

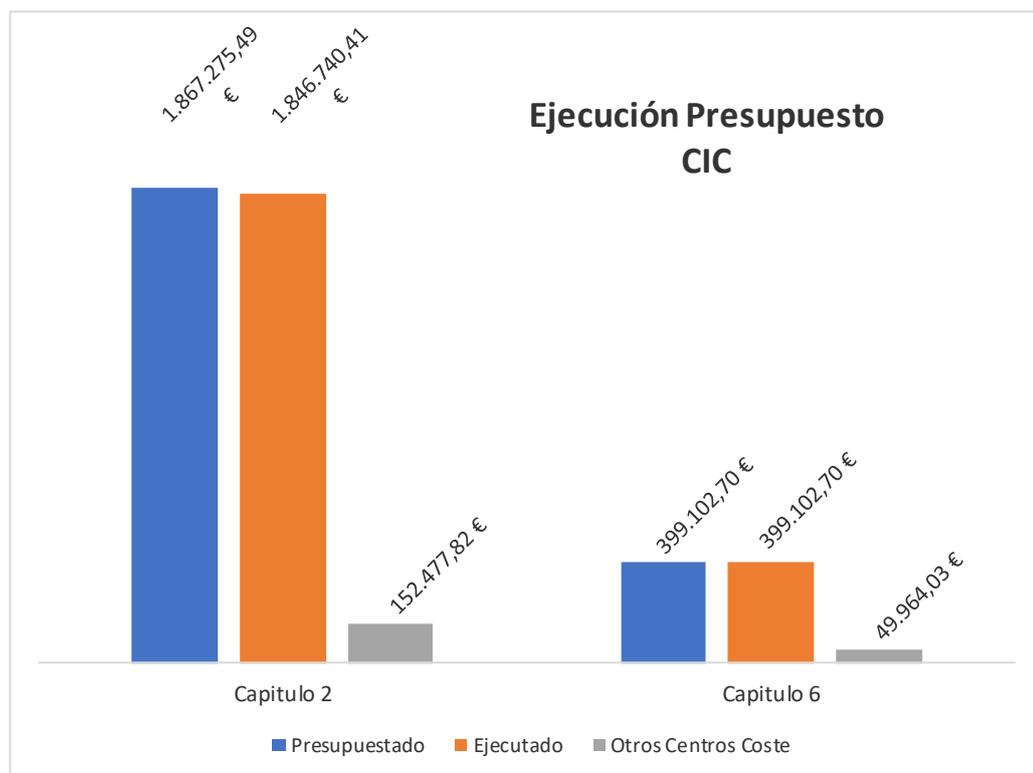
GESTIÓN ADMINISTRATIVA

Gestión Económica

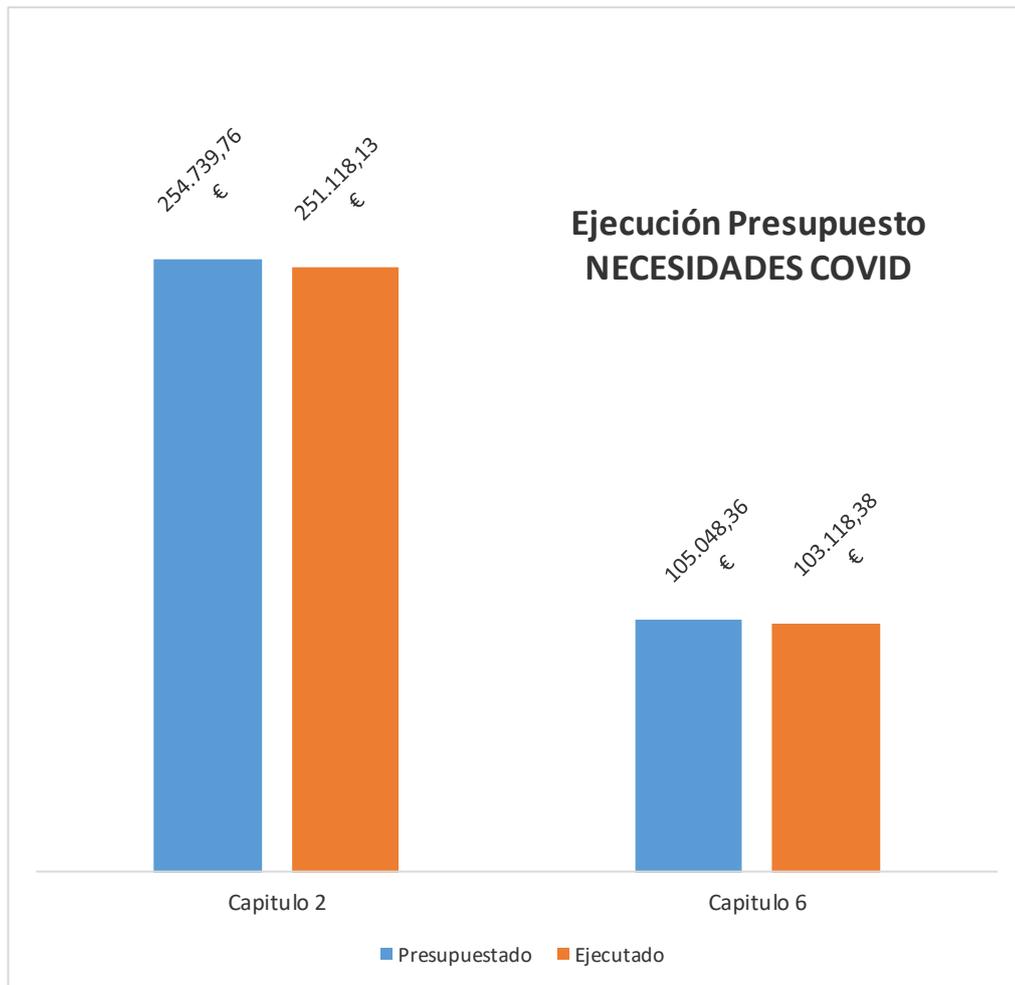
Las tareas relacionadas con la contratación de servicios y suministros son las que suponen una mayor carga de trabajo para la Oficina de Gestión Administrativa.

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 2022.



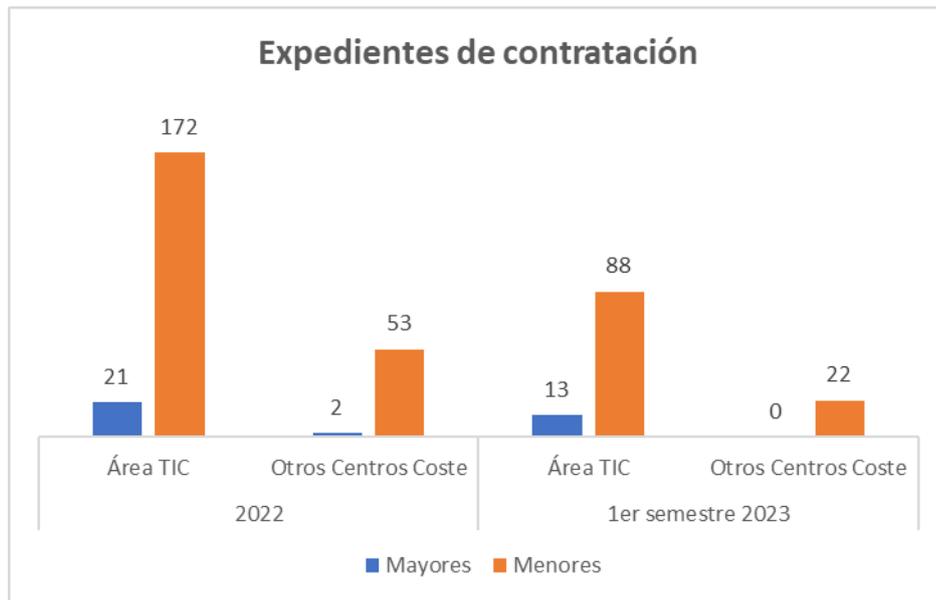
Con motivo de la pandemia de COVID-19 y para atender a las necesidades específicas en materia de equipamiento derivadas de la misma se dota al Centro de Informática de un centro de coste económico diferenciado, cuyo grado de ejecución en el ejercicio se muestra en el siguiente gráfico:



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 recaer sobre el presupuesto del Área, desde esta 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 2022 y el primer semestre de 2023.



Estos expedientes de contratación han generado la tramitación de 326 justificantes de gasto durante el ejercicio 2022 y de 149 durante el primer semestre de 2023.

Las contrataciones de inversiones con cargo al capítulo 6 han supuesto la tramitación en el año 2022 de 1.384 fichas de inventario y de 656 en el primer semestre de 2021

Otros trámites administrativos

A solicitud de los proveedores, se han emitido durante el curso 2022/2023 un total de 4 informes sobre la correcta ejecución de los servicios y/o suministros contratados para su posterior certificación por parte de la Secretaría General.

Para la gestión de comunicaciones internas con otras áreas, servicios y órganos de la Universidad se utiliza la aplicación ECO, que permite su tramitación de forma telemática. A través de este sistema se han emitido 30 comunicaciones y recibido 10 a lo largo del curso.

Por otro lado, se han presentado 112 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 179 ordenadores portátiles.

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

GESTIÓN DE SEGURIDAD

Descripción de tareas seguridad de la información

Política, normas, procedimientos e informes

El 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, sustituye al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

En mayo de 2022 se ha publicado también la guía CCN-STIC 881A Perfil Cumplimiento Específico Universidades.

Las modificaciones que ambas normativas aportan son incluidas en los trabajos realizados durante el curso 2022 – 2023, el particular:

- Se revisa la Política de Seguridad de la información y Protección de Datos de la universidad, para adaptar el marco organizativo, los cambios de denominaciones de principios recogidos en la Política y la actualización de referencia a artículos en la ley
- Se han corregido las referencias a la normativa en aquellas plantillas y documentos usados para la gestión de la seguridad
- Se ha realizado el análisis de riesgo conforme a las medidas del ANEXO II recogidas en el nuevo ENS.
- Se ha actualizado la declaración de aplicabilidad conforme a las nuevas medidas y a lo establecido en el perfil de cumplimiento para universidades

Además de los cambios en la Política de Seguridad de la Información y Protección de Datos derivados del cambio de normativa, en la parte de organización de la seguridad, se incluye la figura del Administrador de Seguridad Delegado que recae en los Jefes de Servicio de Centro de Informática y comunicaciones.

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 comenzado a elaborar nuevos borradores sobre procedimientos de gestión de incidentes de seguridad para establecer las acciones a realizar en el tratamiento de una creciente llegada de alertas de los sistemas de vigilancia que se van desplegando en la Universidad.

- Procedimiento de gestión de la llegada de alertas Trillion
- Procedimiento de gestión de la llegada de alertas Pandora
- Procedimientos de gestión de credenciales comprometidas o en riesgo.
- Procedimiento de gestión de equipos sospechosos de infección por malware

Desde la Comisión de seguridad de la Información y protección de datos se impulsa la creación de un procedimiento de emergencia para incidentes de seguridad con impacto alto en los sistemas. Se adquiere el compromiso de establecer canales de comunicación con la comunidad y entre el Personal con responsabilidades en caso de incidente.

Se han generado los siguientes informes:

- INF_CIC-16_requerimiento_DPD_v.1.1.pdf Informe requerido por el Delegado de Protección de Datos para la gestión de derecho de acceso de un interesado.
- INF_CIC-16_Proyectos_coiberseguridad_v.1.0.docx. Informe sobre valoración y proyectos de seguridad
- INF_CIC-16_Sistemas de Vigilancia_v.1.0.docx. Descripción de los sistemas de vigilancia de la Universidad
- INF_CIC-16_SEGUPO-2425_v01r01. Informe de incidente por posible ransomware en servicio de radio
- INF_CIC-16_SEGUPO-2435_v01r01.docx. Informe incidente extracción de equipo
- INF_CIC-16_equipos_reincidentes.doc. Informe sobre equipos de las conserjerías.
- Informe ejecutivo sobre gestión de incidencias durante 2020.

Comisión de Seguridad de la Información y Protección de datos

Raúl Giráldez, en calidad de Vicerrector de Transformación Digital y en como Responsable de Seguridad, convoca sesión ordinaria con el siguiente orden del día:

1. Aprobación, si procede, del acta de la sesión de constitución y de la 1ª sesión celebradas el 11 de marzo de 2022.
2. Informe del presidente de la Comisión.
3. Informe de gestión de incidentes del año 2022.
4. Informe INES.
5. Aprobación, si procede, de los niveles de riesgo.
6. Aprobación, si procede, de la actualización de la política de seguridad.
7. Ruegos y preguntas.

Se informa y aprueba, según el procedimiento establecido, los niveles de riesgo y la actual Política de Seguridad en su revisión anual obligatoria. Se incorporan los cambios propuestos Política a la espera de su revisión por el Delegado o Delegada de Protección de Datos cuando asuma el cargo. Así mismo se aprueban los niveles de riesgo y se informa de la modificación de la Declaración de Aplicabilidad y del cumplimiento en tiempo y forma del informe INES.

Se presenta el plan de Transformación Digital y se remarca el papel activo de la comisión en el punto estratégico para una Olavide digitalmente + segura.

Se presenta el informe de incidentes de seguridad.

Se informa sobre el proyecto de gestión de identidades.

Se informa sobre las campañas de concienciación que se están llevando a cabo y se determinan acciones para incentivar la participación del personal.

Se adquiere el compromiso de comenzar a elaborar un plan de emergencia habilitando canales de comunicación que funcionen si los sistemas de la Universidad no están operativos.

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 versión 2022.1.8, 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): 3,4 (escala 0-10) – ALTO.

Se genera la siguiente documentación:

- Informe ejecutivo INF_CIC-16_analisis_de_riesgo_2023.doc.
- SOA_Declaración de Aplicabilidad de Medidas del ENS_2023.
- Fichero de análisis de riesgo 2023.

Se genera también el valor del indicador de gestión de la seguridad establecido en marco con un valor de 2,6. Se elabora el informe con el valor y el procedimiento de cálculo.

Se detecta como área de mejora, la necesidad de revisión y ampliación de alcance del análisis de riesgo cuando se definan formalmente las actividades de tratamiento asociadas a la protección de datos de carácter personal.

Se aprueban los niveles de riesgo en la reunión de la Comisión de Seguridad de la Información y Protección de datos de 17 de mayo de 2023.

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 278 incidentes de seguridad

- 6 administradores de sistemas.
- 0 CCN-CERT.
- 0 AndalucíaCERT
- 5 dirección CIC.
- 0 INCIBER-CERT.
- 7 jefe de Gestión de Seguridad.
- 2 proveedores de sistema externos.
- 1 proveedores con sistemas en la UPO.
- 16 responsables UPO externos al CIC.
- 31 sonda SAT-INET.
- 47 sistemas antispam.
- 154 usuarios UPO.
- 3 plataforma antivirus.
- 7 sistemas monitorización
- 1 otros.

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

- Mayor concienciación de usuarios.
- 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.
- 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:

Memoria Área de TIC 2022-2023

- Se ha procedido a informar y concienciar a usuarios 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.

Se están incorporando nuevos servicios de vigilancia, como EDR, EGIDA, Windows DEFENDER for endpoint lo que incrementa el número de alertas a atender.

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 proveedores 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.
- Denuncia a proveedores de aplicaciones de la Universidad de vulnerabilidades detectadas en sus sistemas.

Despliegue 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 periodo contemplado en la memoria se ha terminado de desplegar la herramienta 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 se han detectado un intento de infección de un equipo crítico, detectado y contenido a tiempo por la herramienta.

EGIDA

Bajo el nombre de EGIDA se engloban varias herramientas, actuaciones y servicios que RedIris proporciona a las instituciones afiliadas para un mayor control sobre el tráfico que RedIRIS les entrega. Estas herramientas están sobre todo destinadas a evitar que los servicios de la Universidad presta se vean afectados por un ataque de denegación de servicio.

LA Universidad ha hecho las actuaciones necesarias para integrarse en este nuevo servicio y tener así una barrera de protección frente a ataques DDoS.

Campaña de concienciación

Durante el periodo recogido en esta memoria se han puesto en marcha dos campañas de concienciación online en materia de ciberseguridad para dar respuesta a la obligación normativa en este sentido.

- Campaña de SIMULYCON de RedIris destinado a 1060 persona 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 destina a personal no docente con un total de 400 participantes. Esta campaña consiste seguir unos contenidos que exponen tres casos reales de incidentes de seguridad y explican al participante cómo prevenirlos. Es una campaña pensada para entrenar en la detección y respuesta ante incidentes de seguridad.

Se ha mantenido, como en años anteriores, una labor intensa de concienciación a través de mail desde la cuenta de seguridadti@upo.es, en respuesta a las consultas de los usuarios. Además, se han enviado correos personalizados a todos aquellos usuarios 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 manera se han atendido desde dicha cuenta, por la coordinadora de seguridad de la información, dudas en materia de seguridad que los usuarios 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 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.

En este periodo ha salido a licitación el proyecto de colaboración del programa UNIDIGITAL, liderado por la US, que busca crear portales de seguridad donde se pueda acceder a contenido formativo y desde donde se puedan promover campañas de concienciación dirigidas.

Se ha realizado también concienciación entre el equipo de dirección, durante sesiones específicas y en la reunión de la Comisión de Seguridad, para hacer entender el estado de la seguridad en el Universidad y se ha incluido a los miembros del consejo de gobierno como participantes en las campañas de concienciación.

Por otro lado, en el marco del Seminario sobre gestión pública universitaria 2023, realizado en marzo de 2023 se desarrolla una ponencia - *Hola, me llamo Andrés. Me van a ciberatacar* - a cargo de **Andrés Prado**, que permite a la audiencia conocer de primera mano un ataque de alto impacto sufrido en una Universidad, lo que acerca la percepción del riesgo y la responsabilidad individual y colectiva en materia de seguridad.

Auditorías

- Gestión de identidades realizada por Solutia. Con el fin de reimpulsar el proyecto de gestión de identidades se ha analizado la situación actual para intentar abordar el diseño conceptual del núcleo de la gestión de identidad y comenzar con el modelado. Esta auditoría ha permitido conocer los riesgos de proyectos de estas características que son de larga duración y que generan cambios importantes en la forma de trabajar.
- Revisión de sistemas de bases de datos (ODA) realizada por Solutia. Se han revisado los siguientes aspectos del sistema: arquitectura de cómputo//disco/red, uso de memoria, uso de CPU, actividad de disco y apariciones de errores en alerts. Se han producido detección de vulnerabilidades en los sistemas que han procedido a gestionarse como tales.
- Auditoría Interna sobre contraseñas de personal Staff fuera de norma en canto al tiempo máximo uso de una misma contraseña.

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

Memoria Área de TIC 2022-2023

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 38 incidentes notificados por la sonda, volviéndose a recuperar el número de incidentes respecto al año anterior donde estuvo la sonda inactiva durante unos meses.

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.

Se detectan muchos incidentes generados en equipos BYOD conectados a la wifi.

Identidad y control de acceso

Como ya se puso de manifiesto en periodos anteriores, la gestión de la identidad y el control de accesos constituyen una línea prioritaria de acción ya que está en relación con los indicadores más altos de riesgo y ha sido identificada por auditorías externas como debilidad grave del sistema. El cambio de paradigma impulsado por la extensión del perímetro de seguridad con el cambio de los modos de conexión y trabajo, orientan la seguridad hacia la protección de la identidad como garantía de control del riesgo y prevención de incidentes de seguridad.

Pero no solo se trata de una cuestión técnica, se trata de una cuestión organizacional que es clave a la hora de afrontar los retos de la verdadera transformación digital, en el que usuario su identidad se convierten en el centro de los servicios.

Se retomaron los trabajos desarrollados en cursos anteriores sobre el modelado conceptual de las piezas que componen el mapa de la gestión de identidades: las identidades, los recursos y los permisos de acceso.

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 AndalucíaCERT. Ante la llegada de estos avisos, se determina si hay equipos críticos afectados por la vulnerabilidad. Caso de existir, se procede al despliegue de la solución, la toma de medidas alternativas de contención o la aceptación del riesgo, si la situación del equipo impide actuaciones sobre él

(riesgo de interferir en funcionalidad, equipos en retirada, equipos con falta de mantenimiento, etc.).

Se han gestionado un total de 25 vulnerabilidades muchas en relación a 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.

Cuando el mantenimiento del sistema está externalizado, se trasladan las vulnerabilidades a los proveedores que tienen que aplicar las medidas de seguridad. En particular, se han realizado notificaciones a OCU en relación con equipos obsoletos que se han sustituido por nuevas versiones.

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.

Cambios del modelo puestos de trabajo y almacenamiento de información interna

Se está han realizado los pilotos y las pruebas necesarias para poder comenzar a implementar el nuevo modelo de puesto de trabajo para el PTGAS. Se trata de sustituir el equipo fijo por un equipo portátil, que se utilizará para trabajar tanto en la modalidad presencial como en la modalidad de teletrabajo.

Si bien este modelo incorpora nuevos riesgos asociados a un dispositivo móvil de la Universidad que saldrán de sus instalaciones, mejora la seguridad en el acceso a la información de la Universidad:

- No se utilizarán equipos personales para conectarse a la red de la Universidad mediante VPN. Estos equipos no estaban protegidos con herramientas corporativas y estaban expuestos a usos compartidos con el entorno familiar.
- Se reduce el uso de la VPN, quedando exclusivamente reservado para aquellas personas que requieran el acceso a un servicio que no pueda accederse de otra manera.
- Se incorpora la posibilidad de recuperación de información en equipos personales puesto que parte de la información se replica en la nube.

Este nuevo modelo de trabajo va acompañado de una nueva forma almacenamiento interno de la información compartida de cada unidad del PTGAS. Esta nueva forma de trabajo:

- Permitirá eliminar las VPN

- Mejora las condiciones de recuperación de información en caso de pérdida accidental o intencionada
- Permitirá la retirada del sistema obsoleto de almacenamiento interno que está fuera de mantenimiento.

Formación

Se ha asistido a las siguientes acciones formativas en materia de seguridad:

- Webinar ANA
- Jornada Cambios del nuevo Esquema Nacional de Seguridad
- Presentación de Gloria y herramientas comunes y compartidas
- Identi::SIC, Cara a cara ... con la identidad
- XVI Jornadas STIC CCN-CERT
- Seguridad en infraestructuras de red.
- AWS Immersion Days v2.0
- Seminario gestión pública
- Security Chapters - Itinerario Desarrollo Seguro
- Presentación del Plan de Transformación Digital
- Workshop Secure Identities and access

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 33 %.
- Indicador de mejora continua 33,4%.

No aparecen datos referidos a 2022 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.

El informe INES es presentado y validado por la Comisión de Seguridad en su sesión de 17 de mayo de 2023.

SERVICIO DE APLICACIONES Y SISTEMAS

Administración Electrónica y TIC

La progresiva implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en las universidades y más en particular en la Universidad Pablo de Olavide, ha provocado un profundo cambio en todos los ámbitos propiciando nuevas fórmulas de generar, gestionar y transmitir el conocimiento, la cultura y el saber; nuevas formas de administrar los recursos de la Universidad empleando las tecnologías como soporte del entorno de enseñanza-aprendizaje y las relaciones con sus usuarios directos (Personal Docente e Investigador, Estudiantes y Personal de Administración y Servicios) y con la sociedad en general. Las TIC, principalmente, aunque no de forma exclusiva, constituyen el eje alrededor del cual se ha desarrollado este proceso de transformación.

Administración Electrónica

Durante este curso académico se han seguido manteniendo las distintas infraestructuras y aplicaciones que dan soporte a las plataformas de Administración Electrónica.

OFICINA VIRTUAL

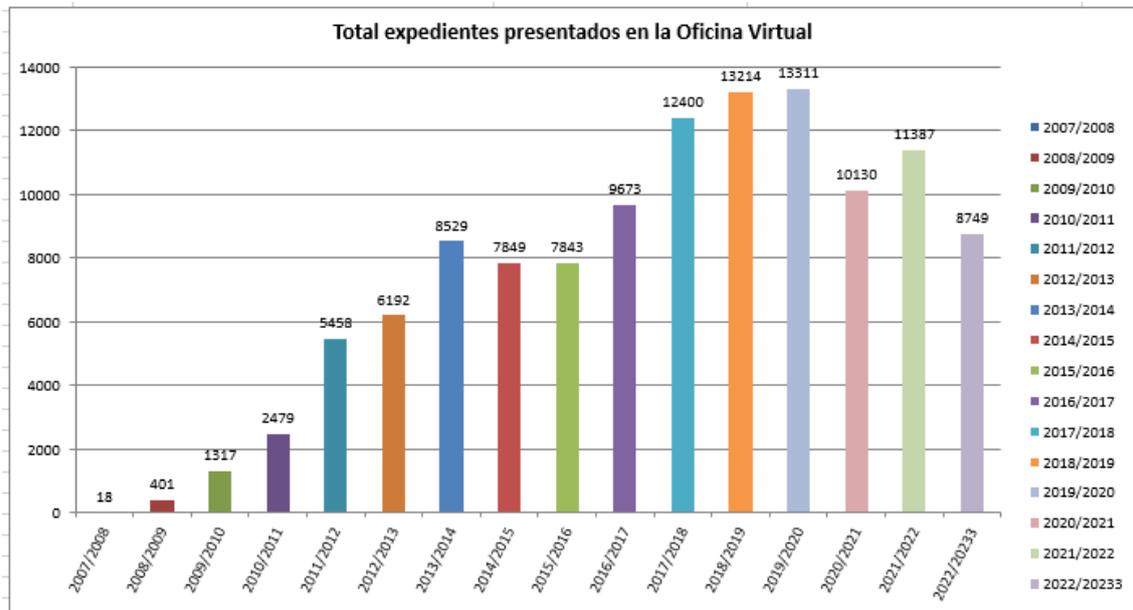
El sistema está basado en el aplicativo Solicit@, y cuyo módulo principal es la Oficina Virtual, portal web desde el cual, la ciudadanía realiza la cumplimentación, firma y presentación telemática de los trámites publicados por la Universidad. También se puede realizar el pago telemático de aquellas solicitudes que lo lleven aparejado.

El acceso a dicha Oficina Virtual se puede realizar con certificado digital, con DNle 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 (PAS, 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

Memoria Área de TIC 2022-2023

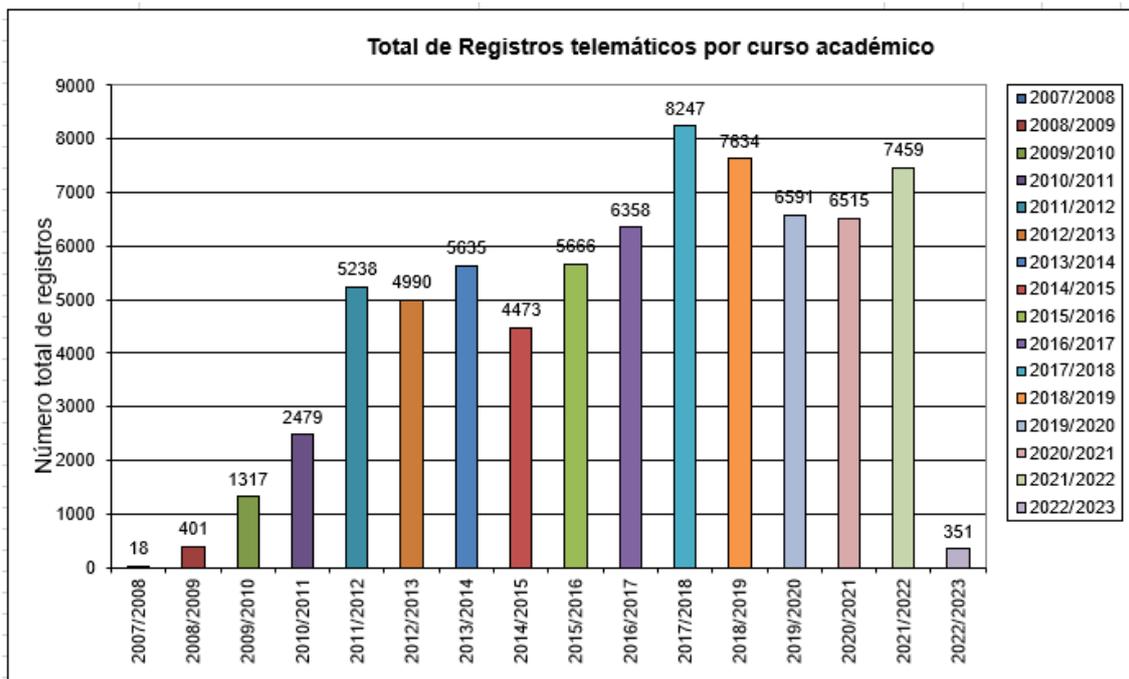
Evolución por curso académico de las solicitudes presentadas en la Oficina Virtual:



Se puede observar un claro descenso en las solicitudes presentadas durante este último período. Esto se debe principalmente a dos factores:

- El procedimiento de Instancia Genérica se presenta desde mayo del año pasado 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 desde principios del año pasado.

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 cuales no. Es por ello por lo que se eliminó esa dependencia del registro telemático de bastantes procedimientos.

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 Funcionarios Habilitados (RFH) para la identificación y autenticación de ciudadanos, 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 de 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 de funcionarios 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:

<https://upo.gob.es/funcionarios-habilitados/>

@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.

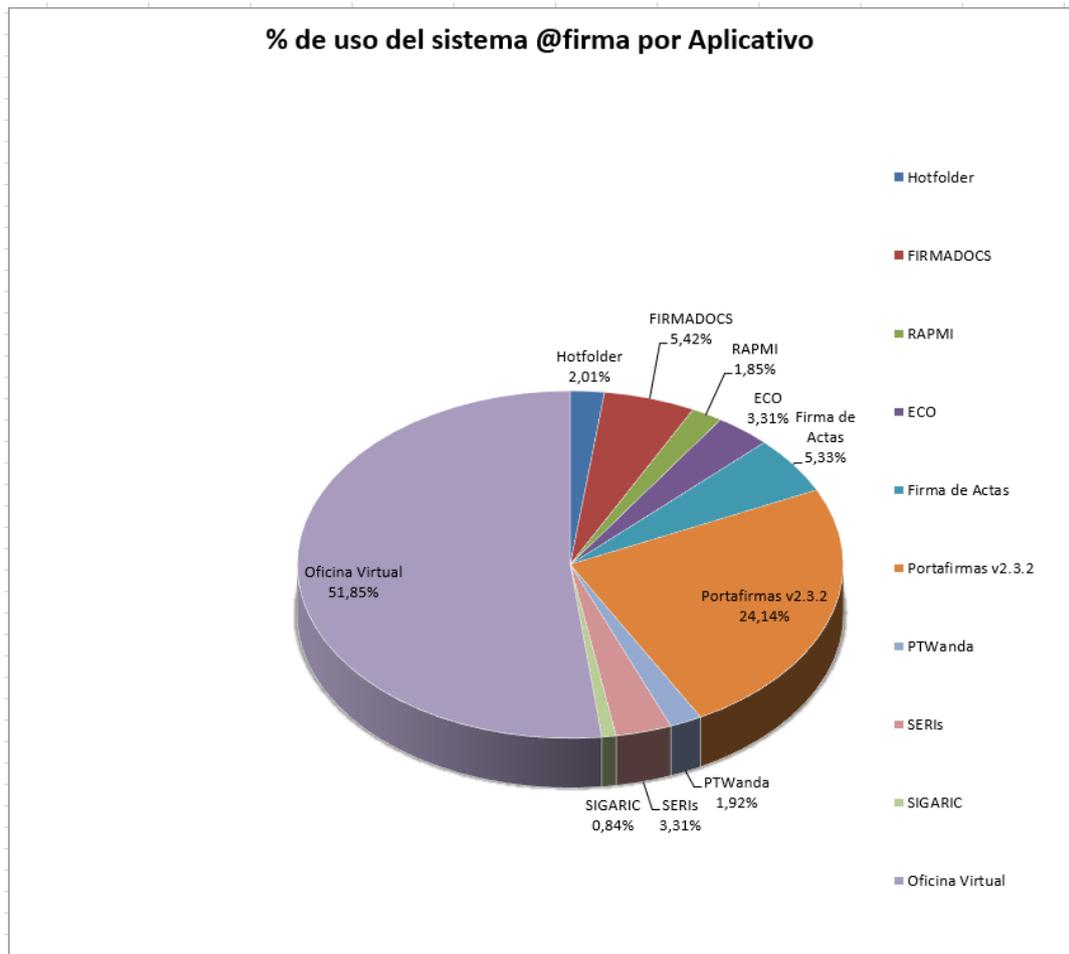
Gracias a @FIRMA, las aplicaciones que la utilicen pueden incorporar procesos de autenticación y firma digital mediante el uso de certificados digitales, independientemente del entorno de desarrollo en que hayan sido programadas.

@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.

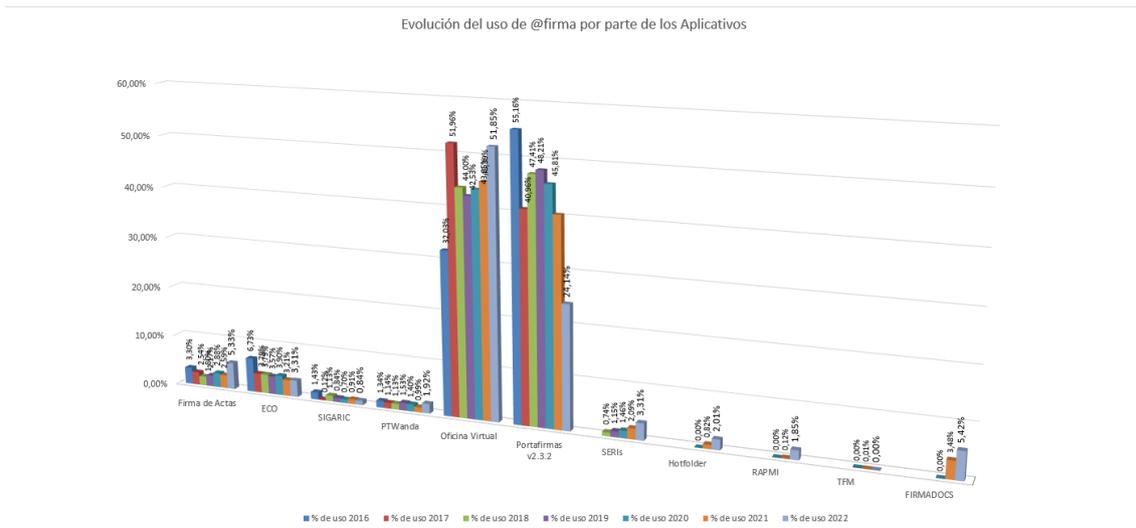
Funcionalidades relacionadas con las políticas de validación de certificados en @firma:

- 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. 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

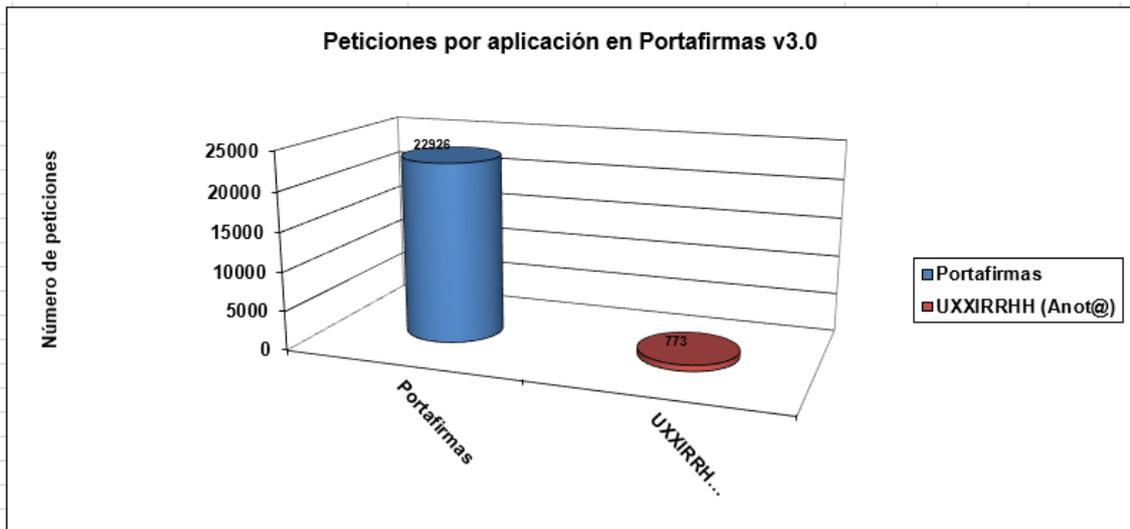
La aplicación Portafirmas es una herramienta destinada a facilitar a sus usuarios el uso de la firma electrónica reconocida en documentos procedentes de distintos sistemas de información, con el objetivo de agilizar la actividad administrativa y disminuir el soporte papel. Realiza las funciones de autenticación, 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 3.0 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.

En el siguiente gráfico se puede ver el número de peticiones enviadas a Portafirmas v3 por tipo de aplicación:

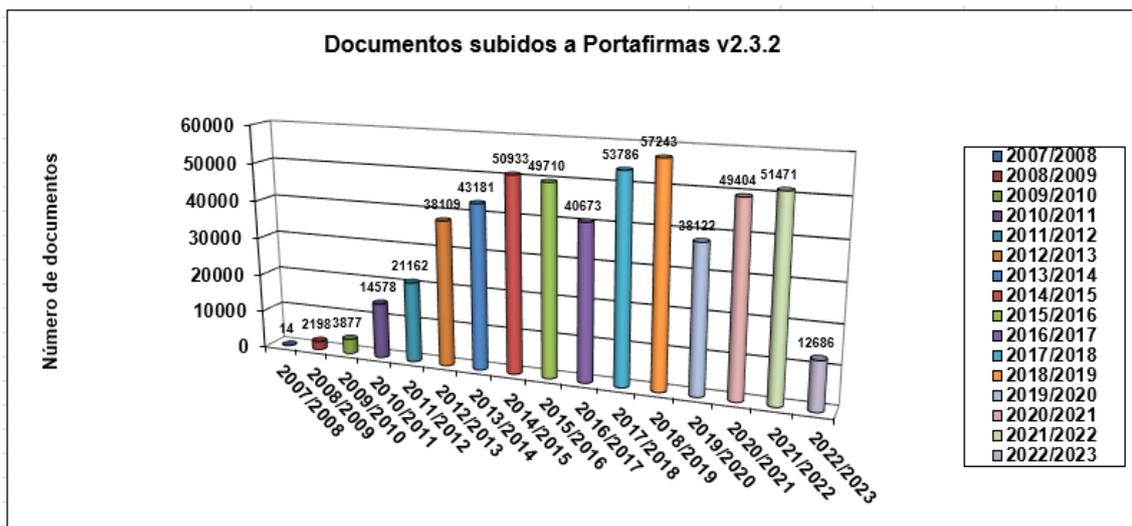


En un futuro será también utilizado por:

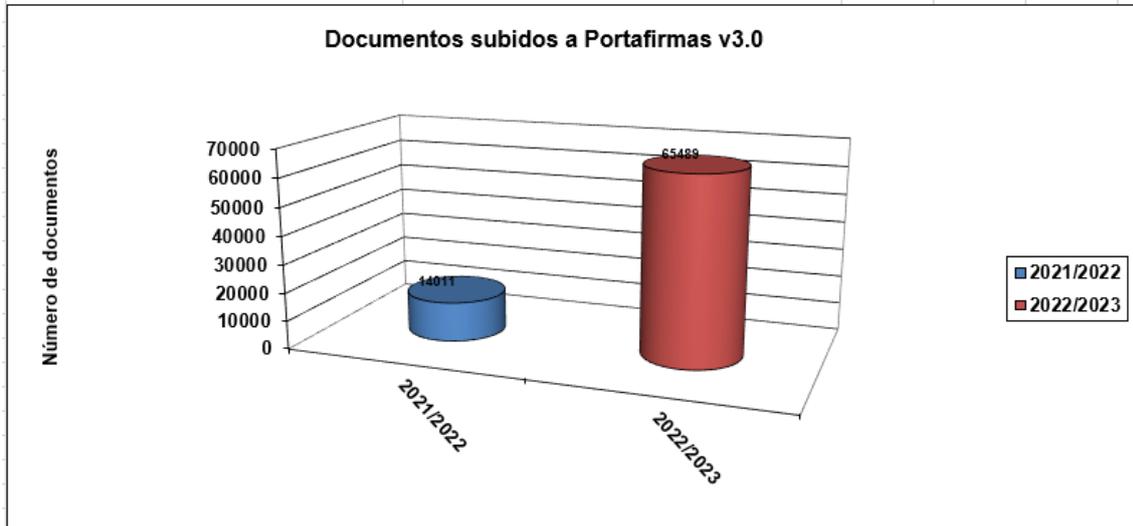
- Los elementos de la infraestructura de la nueva plataforma de tramitación **G-ONCE**, que se encuentra actualmente en fase de desarrollo.
- La aplicación **Docentia** para evaluar la actividad docente y que se encuentra actualmente en fase de pruebas.
- La aplicación **SGIC** (Sistema Garantía Interna de Calidad), que se encuentra en desarrollo.

El antiguo Portafirmas v2.3.2 se utiliza actualmente solo para firma de documentos enviados a través de la aplicación eCO y la plataforma de tramitación, pero se está en trámites de su eliminación definitiva.

Aquí vemos la evolución del número total de documentos subidos a Portafirmas v.2.3.2:



Y la evolución del número total de documentos subidos a Portafirmas v.3 desde su entrada en producción el 24 /02/2022.



PLATAFORMA DE TRAMITACIÓN DE EXPEDIENTES ADMINISTRATIVOS

La Plataforma de Tramitación de expedientes administrativos, 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 PAS, 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.
- Solicitud de Equipamiento Informático descatalogado.
- Etc.

En un futuro relativamente próximo irá siendo sustituida por la plataforma de tramitación GTM, un módulo dentro de la suite G-ONCE.

HOTFOLDER

Esta es una aplicación java desarrollada a medida para la Universidad Pablo de Olavide (UPO), con el objetivo de permitir la firma masiva de documentos de manera simple y sencilla. Su uso es bastante sencillo, ya que se usa la firma de servidor configurada en el servidor @firma de la Universidad y el personal usuario solo tiene que poner los documentos que quiere que sean firmados en un directorio de entrada que lee la aplicación y esperar a que sean firmados, momento a partir del cual se depositan en un directorio de salida.

SEDE ELECTRÓNICA

La sede electrónica de la Universidad Pablo de Olavide está disponible en la dirección web <https://upo.gob.es/> desde septiembre de 2011. El Reglamento de Establecimiento y Funcionamiento de esta sede que da acceso a los servicios de Administración Electrónica de la Universidad Pablo de Olavide fue aprobado por el Consejo de Gobierno de la Universidad el 26 de julio de 2011 y fue publicado en BOJA el 9 de agosto de 2011.

Sobre la Sede se realiza una revisión continua de contenidos, publicando o eliminando aquellas informaciones, normativas, resoluciones que se hayan visto sometidas a cambios.

Se acaba de renovar el certificado de la sede emitido por la autoridad de certificación GEANT Vereniging, vigente hasta mayo de 2024. 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.

- **Datos del certificado de Sede:**

Nombre común (CN): upo.gob.es

Organización (O): Universidad Pablo de Olavide

- Emitido por:

Nombre común (CN): GEANT OV RSA CA 4

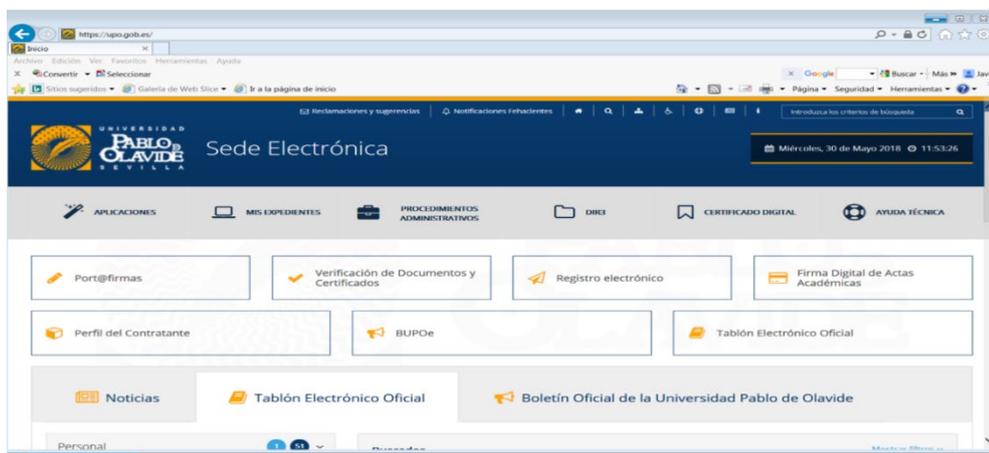
Organización (O): GEANT Vereniging

- Período de validez
Emitido el lunes, 29 de mayo de 2023, 2:00:00
Vencimiento el miércoles, 29 de mayo de 2024, 1:59:59

- Huellas digitales
Huella digital SHA-256
A6 F5 C4 18 CC 2E 65 B7 C5 2E 2E 50 22 4D 89 9D CD F0 B3 B4 D0 A0 FE 44 70 3B CD 4D D9
48 ED E0

Huella digital SHA-1
C5 3F 9A 6C 58 CF 65 67 78 7C FE 87 47 18 D5 A1 B7 B1 22 74

La sede electrónica da cobertura a los requisitos legales requeridos desde el ENI y ENS.



SIA

El Sistema de Información Administrativa (SIA) es una aplicación informática cuya función básica es la de actuar como catálogo de información sobre tramitación administrativa. Incluye procedimientos administrativos y servicios dirigidos al ciudadano y también los propios de las Administraciones Públicas.

SIA da respuesta a la obligación de las administraciones públicas de publicar y mantener actualizadas en el portal web, a efectos informativos, las relaciones de procedimientos de su competencia (artículo 21. 4 de la Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas).

Desde la Universidad se realiza el mantenimiento del listado de procedimientos.

Listado de tramitaciones

[< Volver a la búsqueda](#)

Resultados de la búsqueda			+ Crear trámite	Exportar
Código	Denominación	Organismo responsable	Tipo de tramitación	
3014535	Anulación de matrícula de Grado	Universidad Pablo de Olavide - Vicerrectorado de Gr...	Procedimiento	
3014539	Aportación de documentación para la ...	Universidad Pablo de Olavide - Vicerrectorado de Gr...	Procedimiento	
3014536	Ayudas de acción social: Compensació...	Universidad Pablo de Olavide - Gerencia	Procedimiento	
3015489	Becas propias	Universidad Pablo de Olavide - Vicerrectorado de Es...	Procedimiento	

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 la misma, a través de un sistema de información dedicado, donde puede consultarse y actualizarse. Este sistema reside en la DGMPIAE, 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.
- Los ciudadanos, 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 10 de abril de 2023 y se puede consultar en:

<https://upo.gob.es/dir3/>

NUEVOS PROCEDIMIENTOS EN PRODUCCIÓN

En este periodo se ha desarrollado el siguiente nuevo certificado de respuesta inmediata (SERI).

- **Informe de aprovechamiento del curso "Competencia Digital para Estudiantes de Master":** A través de este servicio se proporcionará a los estudiantes matriculados en los másteres universitarios de la Universidad Pablo de Olavide y que han superado el curso de Competencia Digital impartido por la Biblioteca/CRAI un informe que acredita su aprovechamiento.

PROYECTOS FINALIZADOS Y PUESTOS EN PRODUCCIÓN

- ***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.

Desde entonces se han contabilizado **11329 asientos** en el libro de registro electrónico de **entrada** y **987 asientos** en el libro de registro electrónico de **salida**.

- **ANOT@**

La integración de UNIVERSITAS XXI – RECURSOS HUMANOS con Anot@ RCP (Registro Central de Personal), permite la incorporación de la firma electrónica en el proceso de anotaciones de Registro Central de Personal. Se basa en los siguientes procesos:

- Generación del documento de anotación en UXXI-RRHH a través del servicio EditaRCP del MINHAP.
- Envío del documento a la plataforma de Portafimas.
- Envío de la anotación electrónica y documento firmado al servicio web Anot@.

Empezó a funcionar en el entorno de producción en el mes de marzo de 2022, y se han realizado **776** anotaciones desde entonces.

- **APLICACIÓN PARA LA SOLICITUD, RECONOCIMIENTO Y GESTIÓN DE SOLICITUDES DE MOVILIDAD (RAPMI)**

Aplicación que sirve para gestionar las solicitudes de movilidad (tanto nacionales como internacionales) del estudiantado. En ella los alumnos/as pueden solicitar su estancia en otra Universidad y aportar los certificados de notas cuando su estancia finalice. Por otro lado, los tutores/as validan las solicitudes y elaboran los informes de reconocimiento.

Toda esta información acaba siendo volcada en los expedientes del alumnado, previa supervisión del personal de Área de Gestión de Matrícula y Expediente Académico de Grado.

A su vez, el área de Relaciones Internacionales es el encargado de administrar y gestionar la plataforma.

Adjuntamos a modo de ejemplo, las solicitudes presentadas desde que esta aplicación se encuentra operativa.

PROGRAMA	Nº DE SOLICITUDES
América Latina	24
Atlanticus	41
Bayreuth d. grado extra	11
Erasmus	1.012
Erasmus KA171	1
Erasmus Prácticas	3
Freemover	12
SICUE	113

PROYECTOS EN DESARROLLO

- **G-ONCE (Sede Electrónica, Oficina Virtual, Gestor de Expedientes, etc.).**

G-ONCE es una solución única e integrada para que los organismos públicos puedan dar respuesta 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

G-ONCE incluye, entre otras, las siguientes funcionalidades:

- Sede electrónica: Oficina virtual para el ciudadano: implementación de portales que permitirán a los interesados iniciar trámites, aportar copias digitalizadas de documentos o consultar el estado de la tramitación de sus expedientes. La oficina virtual es multiidioma.
- Portal del Empleado Público: herramientas de backoffice para la gestión interna de trámites.

También es multiidioma.

- Identificación y autenticación con certificados digitales y DNle empleando plataformas de firma electrónica avanzada.
- Catálogo de procedimientos: se incluye una serie de procedimientos comunes plenamente operativos que pueden ser parametrizados y ampliados.
- Generador de formularios virtuales que facilita y agiliza la publicación de nuevos formularios en la Oficina Virtual.
- Generación de documentos asociados a los expedientes tramitados de forma 100% parametrizada.
- Herramienta gráfica de modelado de procedimientos.
- Gestión de interesados y representación.
- Cuadro de mandos basado en monitor de procedimientos.

Actualmente está completamente instalada la infraestructura técnica solicitada en el entorno de desarrollo, así como las integraciones necesarias con las distintas plataformas de la AGE (Notific@, DIR3, SIA, etc.). Hay varios procedimientos en fase de pruebas y el equipo de consultoría de la empresa desarrolladora está manteniendo reuniones con las distintas áreas para seguir avanzando en la implementación de los procedimientos que se han acordado.

En breve se realizará el clonado de esta infraestructura al entorno de producción.

Portal del ciudadano

Trámites y servicios, registro telemático, mis trámites, mis registros, verificador de firmas



Interoperabilidad

Componentes de integración



Portal del empleado público

Tramitación de expedientes



Gestión de documento y expediente electrónico



Componentes de gestión y administración



- **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 el catálogo de servicios que se ofrecen dentro del Cliente Ligero se encuentran:

- Justicia: Consulta de inexistencia de delitos sexuales por datos de filiación.
- DGP: Consulta de Datos de Identidad SCSPv3.
- AEAT: ECOT Contratación con el sector Público.
- TGSS: Estar al Corriente de Pago con la Seguridad Social.
- CCAA: Corriente Pago para Contratación.
- Educación: Títulos Universitarios/NO Universitarios por datos de filiación.
- CCAA: Consulta de Datos de Discapacidad.
- CCAA: Consulta de Título de Familia Numerosa.
- Notarios: Consulta de Copia simple de poderes Notariales.
- Notarios: Consulta de Subsistencia de poderes Notariales.
- INE: Verificación y consulta de datos de residencia con fecha de Última Variación Padronal.

Aplicaciones Corporativas y Sistemas

Portales Web

Durante el presente curso hemos seguido operando las nuevas plataformas Docker de forma satisfactoria. Continuamos sin identificar incidentes de interés, ni de infraestructura, ni de seguridad.

La plataforma WP sigue creciendo y alojando cada vez más espacios, habiéndose identificado un incremento en la demanda sobre todo de espacios relacionados con proyectos de investigación.

La plataforma para uso general también ha dado buenos resultados y seguimos estudiando la migración de algunas aplicaciones corporativas de mayor peso para que también se puedan beneficiar de las ventajas de la tecnología.

Vamos a comenzar el estudio de posibles mejoras en el campo de la configuración y alta de los nuevos servicios que aceleren la puesta en producción de los nuevos portales reduciendo el esfuerzo administrativo.

Con respecto a los CMS corporativos, hemos incorporado una nueva instancia actualizada que en breve empezará a ofrecer contenidos basados en las nuevas versiones de OpenCms, y que supone mejoras en la configuración y gestión frente a sus predecesoras.

También este curso se han retirado algunos sistemas más antiguos que ya presentaban problemas de seguridad y dificultaban la gestión, tanto antiguos servidores de pila LAMP como CMS con versiones obsoletas, tras la migración y actualización de sus contenidos, como por ejemplo las versiones más antiguas de los portales de Facultades y Departamentos.

Con respecto al proxy corporativo, se han incorporado nuevos servicios, lo que facilita la gestión del espacio de direcciones UPO y la conexión segura https, operando sin novedad y de manera satisfactoria.

Se han realizado también mejoras en la configuración para favorecer las labores de administración diaria, que han dado buen resultado.

Se ha migrado el portal de la Escuela Politécnica de tecnología WP a OpenCms, siguiendo la imagen y plantilla del resto de centros.

Se pone en marcha también en tecnología OpenCms, la nueva web de la Escuela de Doctorado.

Se va a independizar la web del Tablón electrónico Oficial (TEO) y del Boletín Oficial de la UPO (BUPO) de la Sede Electrónica actual, de forma que pueda ser usada en el futuro en la nueva Sede.

Correo electrónico

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

Nos dedicamos activamente a mejorar y actualizar continuamente este servicio, con el objetivo de mantenernos a la vanguardia. En el contexto actual, enfatizamos la importancia de redoblar 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 resguardan el sistema de correo contra los diversos y cada vez más sofisticados ataques. Cada incidente nos brinda una oportunidad para adaptar y fortalecer aún más nuestras salvaguardias.

Nuestro enfoque se centra en mantener la eficacia y la rapidez en la detección de ataques dirigidos a la captura de credenciales, logrando detenerlos de manera pronta y eficiente. Además, colaboramos de manera activa con el Instituto Nacional de Ciberseguridad para mejorar la gestión y el tratamiento de los distintos incidentes de seguridad, así como para implementar medidas adecuadas de contención. A su vez, el servicio "Lavadora" de RedIRIS, al que estamos adheridos, sigue manteniendo su eficacia. Este sistema filtra de manera eficiente el correo entrante a nuestra institución, protegiéndonos de una multitud de amenazas y correo no deseado.

Gestión de identidades

El Servicio de Gestión de Identidades de nuestra institución desempeña un papel fundamental al proporcionar diversas opciones de acceso, como nombre de usuario y contraseña, tarjeta inteligente o DNI electrónico. Este servicio sirve 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 ellos se encuentran destacados servicios como "Aula Virtual", "Oficina Virtual", "Firma automatizada", "Repositorio Seguro", "Formación Plan Docente", "Laboratorios Virtuales" y "Servicio de Biblioteca". Además, actúa como punto de acceso a aplicaciones específicas gracias a la integración de nuestra plataforma de Memoria Área de TIC 2022-2023

Identidad con el sistema de Identidad Electrónica para las Administraciones conocido como "@Clave", facilitando así el acceso a usuarios externos a nuestra institución.

Hemos implementado las últimas actualizaciones disponibles 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 al evitar 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 definidos.

Almacenamiento

Hemos dedicado continuos esfuerzos a la actualización de nuestros sistemas de almacenamiento, así como a la retirada de aquellos sistemas más antiguos. Estas acciones garantizan una mayor seguridad y disponibilidad en el acceso a los datos de nuestra institución.

En este sentido, hemos sustituido y modernizado la tecnología de conexión a nuestros sistemas de almacenamiento, con el objetivo de flexibilizar y facilitar futuras ampliaciones y mejoras del servicio. Esto nos permite adaptarnos de manera más eficiente a las demandas crecientes de espacio de almacenamiento generadas por los diferentes servicios de la Universidad.

Particularmente, en respuesta a la creciente amenaza de ataques ransomware que han afectado a entidades tanto públicas como privadas, hemos intensificado nuestras medidas de seguridad. Además de incrementar el espacio disponible para alojar copias de seguridad, hemos implementado salvaguardias adicionales para asegurar la integridad de dichas copias frente a cualquier eventualidad, garantizando su inmutabilidad.

Continuamos trabajando activamente para lograr ampliar nuestra infraestructura de almacenamiento y así proporcionar el espacio necesario requerido por los diversos servicios de la Universidad. Estamos comprometidos en salvaguardar la integridad de los datos y garantizar un acceso seguro a los mismos.

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:

- Aplicación de solicitud de permutas: Desarrollada en lenguaje PHP y base de datos Oracle, ayuda a la gestión de solicitudes del alumnado que quiere realizar permuta con otros alumnos.
- Se amplía la funcionalidad de la aplicación de Horarios para postgrado, añadiendo nuevos controles de cara sobre todo al profesorado externo que impartirá docencia.
- Continúa el piloto de una nueva aplicación de generación y gestión de horarios de la empresa Bullet: Bullet Calendar y Bullet Time Tabler.
- Se pone en producción el componente de Preinscripción de Estudios Propios de UXXI-Académico, el cual conlleva también la gestión de nuevos usuarios de la universidad para que puedan llevar a cabo la solicitud.
- Se termina la validación de un nuevo tablero de datos con la tecnología de Oracle BI para la obtención de datos de alumnos.
- Se continúa con el piloto con Microsoft para la automatización de procesos que se hacen manualmente.
- Tras la puesta en marcha de la nueva aplicación de registros Geiser, se desarrolla una nueva consulta de los datos históricos de la anterior aplicación Aries.
- Se desarrolla un nuevo certificado de IRPF dirigido a proveedores, los cuales se identificarán con @clave y se firma electrónicamente.
- Se pone en marcha un nuevo formulario para los alumnos de la prueba de PEvau, que le permitirá indicar si quieren revisión de examen. En función de su elección, podrán obtener la tarjeta de notas definitivas de cara a convocatorias de preinscripción en otras comunidades autónomas.
- Se prepara un nuevo modelo de encuesta de evaluación docente de cara al curso 2023-24.
- Se implanta la nueva automatrícula Matrux.

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.
- Se cambia la infraestructura que proporciona las consultas web a tecnología ORDS, con dos nodos balanceados.

- Se comienza a migrar aplicativos que estén en php 7 a php8

Se están desarrollando también los siguientes aplicativos:

- BUPO (Boletín oficial de la Universidad Pablo de Olavide).
- TEO (Tablón Electrónico Oficial de la Universidad Pablo de Olavide).
- Gestor de convocatorias de investigación. Se añade además de la integración de este aplicativo con UXXI- Investigación, nuevas integraciones con la plataforma de registro Geiser.
- Se comienza el desarrollo de un aplicativo para la gestión de censos.

Aula Virtual

El acceso al Aula Virtual, plataforma de docencia virtual institucional, se sigue realizando desde <https://campusvirtual.upo.es>

Durante el curso académico 2022-23, el servicio de Aula Virtual ha trabajado intensamente en la implantación de Anthology Ally en la plataforma de docencia virtual, Blackboard Learn. Ally permite hacer el contenido de un curso online más accesible para los alumnos de forma automática, analizando materiales subidos por el profesor con las actuales normas internacionales de accesibilidad y creando por ejemplo versiones accesibles de los mismos en varios formatos y aportando sugerencias de mejora, creando entornos de aprendizaje inclusivos y mejorando la experiencia de aprendizaje de los alumnos.

Al igual que años anteriores, se han realizado labores propias de soporte y seguimiento del servicio 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

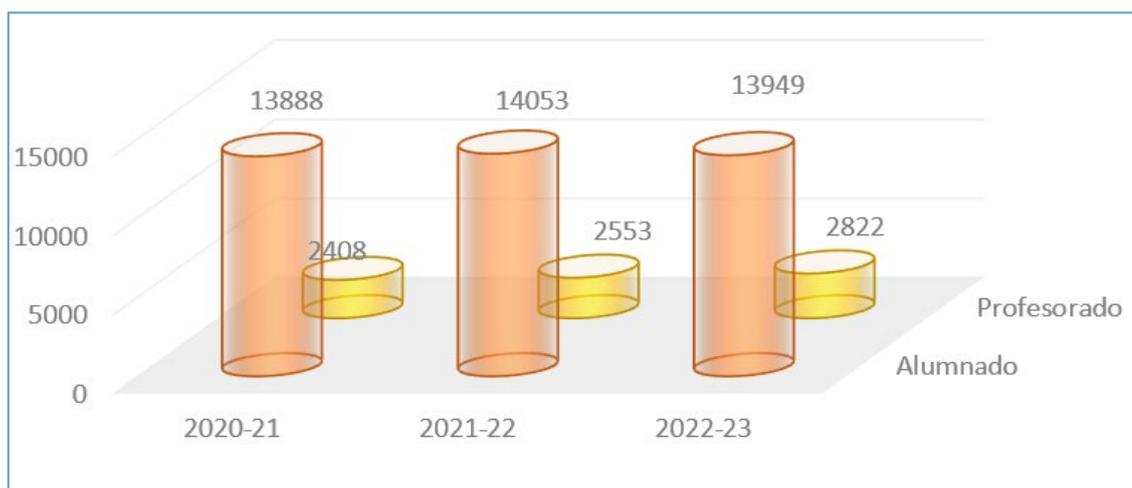
De oficio se crearon todos los espacios virtuales de docencia virtual del curso académico 2022-23, tanto de estudios de Grado como de Postgrado. A petición del CUI se han creado todos los espacios virtuales necesarios para el apoyo a la formación de los alumnos internacionales. Del mismo modo se han creado los espacios virtuales para la actividad docente de los cursos de Formación Permanente.

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:

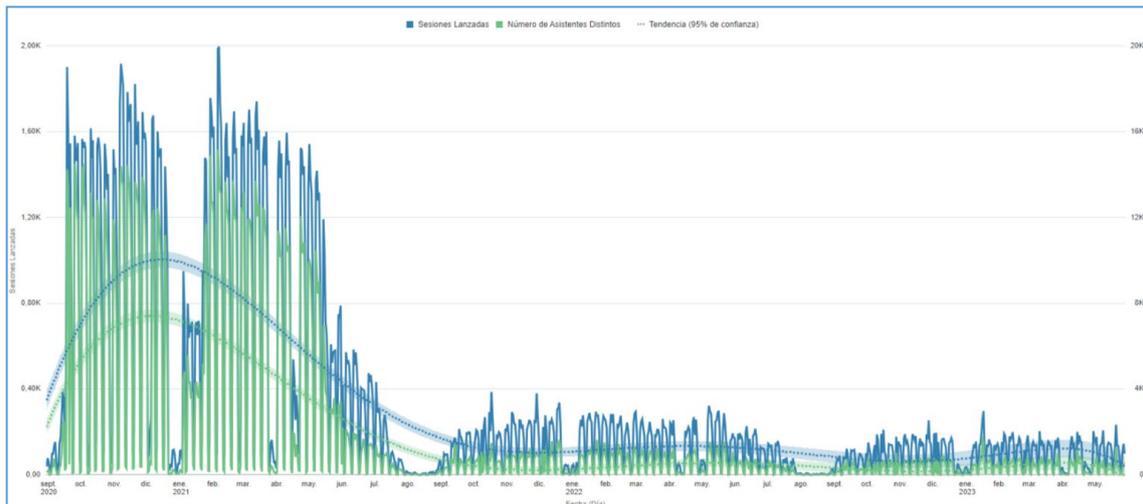
- Con el objetivo de mejorar el tiempo de respuesta de la plataforma y reducir el espacio de almacenamiento, reduciendo así costes de mantenimiento, se han eliminado del Aula Virtual los espacios virtuales del curso 2021-22, así como los usuarios que no tenían ningún espacio virtual asignado en el curso 2022-23.
- Se ha consolidado el apoyo al área de Doctorado para el desarrollo de sus curso de formación.
- A las áreas/unidades en las que se ha justificado la necesidad de crear y gestionar las salas que estimen necesarias para la realización de reuniones, seminarios, jornadas, etc, se les ha proporcionado usuario supervisor de Collaborate, así como la formación y manuales creados especialmente para este acometido, prestando especial atención a los parámetros de configuración de las salas que pueden comprometer la seguridad de las mismas.
- Se ha realizado la integración de Anthology Ally en todos los espacios virtuales.
- Se ha iniciado la preparación del cambio a la nueva versión de Blackboard Learn incorporando la Navegación Ultra, instalándola, configurándola y testeándola en un entorno controlado de pruebas, minimizando así el impacto a los usuarios cuando se vaya a realizar su paso a explotación .

Datos estadísticos del Aula Virtual

Esta gráfica representa el total de usuarios agrupados por perfiles con acceso al Aula Virtual, se observa un ligero aumento en el profesorado manteniéndose el alumnado estable.



En relación al uso de la herramienta de videoconferencia Collaborate Ultra, podemos observar en la gráfica como su uso es algo menor al del curso pasado, alejándose del uso masivo que se hizo durante el 2021-22 en el que la docencia se realizó en modalidad online. 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).



Servicio de Formación e Información al Usuario

El Servicio de Formación e Información, cuyo objetivo es facilitar a los/as usuarios/as toda la información y formación relativa al uso de las herramientas disponibles en la Universidad y que sirven 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 a fin de acercar la plataforma del Aula Virtual y para que su uso sea lo más amigable posible. En este curso se han ampliado las series de video tutoriales iniciadas en el curso 2017-18, [Formación del profesorado para el uso del Aula Virtual](#) y [Formación del alumnado para el uso del Aula Virtual](#), orientadas al profesorado y alumnado respectivamente, con nuevos vídeos profundizando en el uso de las herramientas del Aula Virtual. Actualmente estas series tienen un total de 138 vídeos.

Durante este curso, este servicio ha centrado sus esfuerzos en formar a los profesores sobre el uso de la herramienta Anthology Ally, realizándose 4 sesiones de formación a lo largo del año. Un total de 120 profesores lo realizaron.

Además, se ha dado formación a casi 100 personas de apoyo del área de postgrado, tratándose todas las herramientas básicas, de comunicación grupales, de gestión de alumnado, de evaluación, de gestión de archivos, y la herramienta colaborativa de comunicación integrada: Collaborate Ultra.

SERVICIO DE REDES Y EQUIPAMIENTO

Redes, comunicaciones e infraestructura

WIFI

Actualización

Próximamente, la red WiFi debe ser renovada en su totalidad. Para poder evaluar las mejores opciones se han probado dos tipos de tecnología, ambos respondiendo a WiFi 6. Las pruebas se han realizado en dos edificios diferentes para evaluar la tipología de usuario, frecuencia, anchos de banda utilizados, etc.

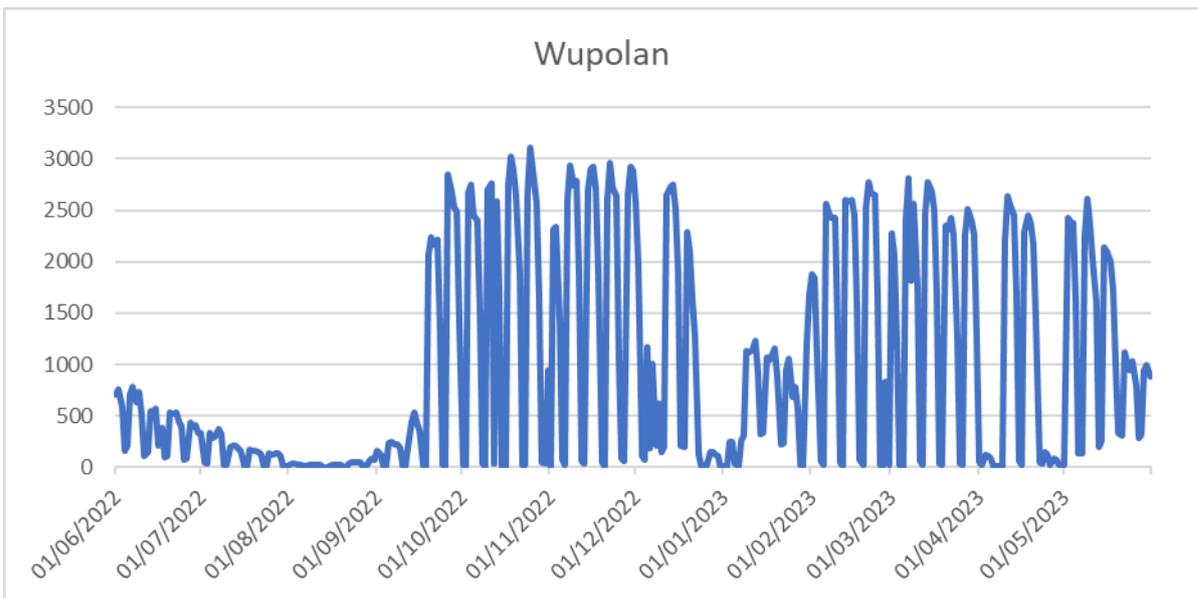
- Edificio 5: Se ha instalado la tecnología de una empresa local, Galgus, cuyas ventajas radican en la simplicidad de la solución.
- Edificio 9: Algo más compleja, pero más robusta, es la tecnología que la marca Juniper ha prestado a la UPO para su evaluación.

Para ambas pruebas se ha tenido que configurar un portal cautivo para identificación y autenticación compatible con las dos soluciones.

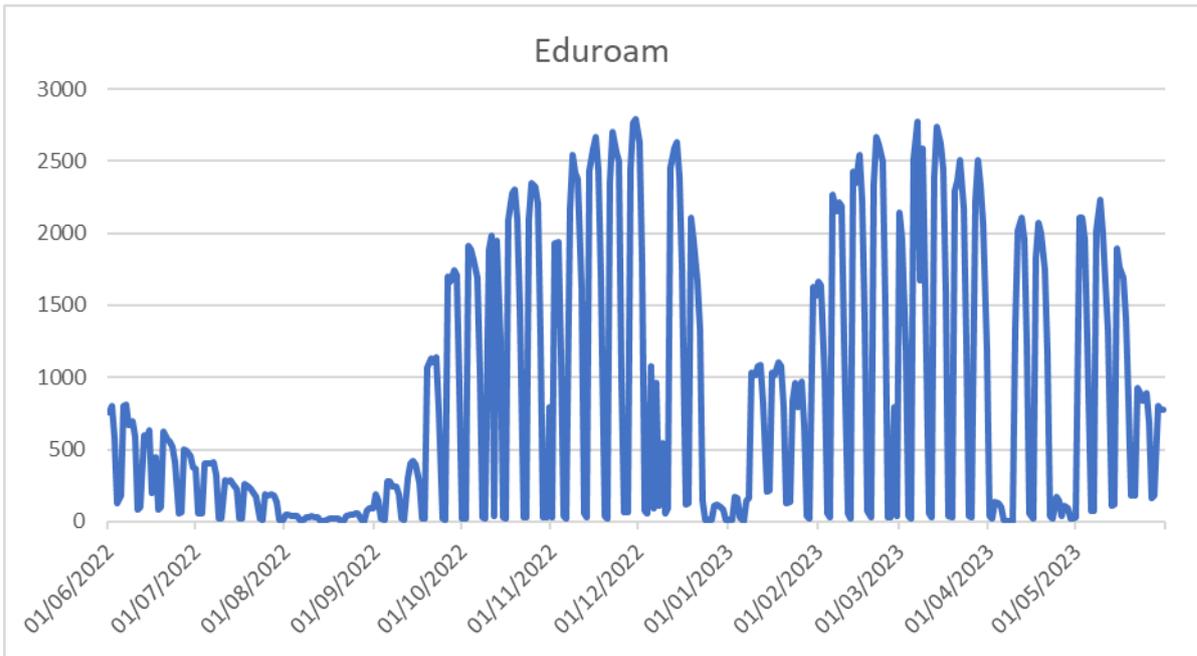
Conexiones

El uso y la conexión a la red WiFi de la UPO ha crecido en este curso un 16 % este curso. A continuación, se muestran unas gráficas en las que pueden verse el elevado número de conexiones existentes en las diferentes modalidades de conexión.

CLIENTES WUPOLAN

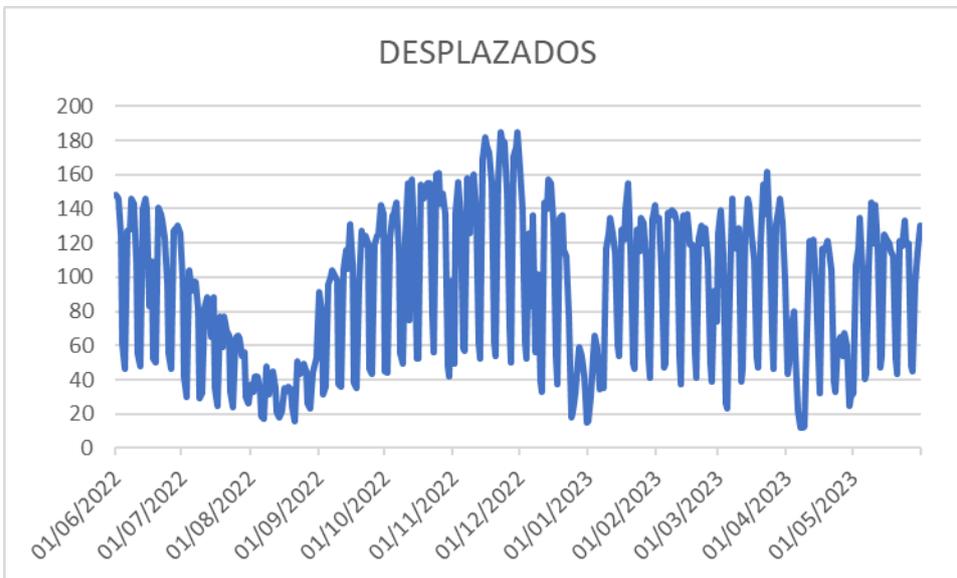


CLIENTES EDUROAM



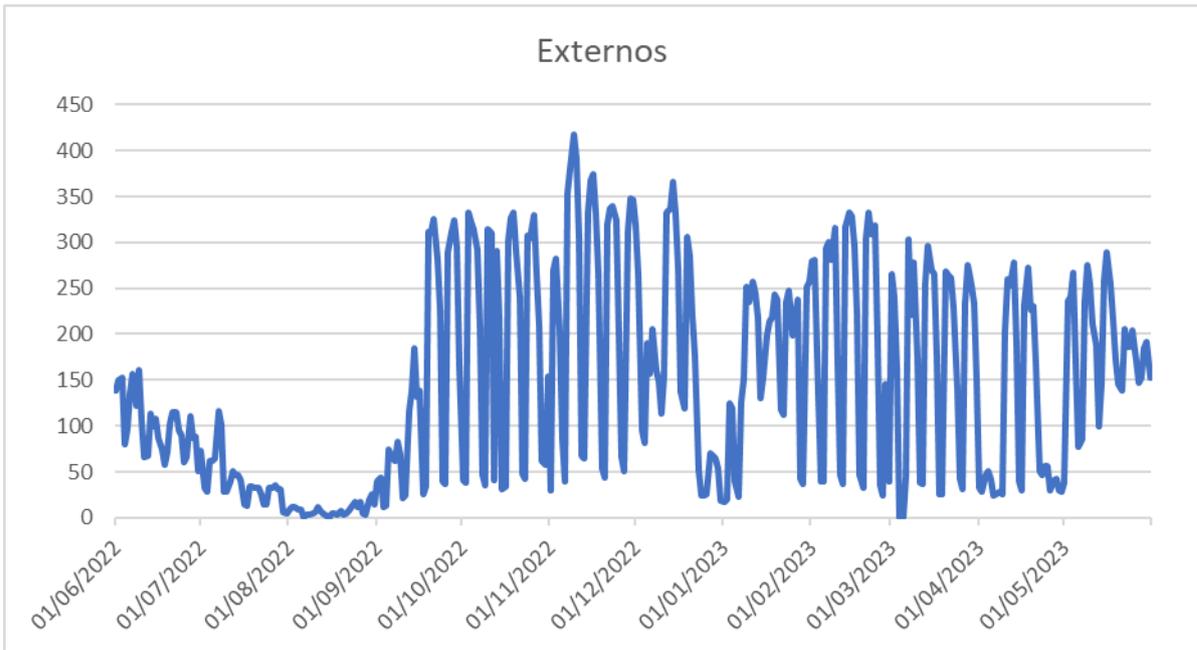
CLIENTES DE OTRAS UNIVERSIDADES DESPLAZADOS A LA UPO

El número de clientes que se ha desplazado a la UPO procedente de otras universidades y ha utilizado la red WiFi para conectarse ha decaído en un 46 % desde el pasado año.



CLIENTES UPO DESPLAZADO A OTRAS UNIVERSIDADES

Crece, en cambio, el número de personas usuarias UPO que utilizan Eduroam fuera de nuestra universidad, en un 62% más anual.



Atención a usuarios

El sistema de configuración basado en código QR iniciado el pasado curso ha dado como resultado la reducción de usuarios y usuarias del servicio de configuración WiFi, siendo ya testimonial su uso.



TELEFONÍA

Proyecto Faro

El proyecto Faro consiste en el fin de las centrales analógicas y el fin del cobre, pasando la comunicación de voz y datos de los operadores españoles a centrales digitales y a fibra.

Con el fin de no quedarnos desprotegidos ante este cambio se han tenido que realizar una serie de adaptaciones en diferentes puntos de la UPO, de modo que se han situado estratégicamente puntos de servicio de operador. De este modo, las líneas analógicas (backups de la centralita de la UPO, tiendas privadas) pasan a ser fibra de cliente directamente de operador.

Datos telefonía

Respecto al número de líneas fijas, ha sido poca la variación respecto a pasados años. Las líneas móviles (213 en la actualidad) han tenido un incremento de un 33 % motivado tanto por el teletrabajo como por el proyecto de puesto de movilidad.

Se continua también con el proyecto de renove de móviles bianual, teniendo un 20 %.

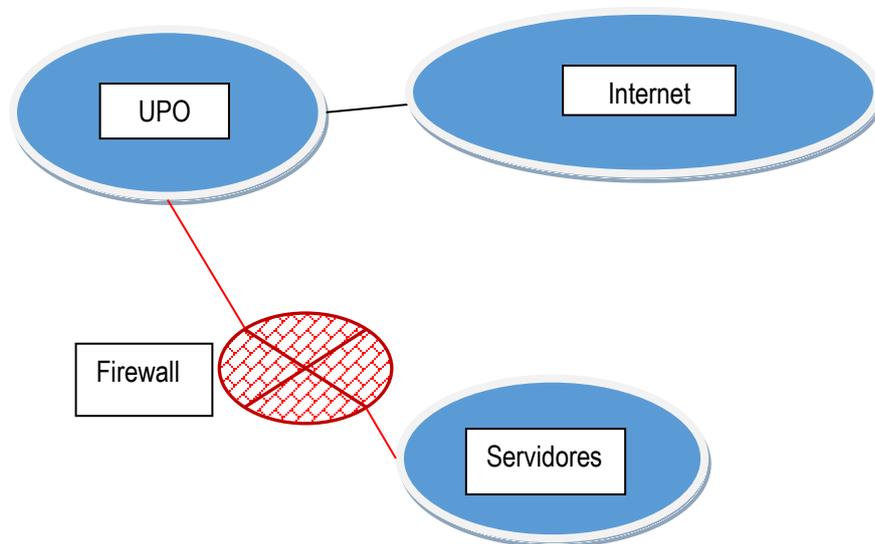
Destacar también la puesta en marcha de la alta disponibilidad en la centralita de telefonía. En la UPO existen dos equipos para telefonía. Uno de ellos, el principal, se encuentra situado en el CPD1, el otro, secundario, se encuentra alojado en el Punto de Presencia (PdP). Las llamadas entrantes y salientes se realizan desde el CPD1, donde se encuentra el enlace con la red de telefonía nacional. Pues bien, la alta disponibilidad ha consistido en la activación de un enlace auxiliar que conecta la parte de la centralita del PdP con la red de telefonía nacional para que, en caso de caída del enlace principal, las llamadas puedan realizarse por el secundario.

SEGURIDAD EN LAS COMUNICACIONES

Securización de servidores

Siguiendo con la política de prevención de la UPO frente a ataques informáticos, se ha instalado un sistema de cortafuegos que va a administrar la zona de máxima seguridad, distribuida por los diferentes CPDs y que albergan los servidores donde se alojan los servicios más significativos de la UPO.

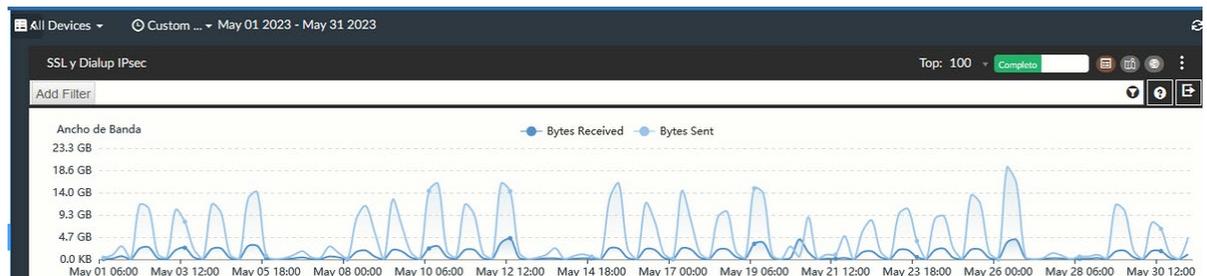
Este firewall es una cesión de una empresa conocida de suministros de seguridad y está aún en pruebas.



Conexiones VPN

Durante el curso 2022/2023 se ha continuado con el teletrabajo a través de las VPN creadas para este fin.

Como medio de conexión desde el exterior a los equipos de la universidad se han seguido usando las redes privadas virtuales (VPN), ya con doble factor de autenticación, teniendo alrededor de las 3.500 conexiones mensuales, consumiendo alrededor de los 18 Gb de datos.



Seguridad Perimetral

Siguiendo con los sistemas de protección, esta vez externos, la UPO se ha unido al proyecto EGIDA, de RedIris.

Bajo el nombre de EGIDA se engloban varias herramientas , actuaciones y servicios que proporcionan a las instituciones afiliadas a RedIRIS un mayor control sobre el tráfico que RedIRIS les entrega, estas herramientas están sobre todo destinadas a evitar que los servicios que la institución presta se vean afectados por un ataque de denegación de servicio .

Los recursos que proporciona RedIRIS para evitar estos problemas son los siguientes:

Autofiltrado

Permite que la propia organización indique al troncal de RedIRIS de que direcciones propias no quiere recibir tráfico. Esto provoca de forma efectiva una denegación de tráfico contra esta dirección pero muchas veces es un mal menor ante el colapso de tráfico en el enlace.

Limpieza de tráfico

Este servicio se activa baja demanda y permite reenviar el tráfico que circula por RedIRIS con destino una institución a un sistema especializado de análisis de tráfico que lo descartará si no es legítimo entregando el tráfico lícito a la institución. De esta forma, el tráfico con destino estas direcciones es "limpiado" y se evita la saturación del enlace de la organización.

Red de datos

Durante este curso se han llevado varias acciones a nivel de red de datos física:

- Renovación de equipamiento obsoleto: se han cambiado por obsolescencia un total de 2 equipos de red de puesto de trabajo en biblioteca, sin afectación a servicio.
- Instalación de equipamiento de red para la configuración de puestos de aire acondicionado, placas solares y puertas en el edificio Nuevo Animalario.
- En el centro de Housing se han actualizado los equipos que conectan los servidores de investigación a equipos de 10 Gb en el acceso a red global.
- En el centro de Housing se han instalado este curso dos equipos, llegando de este modo a los límites de su capacidad respecto al suministro de red eléctrica protegida.

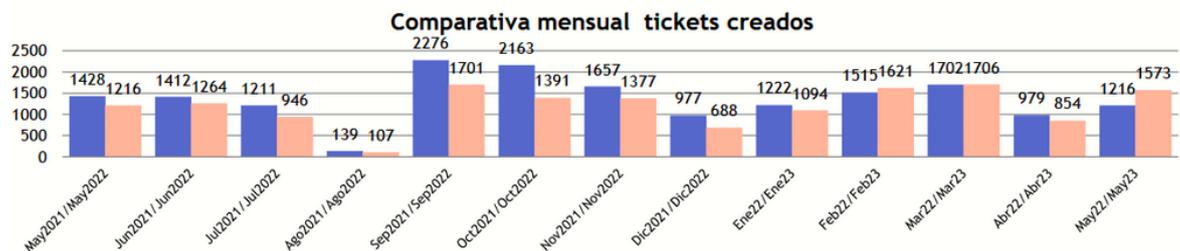
- El acceso a Internet de red RICA fue actualizado el pasado mes de noviembre, pasando de tener un ancho de banda de 10 Gbps a 100 Gbps.
- Se han realizado seis actuaciones de mejora de la red en diferentes puntos de la UPO.
- Se ha realizado una ampliación de la red en la sala 3 del edificio 27.

CENTRO DE SERVICIOS

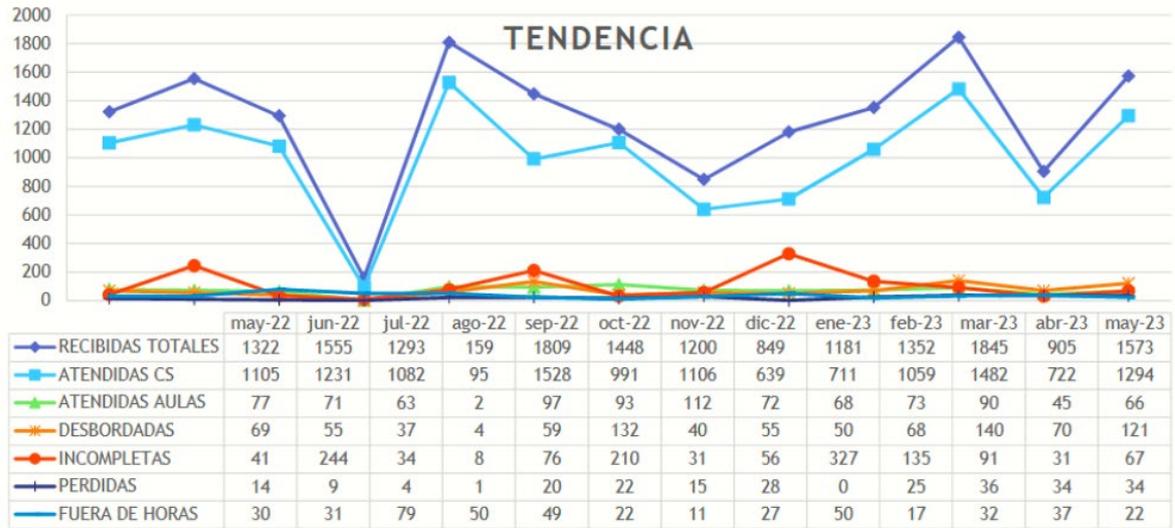
Este curso se ha renovado la licitación del Centro de Servicios, que ha vuelto a recaer sobre Econocom.

Datos del servicio

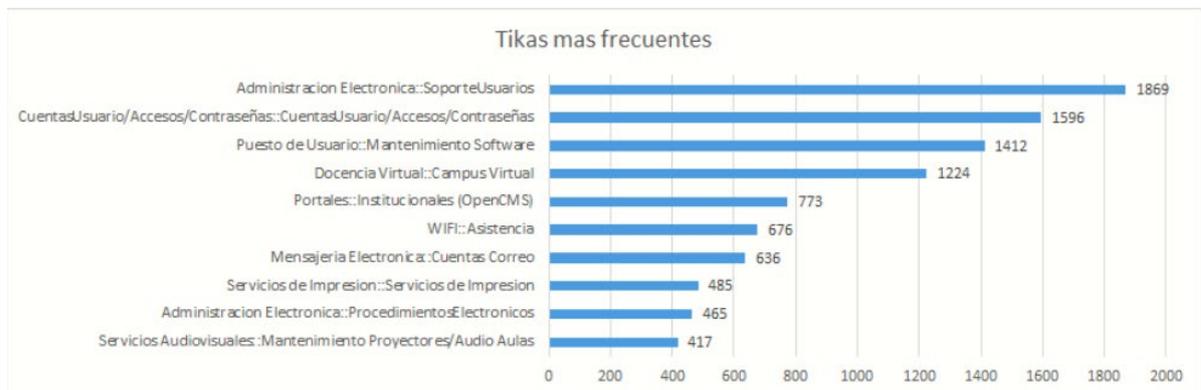
Tickets creados: El número de tickets se mantiene en la misma línea del pasado año, con ligera tendencia a la baja en determinados meses.



Atención telefónica: la media del número de llamadas ronda sobre las 1800 mensuales, con un aumento de un 12% respecto al año anteriorj.



Top Ten de tickets por materia: a continuación, se muestra un gráfico de las 10 materias con tickets más frecuentes.



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,

Memoria Área de TIC 2022-2023

- 120 aulas de docencia en su vertiente audiovisual
- 50 espacios de docencia adicionales (seminarios, laboratorios, etc.),

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

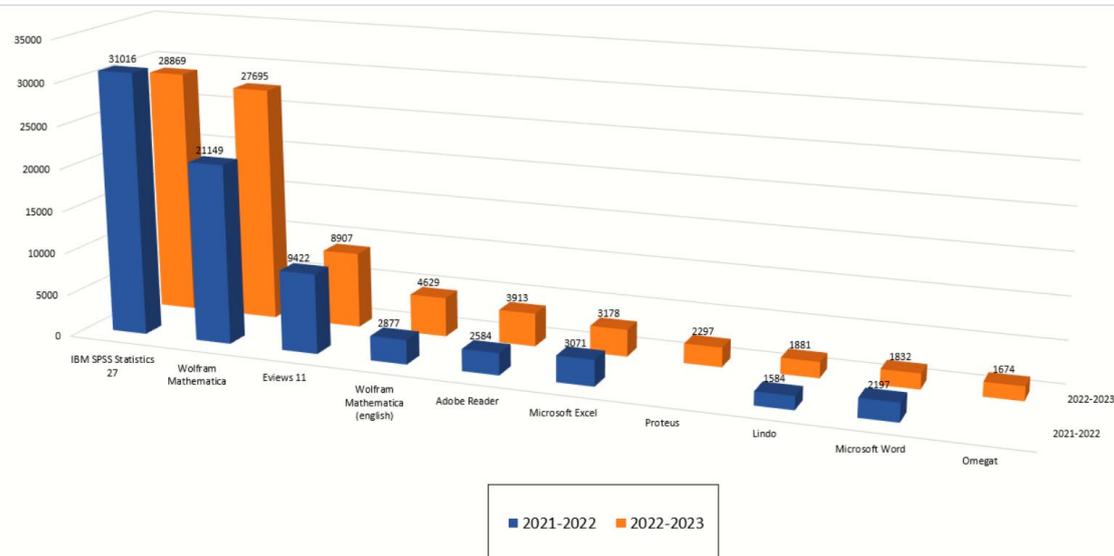
- Gafas 3D. Dentro del Plan de Transformación Digital liderado por el Vicerrectorado de Transformación Digital el Espacio Multimedia del CIC ha gestionado la adquisición de un conjunto de gafas 3D. En este marco, se han configurado y utilizado con nuestro asesoramiento para la EPD “Seguridad en entornos deportivos”.
- En las aulas de docencia, se ha gestionado la adquisición de nuevos equipos para el puesto del profesorado, ya que los antiguos no tenían soporte suficiente para los nuevos requisitos audiovisuales, con la consecuente actualización de los drivers para las cámaras, y demás dispositivos existentes en las aulas de docencia.
- Se han llevado a cabo cinco actuaciones para mejora o alivio de algunas de las deficiencias que con los años van adquiriendo las salas multimedia, así como la remodelación casi al completo de la sala de grado 2 del edificio 25, que debido a una avería se vio afectada por un escape de agua.
- Se han llevado a cabo dos reparaciones de los equipos TOTEMS de teletornos distribuidos por la Universidad.
- Se ha mejorado el sistema de soporte para streaming de la UPO, instalándolo en un servidor físico dedicado.
- SE ha instalado un nuevo equipamiento de videoconferencias en las salas de juntas 1 y 2 de Rectorado.
- A lo largo del año se han dado cuatro seminarios de uso de audiovisuales en la aulas docentes, dos de ellos dirigidos a los ayudantes de servicio y los otros dos para voluntarios participantes en distintos congresos como asistentes de primera línea.

También desde este departamento se llevan temas colaterales, como gestión de llaves y tarjetas de apertura inteligente. En este sentido ha habido un total de 21 actuaciones a llevar a cabo.

MyAPPS

El servicio de aplicaciones de aulas de informática en la nube MyApps 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. Este año se ha incorporado como novedad el uso de HTML5 que permite utilizarlo sin tener que instalar ningún tipo de cliente en el ordenador, facilitando de este modo el acceso.

En el gráfico que se incluye a continuación, se ofrece una comparativa de las 10 aplicaciones más usadas en Myapps - UPO en los dos últimos cursos académicos-



Equipamiento, Aulas y Laboratorios

*** Puesto de usuario.**

Se ha consolidado el producto Intune de Microsoft como sistema de gestión del puesto de usuario.

- Imágenes para instalación de sistema operativo y software corporativo.

La instalación de sistema operativo y aplicaciones basada en imágenes específicas para cada modelo de ordenador (39 imágenes y 344 variantes) se ha sustituido definitivamente por una sola imagen genérica, que permite la instalación en equipos que incorporan la última generación de procesadores.

Esta nueva imagen forma parte del nuevo sistema de gestión del Puesto de Usuario: Intune de Microsoft, que cambia el concepto actual de imágenes personalizadas para cada modelo de equipo y con diferentes configuraciones, por un modelo de imagen única e instalación posterior del software en base a la funcionalidad del equipo.

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 71.

Los perfiles de configuración gestionados desde Intune son actualmente 26, 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.

Actualmente hay 1013 ordenadores gestionados con Intune.

- Renovación de Equipos.

Tras el periodo de transición que ha significado el Renove 2021 y Renove 2022 (incorporación de Intune; gestión de inventario con Listas, Formularios y Teams; Sistema Dinámico de Adquisiciones) en el próximo Renove 2023 ya se aplicará el cambio del sistema de renovación de los equipos de PDI, pasando a ser algo similar al renove PAS, en el que el CIC se encarga de definir qué equipos tienen una antigüedad tal que necesiten ser sustituidos, descargando a los Departamentos de la tarea de definir qué equipos quieren renovar o no.

En el plan Renove 2021 se han sustituido 183 ordenadores de PDI, y se han asignado 40 equipos nuevos a los Ayte. Doctor de los diferentes Departamentos.

*** Puesto de Usuario Móvil.**

El sistema de Puesto de Usuario 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 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 6, con un total de 21 usuarios.

* **Samba - Sharepoint**

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 7.9 TB

Número de Grupos 164

Número de Usuarios 615

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 extraordinario incremento de 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.

* **BSCW**

La herramienta de trabajo Colaborativa BSCW es utilizada por PDI, PAS y Alumnos de Postgrado.

Usuarios registrador 8513

Volumen de datos 2,8 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 plantee sustituir este servicio por Sharepoint.

* **Licencias Campus**

Se han adquirido licencias Campus del software: Matlab, ArcGs 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.

Microsoft 365 A3 for faculty	1300	
Microsoft 365 A3 for students use benefit	52000	
Microsoft 365 A3 for students use benefit	52000	22694

* Aulas

Se da por finalizado el uso de Altiris como sistema de gestión de Aulas de Informática y Docencia.

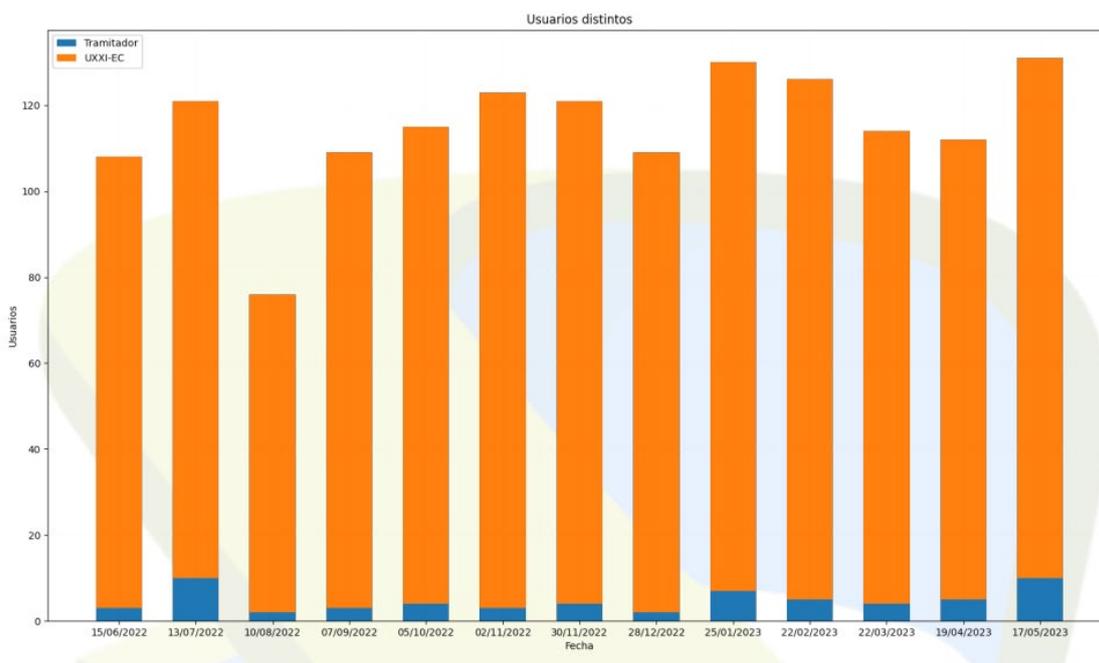
En su lugar, se utiliza Microsoft Intune, optimizando así la preparación de aplicaciones comunes a PTGAS, PDI y Aulas, que se realizaban de forma independiente para Altiris y Kaspersky.

Todas las aulas han sido actualizadas a Windows 10 LTSC 2021. Esta actualización ha requerido la instalación de discos de estado sólido SSD en 109 equipos, algo antiguos, cuya vida útil se prolonga así unos 2-3 años.

Las Aulas de Docencia se han integrado también en la gestión mediante Intune, lo que ha disminuido considerablemente el número de incidencias que había con el modelo Kaspersky/Congelación de equipo, y por otra parte, se gana en seguridad, al permitir la instalación de actualizaciones del sistema operativo.

* Aplicaciones virtuales UDS.

Este sistema de aplicaciones virtuales está orientado al uso por parte del PAS, si bien algunos usuarios con equipos Mac y Linux lo utilizan para acceder a algunos servicios que requieren IE, como puede ser Tramitador.



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 2022/2023 y que son específicas de TI.

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

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: 13
- ✓ Modalidad de actividad formativa:
 - Presencial: 2
 - Virtual: 11
- ✓ % participación personal CIC: 72,73 % (24 de 33)
- ✓ Nº horas formación TI 2022/2023: 175 horas
- ✓ Coste total: 11.524,19 €

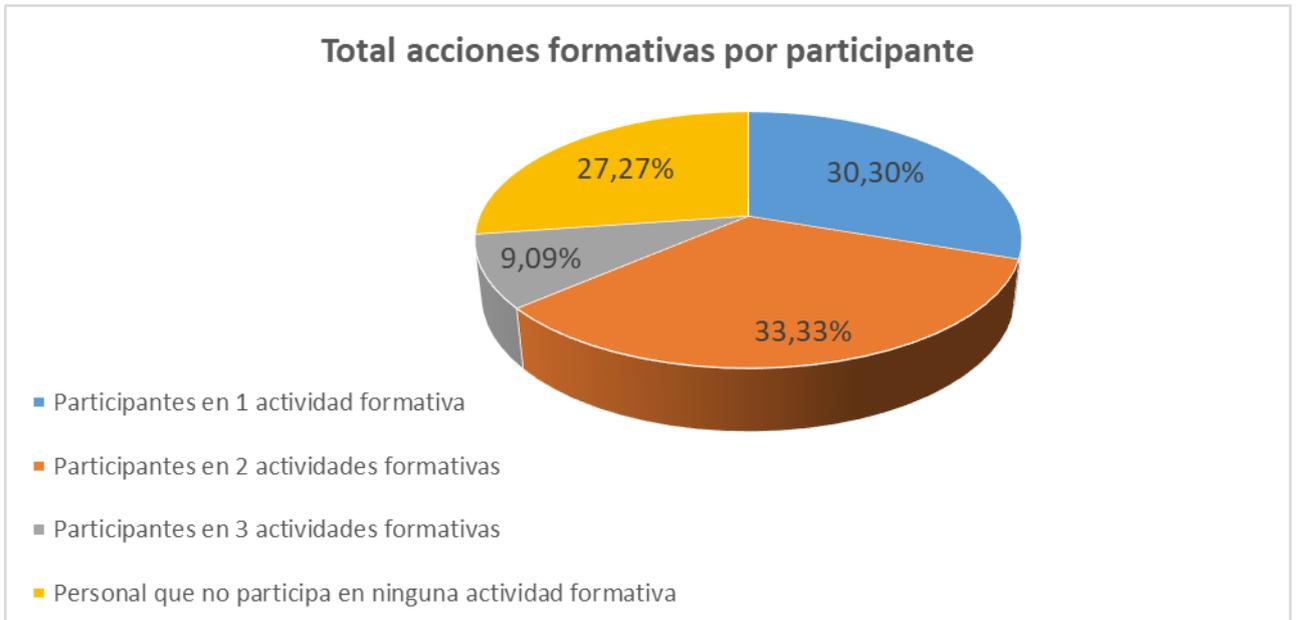
Detalle actividades formativas TI realizadas:

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Veeam Backup & Replication V11: Architecture and Design	14,00	1
Webinar solución ANA CCN-CERT para Universidades	2,00	1
Power Platform para usuarios de IT	9,00	1
Power Platform Deep Dive	9,00	2
Formacion ad hoc en Junos	14,00	5
AWS	8,00	19
X CURSO STIC – SEGURIDAD EN INFRAESTRUCTURAS DE RED	40,00	1
Introducción a NetSupport School	1,00	3
Administración Avanzada con PowerShell	25,00	4
Security Chapters - Itinerario Desarrollo Seguro	16,00	1
Seguridad en Infraestructuras de Red	15,00	1
Nuevo Esquema Nacional de Seguridad (ENS)	20,00	1
Anatomía del Ransomware	2,00	1

Acciones formativas TI por participante:

Participantes en 1 actividad formativa: 10
 Participantes en 2 actividades formativas: 11
 Participantes en 3 actividades formativas: 3
 Personal que no participa en ninguna actividad formativa: 9

Memoria Área de TIC 2022-2023



Formación específica en seguridad

Se ha asistido a las siguientes acciones formativas en materia de seguridad:

- Webinar ANA
- Jornada Cambios del nuevo Esquema Nacional de Seguridad
- Presentación de Gloria y herramientas comunes y compartidas
- Identi::SIC, Cara a cara ... con la identidad
- XVI Jornadas STIC CCN-CERT
- Seguridad en infraestructuras de red.
- AWS Immersion Days v2.0
- Seminario gestión pública
- Security Chapters - Itinerario Desarrollo Seguro
- Presentación del Plan de Transformación Digital
- Workshop Secure Identities and access

Formación específica en Redes y Multimedia

Este curso se han recibido dos formaciones de red y telefonía:

- Curso de servicios de tarificación de centralita.
- Curso de Sistema Operativo JUNOS

En otro aspecto de la formación, se han impartido cuatro seminarios de uso de audiovisuales en la aulas docentes, dos de ellos dirigidos a los ayudantes de servicio y los otros dos para voluntarios participantes en distintos congresos como asistentes de primera línea

Cabe destacar que hemos tenido dos tipos de usuarios a los que hemos tenido que ofrecer formación, ocupando gran parte de nuestro tiempo:

- Personal de Primera Experiencia Laboral: compañeros trabajadores a los que hemos tenido que formar para que puedan desempeñar su primer trabajo, tal como es el objetivo. Se han hecho dos meses de formación para cuatro personas en esta área, dos de las cuales se han marchado al encontrar un trabajo diferente.
- Becarios de FP. De esta modalidad ha habido dos tipos de personas: dos de grado medio y dos de grado básico. A ambos grupos se les ha dedicado el tiempo que se ha podido, ya que en ocasiones, debido a la falta de personal (tres personas menos) no se le ha podido dedicar todo el tiempo que merecen. Han sido cuatro meses en las que se les ha dado formación sobre redes de datos y de voz, equipos de red (switches) y en instalaciones audiovisuales.

También se ha participado en el I Seminario sobre Gestión Pública Universitaria, organizadas por la gerencia de la Universidad.

Otras actividades.

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

- Webinar "Da el salto de Excel a Power BI"
- Webinar "Plataforma VORTAL: Posibilidades que ofrece en la Contratación Menor"
- X Jornadas SAT
- Sesión Continuidad de Negocio para Universidades. Telefónica
- Actualización de la Plataforma de Veeam: V11A y más
- Backup & Disaster Recovery en Universidades
- Webinar Open Education Analytics
- Webinar EMMA y la adecuación al ENS para Universidades

Actividades de concienciación

A destacar la participación obligatoria de todo el personal en las siguientes videoconferencias organizadas por RedIRIS:

- Experiencias con ransomware en la Universidad de Castilla – La Mancha
- Experiencias con ransomware en la Universidad Autónoma de Barcelona

Además de las acciones puramente formativas, el personal del Área ha participado en las siguientes actividades, todas ellas en modalidad virtual o híbrido presencial/virtual:

- Actualización del ENS en las AAPP
- Microsoft Power Platform Virtual Training Day: Fundamentals
- Cloud para Docencia y Ciberseguridad

- Jornadas indetiSIC 2022
- TECNIRIS-82: Servicio @FIRMA de RedIRIS
- Seminario Gestión Pública Universitaria. Experiencias Transformación Digital
- Webinar containers, la tormenta perfecta