario utilizar este mismo portátil en casa, en lugar de requerir un equipo adicional (propio, o proporcionado por la Universidad) con el que conectarse por VPN a su puesto de trabajo en la UPO.

Con este nuevo modelo, el portátil debe estar preparado para acceder a los mismos servicios, tanto desde dentro como desde fuera de la Universidad.

El número de áreas que actualmente utilizan este nuevo sistema es de 10, con un total de 47 puestos, como puede verse en el gráfico que se muestra a continuación:



Base de datos de inventario.

Se ha consolidado la base de datos de equipamiento informático, ubicada en Sharepoint para su gestión y exportada de forma diaria para ser consultada por los Departamentos.

En esta base de datos se tiene información de ubicación, estado, asignación, etc. de los siguientes elementos: PCs sobremesa (2534), PCs portátiles (725), Dock Stations (64), Monitores (193)

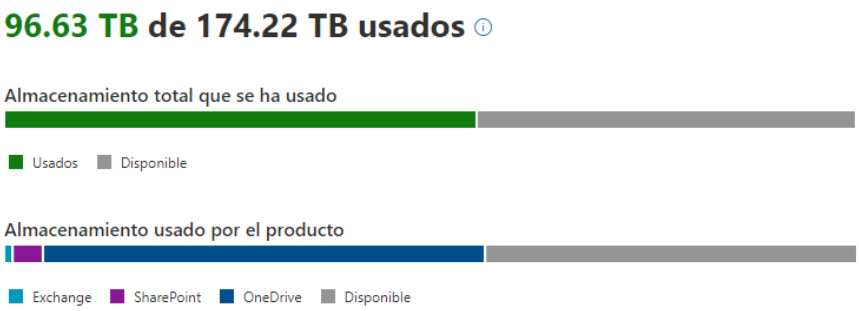
Samba – Sharepoint - Onedrive

El servicio de compartición de ficheros utilizado en PAS, se mantiene bastante estable, tanto en espacio ocupado como en número de usuarios y grupos.
Espacio ocupado 4.1 TB
Número de Grupos 134
Número de Usuarios 607

Dado que este sistema de gestión de archivos es algo obsoleto, en aquellas áreas que pasan al modelo de Puesto Móvil, se están migrando los contenidos a Sharepoint.

El incremento de la capacidad disponible, las facilidades de recuperación de datos perdidos y la posibilidad de acceder a la información desde cualquier ubicación, han sido claves a la hora de optar por este sistema.

Por otra parte, se está haciendo extensivo el uso de Onedrive como sistema de almacenamiento personal.



BSCW

La herramienta de trabajo Colaborativa BSCW es utilizada por PDI, PAS y Alumnos de Postgrado.
Usuarios registrados 8656
Volumen de datos 2,9 Tb

La versión actual de esta herramienta está discontinuada, y el fabricante ha pasado a comercializarlo como servicio de pago en la nube. De ahí que se está planteando sustituir este servicio por Sharepoint.

*** Licencias Campus**

Se han adquirido licencias Campus del software: Matlab, ArcGis Pro y ArcGis Online.

El número de usuarios con acceso a Microsoft 365 (antes Office 365) es de 22.694 teniendo asignadas las siguientes licencias.

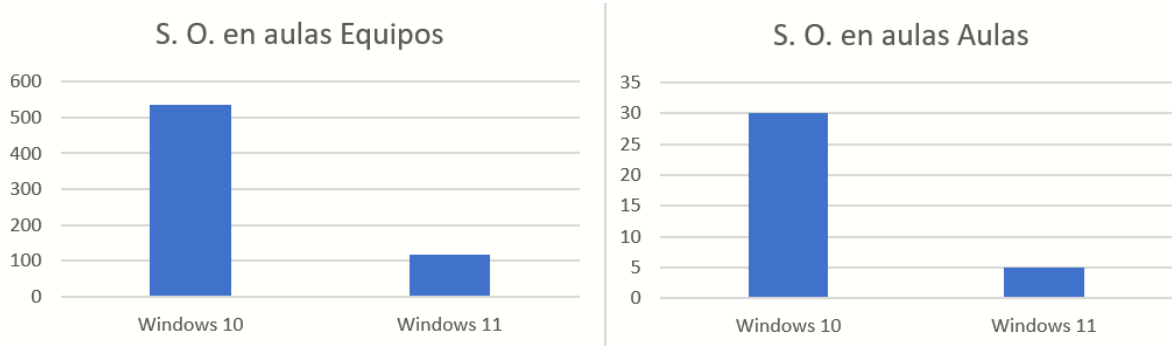
*** Aulas**

Los equipos incluidos en el Renove 2024 de aulas (99 PCs) ya corren sobre el sistema operativo Windows 11.

Este mismo año está prevista la renovación de otros 136 equipos que tienen aún disco duro mecánico y solo 8 GB de memoria.

Se continúa con la transición a Windows 11 en los equipos cuyo hardware permite que este SO se ejecute con cierta fluidez.

SO Windows 10 -- 30 aulas y 536 equipos
SO Windows 11 -- 5 aulas y 117 equipos



*** Atención a Escuela Politécnica**
La atención a la Escuela Politécnica se resume de la siguiente manera:

- Solicitudes para asignaturas por parte del cuerpo docente: 40
- Cambios en la configuración de la red asignada a la escuela: 4
- Actualizaciones de software de los laboratorios de la escuela: 9
- Actuaciones de hardware: 6

GESTIÓN DE SEGURIDAD

Descripción de tareas seguridad de la información

Política, normas, procedimientos e informes

En el curso 2022/2023 se realizó una revisión de la Política de Seguridad de la Información y Protección de Datos con el fin de adaptarla al 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. Desde entonces se está a la espera que se realice una

revisión de los aspectos de protección de datos, a propuesta del Delegado o Delegada de Protección de Datos, para que la Comisión de Seguridad y Protección de Datos pueda dar su conformidad a la nueva versión y elevarla al órgano de gobierno para su aprobación.

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.

Se han generado los siguientes informes:

- INF_CIC-16_Subred23_v.1.1.docx procedimiento de gestión de subred de pruebas
- NF_CIC-16_Cronos_v.1.0.docx. Análisis de riesgos de integración de aplicación Cronos
- INF_CIC-16_SoporteEquipos_v.1.0.docx Clasificación y soporte de equipos informáticos.
- INF_CIC-16_vlan200.docx. Informe de incidentes subred de CS/alianzas externas
- INF_CIC-16_ENS_log_v.1.0.docx referencias normativas explícitas del ENS en materia de registro de actividad o log
- INF_CIC-16_ENS_equipocliente_v.1.0.docx Informe medidas de seguridad ENS que aplican a equipos clientes.
- INF_CIC-16_reconfparoe_v.1.0.docx Análisis de riesgo equipo arranque dual
- INF_CIC-16_VPN_Econocom_v.1.1. Análisis de riesgo VPN de Econocom
- INF_CIC-16_WifiFT_v.1.1.docx. Análisis de riesgos usuarios wifi genéricos Flora Tristán
- INF_CIC-16_labbib_v.1.1.docx Análisis de riesgos laboratorio multimedia biblioteca.
- INF_CIC-16_DptoGHF_v.1.1.docx Análisis de riesgos equipo Departamento Geografía e Historia
- INF_CIC-16_ENS_contratacion_v.1.0.docx. Requisitos cumplimiento contratación.

Comisión de Seguridad de la Información y Protección de Datos

Durante el curso 2023/2024 no se ha reunido la Comisión de Seguridad y Protección de datos.

Tras el cese del anterior Delegado de protección de datos, la figura de Delegado de Protección de Datos se ha contratado como servicio a una persona externa a la organización.

Desde el Centro de Informática se ha promovido una reunión con la Secretaría General para abordar temas que afectan a la seguridad de la información en relación con el DPD. Entre otras cosas:

- Revisión de la política de seguridad y protección de datos.
- Colaboración en materia de incidentes de seguridad y brechas de seguridad.
- Colaboración en análisis de riesgos que afecten a datos personales.
- Informe de brechas de seguridad.
- Revisión de la organización de la seguridad por si hiciera falta modificar la política en relación con la nueva figura de DPD.

Se mantiene una primera reunión con la secretaría General y una segunda reunión con la delegada de Protección de Datos el 3 de junio. Se establece la forma de contacto y se le facilita la normativa de seguridad propia en relación con la protección de datos personales, así como informe de brechas de seguridad.

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 2023.2.2 (22.11.2023), 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): 4,5 (escala 0-10) – MUY ALTO.
- Riesgo presente máximo (con las salvaguardas aplicadas actualmente): 3,0 (escala 0-10) – ALTO.

Se genera la siguiente documentación:

- Informe ejecutivo INF_CIC-16_analisis_de_riesgo_2024.doc.
- SOA_Declaración de Aplicabilidad de Medidas del ENS_2024.
- Fichero de análisis de riesgo 2024.

Se genera también el valor del indicador de gestión de la seguridad establecido en marco con un valor de 2,2. 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 267 incidentes de seguridad.

	origen	Número	%
Externo			
Andalucía CERT	ACERT	1	0,37
INCIBE-CERT	INCIBE	5	1,87
CCN-CERT	CCN-CERT	0	0
Proveedores con sistemas externos	PRO	0	0
Proveedores con sistemas en la UPO	PRU	0	0
Ciudadanos	CIU	0	0
Auditorías	AUD	1	0,37
Interno - Sistemas detección automática			
Servicio Antivirus	VIR	16	5,99
Sonda SAT-INET	SAT	48	17,98
Servicio Antispam	SPA	40	14,98
Otros servicios de monitorización	MON	15	5,62
Interno - Personal UPO			
Responsables UPO	RPS	7	2,62
Personal upo	USR	123	46,07
Interno - Personal CIC			
Jefe de gestión de seguridad	JGS	1	0,37
Dirección del CIC	DIR	5	1,87
Administradores de sistemas CIC	ADM	2	0,75
Otros	OTR	3	1,12

Las auditorías por lo general encuentran hallazgos que son vulnerabilidades y así se registran en el sistema. Pero en ocasiones puede detectarse hallazgos que son en sí un incidente de seguridad. El incidente contabilizado en relación con auditoría consistió en la localización de un equipo de trabajo de personal técnico TIC ubicado en una subred de pruebas sin que estuviera autorizado. Esto constituye un incidente de seguridad por incumplimiento de procedimiento. La subred de pruebas y la subred de trabajo del personal del CIC tienen configuraciones de seguridad diferentes. Este dispositivo carecía de las medidas de protección adecuadas y podía usarse para actividades restringidas en otros equipos.

En general se mantiene la tendencia a una disminución de los incidentes de seguridad. Esto puede atribuirse a varios motivos:

- Mayor concienciación de usuarios/as.
- Mejora en la protección perimetral y control de la superficie de exposición.
- Retirada de equipos y sistemas obsoletos que generaban alertas de seguridad.

- Mayor control de equipos expuestos.
- Mayor actualización de sistemas y corrección de vulnerabilidades.
- Mayor rigor en los procesos de autorización.
- Mejoras en el servicio de LAVADORA de RedIRIS.

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.
- Mejora en la configuración de sistemas de detección automática de correos se spam y envío directo a zona de cuarentena.
- Incremento en el número de equipos protegidos por antivirus profesional.

Las auditorías que se han realizado en el curso han generado un gran volumen de gestión que ha requerido mejoras en la herramienta de registro y seguimiento. Se ha modificado esta base SEGSERV para que permita registro y seguimiento de cada vulnerabilidad, así como la emisión de informes.

Se pone de manifiesto nuevamente la necesidad de una mejora en la gestión de vulnerabilidades para evitar incidentes en máquinas expuestas. Además, se hace necesaria la retirada de sistemas obsoletos y no mantenidos. Se hace necesaria también una gestión con los/as proveedores/as para instar a la corrección de vulnerabilidades detectadas por los sistemas de vigilancia.

Notificación de incidentes

Durante el año analizado no se ha procedido a la notificación oficial al CCN-CERT ya que no se han registrado incidentes de nivel alto.

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 detectados en sus sistemas con un total de 6 (OCU, fundación, Econocom y empresa proveedora página de la OTRI).
- Denuncias a organizaciones desde cuyos sistemas se estaban recibiendo ataques con un total de 11 notificaciones (Gmail, Universidad de Granada y Junta de Andalucía).

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 2023/2024 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.

El EDR deberá ofrecer 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

Campañas de concienciación

Durante el periodo que abarca esta memoria se han concluido las campañas de concienciación cuya puesta en marcha estuvo recogida en la memoria anterior.

- Campaña de SIMULYCON de RedIRIS destinado a 1060 personas del colectivo PDI. Esta campaña consiste en una evaluación inicial, unos contenidos formativos y un conjunto de simulacros de phishing para determinar la vulnerabilidad del colectivo.
- Campaña con la empresa Entelgy destinada a personal no docente con un total de 400 participantes. Esta campaña consiste en seguir unos contenidos que exponen tres casos reales de incidentes de seguridad y explican al/la participante cómo prevenirlos. Es una campaña pensada para entrenar en la detección y respuesta ante incidentes de seguridad.

Se han realizado los informes de cierre de cada una de las campañas:
- INF_CIC-16_concienciacion_entenlgy_2023_v.2.0
- INF_CIC-16_concienciacion_redIris_2023_v.1.0.docx

Los resultados generales son:

SYMULYCON:

Resultados de formación peramente	
Total de participantes	1063
Total de personas que han iniciado la formación	250 (24% del total)
Total de personas que no inicia la formación (0% ejecución)	813 (76% del total)
Total de personas que inician y completan la formación	76 (7% del total y 30 % de los que han accedido)
Total de personas que inician y No completan la formación	174 (16 % del total y 70% de los que han accedido)

ENTELGY:

Total de participantes	433
Total de personas que han iniciado la formación	218 (51% del total)
Total de personas que no inicia la formación (0% ejecución)	215 (49% del total)
Total de personas que completan la formación (>= 80 % ejecución)	131 (30% del total y 60 % de los que han accedido)
Total de personas que No completan la formación (< 80 % ejecución)	87 (24% del total y 40% de los que han accedido)
Total de personas que con adherencia (*) a la campaña (>=60% ejecución)	142 (33% del total y 65% de los que han accedido)

(*) El 60% del contenido lo conforman los bloques importantes de formación (excluye test y videos finales)

Taller de concienciación

Se ha preparado y realizado una formación de 3 horas para impartir a colectivos de la Universidad. Se ha comenzado con un piloto para Centro de Servicios a usuarios y usuarias y alianzas externas del CIC. Ha consistido en dos sesiones presenciales de 3 horas para que todo el personal de estas empresas pudiera asistir sin afectar a sus servicios.

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 ha hecho campaña de concienciación en aquellos usuarios con quejas para explicar:

- las necesarias demoras en algunos procedimientos para cumplir con los requisitos de seguridad
- la necesidad de 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

Durante este curso académico se ha completado el lote 2 de la licitación del proyecto CONSEG de UNIDIGITAL, liderado por la US, en el que se han creado contenidos creados para concienciar en el ámbito de las universidades.

Durante el mes de junio de 2024 se espera finalizar el lote 1 con el despliegue de las instancias de la plataforma que permitirá diseñar y operar campañas de ciberseguridad donde puedan ponerse a disposición contenidos o realizar campañas de phishing.

Ponencia ciberseguridad

En el marco del Seminario sobre gestión pública universitaria 2024, realizado en abril se desarrolla una ponencia a cargo de Belén Prados Suárez, doctora en Informática y profesora titular del Departamento de Lenguajes y Sistemas Informáticos de la Universidad de Granada, “Univers-IA: fraudes, valores, retos y oportunidades”, donde se abordan los nuevos riesgos de ciberseguridad asociados a la Inteligencia Artificial (IA).

Auditoría ENISA

La empresa externa, S2Grupo, en el marco de un proyecto auspiciado por la organización ENISA (Agencia de la Unión Europea para la Ciberseguridad, https://www.enisa.europa.eu/about-enisa/about/es, que se ha canalizado a través de la CRUE (Conferencia de Rectores de las Universidades Españolas) ha realizado una auditoría de seguridad. En la auditoría, se ha analizado la superficie de exposición de la Universidad en busca de vulnerabilidades. Las vulnerabilidades son la puerta de entrada que aprovechan los atacantes, por lo que mantenerlas abiertas nos debilitan y aumentan el riesgo de sufrir incidentes de seguridad. El impacto de un ataque en uno de nuestros activos pone en riesgo a toda la Universidad, ya que puede propagarse entre el resto de los activos.

En algunos casos los auditories han realizado explotación de estas vulnerabilidades, obteniendo acceso real a nuestros sistemas, obteniendo credenciales de acceso y accediendo a información sensible.

El Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de Mayo) nos responsabiliza como administración pública a implementar una serie de medidas y a adoptar una serie 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.

La auditoría constaba de tres fases:

- Auditoría externa: análisis de vulnerabilidades desde el exterior de la organización.
- Auditoría interna: análisis de vulnerabilidades conectados a la red de la universidad.
- Auditoría web: análisis de vulnerabilidades de sistemas web de la Universidad.

Como resultado de estos análisis se han encontrado un total de 54 vulnerabilidades que afectan a un total de 270 dispositivos.

Par abordar el registro y tratamiento de estas vulnerabilidades se está llevando a cabo un proceso de:

- Registro en herramientas internas.
- Localización de equipos y sus responsables.
- Elaboración de informes.
- Notificación a los responsables.
- Seguimiento de las acciones.
- Cierre de vulnerabilidades cuando son resueltas.

El proceso se está abordando atendiendo a la criticidad de las vulnerabilidades encontradas. Se están presentando distintos tipos de cierre:

- Cierre por restirada o sustitución del equipo.
- Cierre por mitigación de vulnerabilidades aplicando actualizaciones y correcciones sugeridas.
- Seguimiento a medio plazo pendiente de retirada de equipo sin mantenimiento.

Las acciones más comunes para mitigar las vulnerabilidades están siendo:

- Actualización de aplicaciones y sistemas operativos.
- Configuración segura de servidores web:

  - Incluir cabeceras *https response* de seguridad.
  - Eliminación de cabeceras https con información sobre sistemas.
  - Eliminación de permisos de acceso a archivos del servidor web.
  - Eliminación de configuración y archivos por defecto
- Eliminar protocolos obsoletos para el encriptado de comunicaciones seguras.
- Eliminación de plugins vulnerables.
- Eliminación de funcionalidad no necesaria.

Los responsables de los dispositivos son: personal del CIC, personal de la Universidad a cargo de dispositivos no gestionados por el CIC, personal externo a la universidad (fundación, CABD, etc.) y proveedores externos de servicios TIC.

PILOTO ELSA

Durante el primer trimestre de 2024 la Universidad Pablo de Olavide ha sido seleccionada por la CRUE-TIC mediante procedimiento de sorteo, para participar en el proyecto del piloto de la herramienta ELSA del CCN-CERT. ELSA (Exposición Local y Superficie de Ataque) es la solución de análisis de exposición desarrollada por el CCN-CERT que permite la monitorización a nivel nacional de todos los activos conectados a Internet para detectar posibles vectores de ataque y vulnerabilidades de todo organismo o entidad de la administración pública, con el objetivo de mejorar la capacidad estatal de respuesta ante incidentes.

Durante el piloto la Universidad ha podido acceder a la plataforma web de ELSA y ha revisado los datos recopilados. Se ha mantenido un contacto con el equipo de desarrollo de la herramienta para notificar incidentes detectados y propuestas de mejora sobre todo en relación con la gestión de la información que facilita la herramienta.

Esta herramienta ha permitido:

- Reducir la superficie de exposición eliminando 3 sistemas que permanecían expuestos al exterior
- Comunicar informe de vulnerabilidades críticas y su corrección para un sistema alojado fuera de las instalaciones de la Universidad.

Se ha reportado la experiencia en las reuniones mensuales de la CRUE-TIC.

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.

RED Nacional de SOC

En Noviembre de 2023 la Universidad quedó adherida a la Red Nacional de SOC [RNS]. La Red Nacional de SOC (RNS) es la plataforma que integra los SOC de todos los organismos públicos de la Administración, junto con las entidades proveedoras que prestan dichos servicios de SOC y las entidades públicas que se benefician de los mismos.

Su objetivo principal es impulsar la capacidad de protección de sus miembros mediante el bloqueo casi inmediato de cualquier indicio de actividad anómala que se esté detectando en cualquier punto de la Administración.

Al no disponer de SOC la universidad colabora en calidad de invitada. Recibiendo la información que difunda la RNS y el acceso a las herramientas que facilite.

Reyes

En noviembre de 2023 la Universidad se ha suscrito al servicio de REYES del CCN-CERT. REYES es una solución desarrollada por el CCN-CERT para agilizar la labor de análisis de ciberincidentes y compartir información de ciberamenazas. Es una herramienta de investigación y análisis de ciberamenazas y ciberincidentes para el intercambio de ciberinteligencia.

A través de este portal centralizado de información puede realizarse cualquier investigación de forma rápida y sencilla, accediendo desde una única plataforma a la información más valiosa sobre ciberincidentes. Una información contextualizada y correlada con las principales fuentes de información, tanto públicas como privadas.

Redtrust Gestión de certificados electrónicos.

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. Se detecta un riesgo asociado al uso de certificado de representante de la organización por personas diferentes al titular del certificado. El particular en:

- La distribución e instalación manual del certificado en equipos finales de usuarios autorizados lo que dificulta el mantenimiento y retirada del certificado cuando deja de ser necesario
- Falta de registros de acciones realizadas con el certificado.
- Imposibilidad de establecer políticas que controlen el acceso y uso de estos certificados.

Se hace necesario un sistema que permita gestionar la delegación de firma mediante certificados digitales en algunos procedimientos internos en los que se requiere la firma de autoridades de representación de la Universidad. RedTrust es una plataforma que permite gestionar y controlar el acceso y uso de estos

certificados, así como facilitar la trazabilidad de las acciones que se realizan ellos, garantizando las condiciones de seguridad necesarias y mitigando el riesgo asociado a este tipo de operaciones.

Se ha realizado un proyecto piloto en fase de pruebas tras lo que se ha procedido a la adquisición y despliegue. En estos momentos se encuentra en fase de despliegue, realizando las pruebas con los primeros usuarios.

Además de esta medida técnica, a nivel organizativo, se está elaborando un procedimiento que establezca los requisitos para el uso de los certificados y los procesos de autorización asociados.

Gestión de vulnerabilidades

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. Este curso académico se han incorporado las vulnerabilidades detectadas en los procesos de auditorías (ver apartado ENISA) y en las detectadas por las herramientas de detección de superficie expuesta.

Se han gestionado un total de 78 vulnerabilidades, muchas en relación con tecnologías de publicaciones de páginas web o de virtualización. De especial impacto ha sido la que afectaba a las máquinas desplegadas en entornos virtuales, lo que ha llevado un proceso coordinado de actuación en muchas de las máquinas soportadas por el CIC.

Se mantienen las acciones de seguimiento de sistemas operativos obsoletos que ya no tienen soporte de mantenimiento de actualizaciones de seguridad, quedando reducido a un conjunto pequeño y controlado de equipos cuya migración no garantiza la continuidad de los servicios que albergan. Para esto equipos se han tomado medidas alternativas como el apagado y encendido controlado o un mayor grado de aislamiento.

Realización anual del informe 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 32.12 %.
- Indicador de mejora continua 67.68 %.

No aparecen datos referidos a 2023 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%.

Se genera la siguiente documentación:

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

Tras el cierre de año del informe INES el resultado sectorial emitido por el CCN CERT ha despertado dudas entre las universidades que han detectado errores o ambigüedades. Se ha realizado un informe detallado de diferencias detectadas en el informe sectorial en relación con los datos INES de la UPO y que se ha enviado a la CRUE-TIC de seguridad quien ha canalizado las comunicaciones con el CCN-CERT.

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 cumplimentado en tiempo y forma la encuesta que permitirá la recopilación de datos para alcanzar los objetivos de este proyecto.

Servicio DNS Firewall de RedIRIS.

En Julio de 2023 la Universidad se incorpora al servicio DNS Firewall de RedIRIS. Un DNS firewall es una herramienta de seguridad, adicional y complementaria a los firewalls tradicionales y otras herramientas de inspección de tráfico, enfocado únicamente al tráfico DNS, y que se encarga de redirigir o bloquear el acceso de los usuarios finales a sitios maliciosos. RedIRIS pone a disposición de sus instituciones un servicio de DNS Firewall basado en la plataforma Cisco Umbrella, que tiene las siguientes características:

- Arquitectura cloud Anycast para garantizar la mayor disponibilidad posible y resiliencia ante fallos, con más de 30 nodos y alta dispersión geográfica.

- Servicio multitenant, de forma que cada institución puede personalizar el funcionamiento del servicio y obtener sus propias estadísticas de uso y alertas.

- Despliegue sencillo, ya que sólo es necesario reencaminar el tráfico DNS hacia los resolvers del servicio. (En el caso de querer estadísticas avanzadas, es necesaria la instalación de virtual appliance en la red de la institución usuaria del servicio).

FORMACIÓN

Actividades formativas específicas TI

Se presenta a continuación un resumen de las actividades formativas a las que ha asistido el personal del Área a lo largo del curso 2023/2024 y que son específicas de TI.

Las actividades que aquí se detallan no están incluidas dentro del Plan de Formación anual del PTGAS.

En este caso, se trata de actividades formativas derivadas de implementación de nuevos servicios, proyectos, despliegue de herramientas para la gestión propia de los servicios, etc… que conlleva una formación específica al personal TI.

Resumen de datos

- ✓ Nº actividades formativas distintas: 18
- ✓ Modalidad de actividad formativa:
  - Virtual: 18
- ✓ % participación personal CIC: 62,96 % (17 de 27)
- ✓ Nº horas formación TI 2023/2024: 210 horas, 15 minutos
- ✓ Coste total: 368,43 €

Detalle actividades formativas TI realizadas

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Administración electrónica básica	6,00	1
Concienciación en Ciberseguridad: The Firewall Mindset	3,00	10
Cooperar en equipos en red aprovechando las herramientas digitales	1,25	1
Creación y gestión de formularios web	6,00	1
Curso básico STIC - Seguridad en entornos Windows	15,00	1
Curso de Certificados Digitales	15,00	2
Curso de Seguridad de las Tecnologías de la Información y las Comunicaciones	30,00	1
Curso de Trazabilidad del Dato	10,00	1
Curso formación CAPA	1,00	1
Curso Introduccion a Kubernetes	40,00	1
Curso Introduction to Cloud Infrastructure Technologies	49,00	1
Gestión de Expedientes Electrónicos con G-TM	3,00	2
G-Forms: Definición de formularios	3,00	1
G-Settings: Consola de administración de la plataforma G-Once	3,00	3
Herramienta RedTrust	1,00	1
Model@: Definición de procedimientos electrónicos	3,00	1
STIC Amazon Web Service (AWS) en el ENS	20,00	1
The firewall mindset	1,00	1

Acciones formativas TI por participante

Participantes en 1 actividad formativa: 11
Participantes en 2 actividades formativas: 3
Participantes en 3 actividades formativas: 1
Participantes en 4 actividades formativas: 1
Participantes en 7 actividades formativas: 1
Personal que no participa en ninguna actividad formativa: 10

Otra formación

El personal del Área ha tomado parte en las siguientes actividades formativas de carácter general:

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Análisis de costes en los contratos públicos	20,00	1
Aprender a aprender	3,00	1
Atención al cliente	2,75	1
Atrévete con Excel	3,00	1
Cómo manejar los conflictos	3,00	2
Comunicación oral en ingles (Nivel B1). Módulo 1 al 5	50,00	1
Crecimiento personal y profesional con enfoque de género	4,00	4
Curso práctico sobre aplicación Marco	3,00	1
Gestión Lean	4,00	2
Gestionar la agresividad	3,00	1
Habilidades para el Teletrabajo	1,25	2
Inteligencia Artificial	4,75	1
Mapas mentales	6,00	1
Mejora tus competencias digitales	3,00	1
Microsoft 365: Powerpoint	3,00	1
Microsoft 365: Teams	3,00	12
Microsoft 365: Word	3,00	1
Optimizando la Colaboración: Trabajo Eficiente con Microsoft Teams y Office 365	3,00	3
Potenciando la colaboración: Videoconferencias con Microsoft Teams	2,00	1
Primeros auxilios	3,00	1
Puesta en práctica de una contratación pública estratégica y sostenible alineada con la Agenda 2030	15,00	2
Reuniones sensacionales	1,75	1
SCRUM	3,00	2
Sensibilización y detección de la violencia de género	8,00	2
Teletrabajo y Equipos Virtuales	3,00	2
Todo oídos: Cómo escuchar de forma activa	3,00	1
Todos a bordo	2,75	1
Trabaja desde casa	3,00	3
Trabaja en equipo con Microsoft 365	3,00	6
Trabajo en equipo: ¡todos a una!	3,00	2
Un proyecto de diez	3,00	1

Otras actividades

Además de las acciones puramente formativas, el personal del Área ha participado en las siguientes actividades:

- ¿Qué es el CPSTIC (CCN-STIC-105) y qué valor aporta?
- 47ª Jornadas CRUE Digitalización
- 48ª Jornadas CRUE Digitalización
- Acceso seguro a dispositivos de almacenamiento externo USB Confirmación
- Amazon web Services (AWS) y el emprendimiento en educación: soluciones para universidades en la era de la IA generativa
- Commscope: Subsistema horizontal
- Commscope: Tipo de cableado estructurado
- Desayuno tecnológico Secure&IT - Sevilla
- European Learning Model (ELM)
- Evento Innova360, Dos Hermanas
- Gestión de la regulación (NIS2, DORA, ENS)
- III Jornadas Anticorrupción
- IV Jornadas Presenciales de CertiDigital “Integrando CertiDigital en el entorno universitario”
- Jornadas IDENTI::SIC
- La protección de datos moderna
- Low-Code como acelerador de las AAPP
- Modernización de las infraestructuras de Red en Universidades
- Nueva Sede Electrónica UPO
- Nuevos Sistemas de Identidad Digital en la AAPP: Identidad Digital Autogestionada
- Requisitos de seguridad exigibles a proveedores. ENS y RGPD
- Riesgos y responsabilidad en la IA
- Seminario Gestión Pública Universitaria. Integridad Institucional: abordando el fraude en la gestión universitaria
- Sesión de concienciación sobre ciberseguridad
- Soluciones UEM/MDM con dispositivos seguros
- V Jornadas Digitales Certidigital. Ampliando Horizontes
- VI Jornadas FOLTE. La universidad de hoy: una visión integrada de la tecnología y la pedagogía
- Webinar Blackboard Learn Ultra y la revolución de la IA: Simplificando la creación de contenidos educativos
- Webinar 5 razones principales por las que Blackboard Learn Ultra es único
- Webinar Blackboard Data: Analítica de Formación para la toma de decisiones
- Webinar Blackboard Learn Ultra Office Hours
- Webinar Class para Microsoft Teams: La nueva generación de aulas virtuales
- Webinar EvalCOMIX y GradeScope para la Evaluación Educativa
- Webinar La ética en el uso de la inteligencia artificial
- Webinar OCU Compartir y priorizar mejoras de UXXI a través de QUATERNI XXI
- Webinar Optimizando la Experiencia Educativa: Integración de Microsoft y Google en Blackboard Learn Ultra

- Webinar Tiempos de IA generativa en Educación Superior
- Webinar Transformando la Evaluación online: Explorando las posibilidades de Flexible Grading en Blackboard Learn Ultra
- Webinar Zero-trust: Una visión 360° desde el punto de vista de la identidad
- Webinar: API de LUCIA e integración
- Webinar: metaOLVIDO: Gestión y tratamiento automático de metadatos
- Workshop Certidigital para equipo de gobierno
- Workshop Certidigital para equipo técnico (API)
- Workshop Certidigital para equipo técnico (Arquitectura)
- Workshop Microsoft – Protección en contra amenazas
- XVII Jornadas STIC CCN-CERT