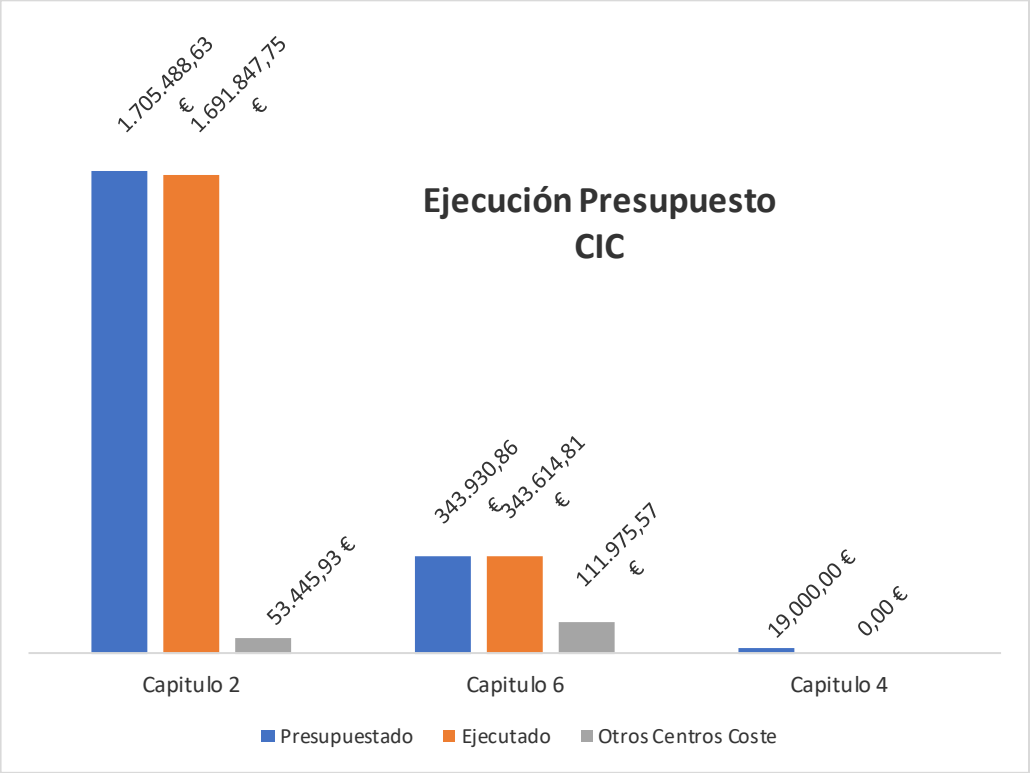
GESTIÓN ADMINISTRATIVA

Gestión Económica

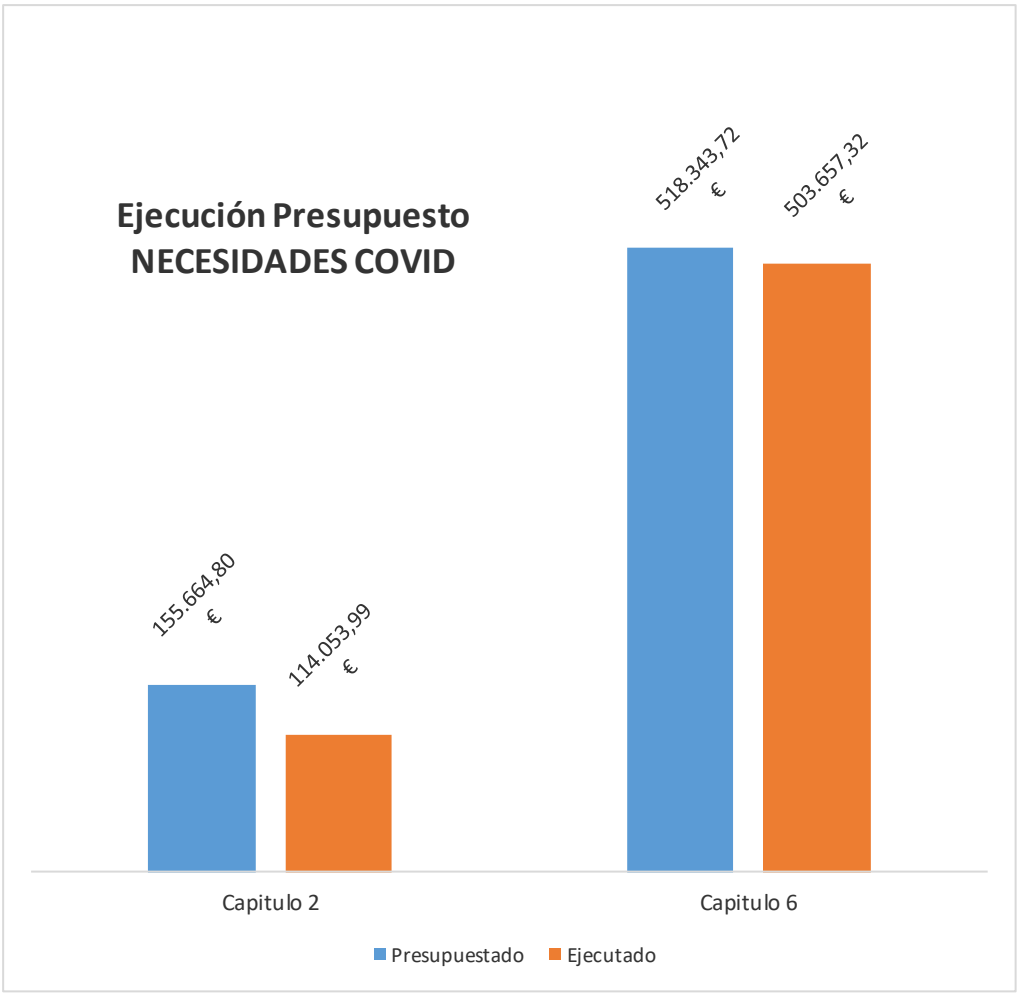
Las tareas relacionadas con la contratación de servicios y suministros son las que suponen una mayor carga de trabajo para la Oficina de Gestión Administrativa.

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 2021.



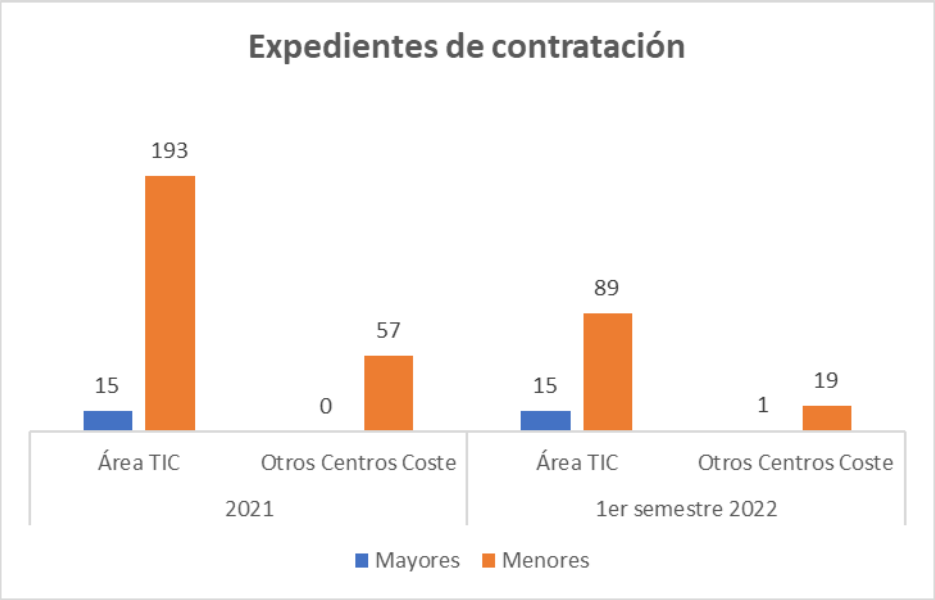
Con motivo de la pandemia de COVID-19 y para atender a las necesidades específicas en materia de equipamiento derivadas de la misma se dota al Centro de Informática de un centro de coste económico diferenciado, cuyo grado de ejecución en el ejercicio se muestra en el siguiente gráfico:



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 recae 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 2021 y el primer semestre de 2022.



Estos expedientes de contratación han generado la tramitación de 459 justificantes de gasto durante el ejercicio 2021 y de 156 durante el primer semestre de 2022.

Las contrataciones de inversiones con cargo al capítulo 6 han supuesto la tramitación en el año 2021 de 1.442 fichas de inventario y de 232 en el primer semestre de 2021

Otros trámites administrativos

A solicitud de los proveedores, se han emitido durante el curso 2021/2022 un total de 10 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 48 comunicaciones y recibido 18 a lo largo del curso.

Por otro lado, se han presentado 90 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 164 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.

La Gestión Administrativa del Área de TIC está en continuo proceso de digitalización, reduciendo la emisión de documentación en formato papel a aquella cuya normativa específica exija tramitación y firma de documentación en soporte documental. Esta opción se ha mostrado de gran utilidad para la gestión en la modalidad de teletrabajo. La no dependencia de la documentación en formato físico ha permitido continuar con la gestión administrativa en la modalidad de teletrabajo con un nulo nivel de incidencias.

GESTIÓN DE SEGURIDAD

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.

El objeto de la norma es la actualización del Esquema Nacional de Seguridad (ENS) para adaptarlo a la nueva realidad normativa y al incremento de las ciberamenazas tanto cuantitativa como cualitativamente, y así poder garantizar una respuesta más adecuada ante los ciberataques, propiciando la resiliencia de los sistemas, y proporcionando un tratamiento más seguro de la información y los servicios públicos.

Esta norma base de obligado cumplimiento para la UPO, obligará a la revisión de su política de seguridad y a la adecuación de la organización de la seguridad a la nueva normativa. Las novedades más significativas son:

- clarificación de la norma,
- redefinición de responsabilidades y organización de la seguridad,
- obligación de vigilancia continua y
- cambio en las medidas a aplicar:
    - Mayores requisitos para cumplimiento. Refuerzos en materias como gestión de la identidad.
    - Medidas nuevas para servicios en la nube y protección de la cadena de suministro.

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

El incremento de ataques con consecuencias graves en Universidades, pone el foco en la necesidad de crear un procedimiento que organice las actuaciones en casos de incidentes graves, recogiendo las responsabilidades de cada perfil, los cauces de comunicaciones y las acciones necesarias para garantizar el cumplimiento legal y la recuperación d ellos sistemas de forma organizada. Este procedimiento debería recoger las mejores prácticas reconocidas en la industria y la experiencia aportada por organizaciones similares compartida en foros sectoriales. Este procedimiento debería implicar a toda la organización y a todas sus unidades organizativas.

- Procedimiento de emergencia.

Se han generado los siguientes informes:

- INF_CIC-16_TECNIRIS_v.1.0.docx – Resumen de propuestas de mejora de los administradores de sistemas.
- INF_CIC-16_ENS_requisitos_sw_completo_v01r01.pdf – Informe de requisitos de seguridad ENS para proyectos de desarrollo a medida.
- INF_CIC-16_DptoAntorpologia_v.1.0 – pdf – Informe sobre situación configuración singular de equipos del Departamento de Antropología

- INF_CIC-16_botanica.pdf - Informe sobre situación configuración singular de equipos del Departamento de Botánica.
- Informe ejecutivo sobre gestión de incidencias durante 2020.

Se ha procedido a mejorar la operación de los siguientes procedimientos:

- Procedimiento de autorización de apertura de puertos
- Procedimiento de gestión de actualizaciones.
- Procedimiento de apagado/encendido de equipos

Comisión de Seguridad de la Información y Protección de datos

Tras el cambio del equipo de gobierno, Raúl Giráldez, en calidad de Vicerrector de Transformación Digital y Calidad y en calidad de Responsable de Seguridad, convoca sesión de constitución de la Comisión de la Seguridad de la Información y Protección de Datos (en lo que sigue la Comisión) el viernes 11 de marzo de 2022 y convoca la 1ª sesión ordinaria con el siguiente orden del día:

- Presentación de la Comisión y contextualización.
- Aprobación, si procede, de la actualización de la política.
- Aprobación, si procede, de los niveles de riesgo.
- Informe INES.
- La seguridad TI.
- Ruegos y preguntas.

Durante la sesión se presenta la Comisión y se presentan los roles y organización de la seguridad que se contempla en la política de Seguridad de la Información y Protección de Datos de la Universidad, para establecer las responsabilidades asociadas a cada uno de los integrantes de la Comisión.

Se informa y aprueba, según el procedimiento establecido, los niveles de riesgo y la actual Política de Seguridad en su revisión anual obligatoria.

Se informa sobre las obligaciones derivadas del cumplimiento normativo y se hace un resumen de las principales actividades del CIC en relación a la Seguridad.

Se realiza una labor importante de concienciación, para entender que más allá de las acciones técnicas en la implantación de medidas de seguridad, debe haber un gobierno de la seguridad, fuera del ámbito TIC, que promueva los cambios necesarios para permitir la implantación de la seguridad como proceso integral, no solo asumiendo cada individuo su responsabilidad en función del rol dentro de la organización, sino como organización en sus procedimientos y normativas.

Se acuerda abordar en una segunda sesión los objetivos y las estrategias a marcar para conseguir el cumplimiento normativo y mitigar los riesgos asociados a la seguridad de la información

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 7.4, dando continuidad a los criterios establecido en análisis anteriores.

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): 3,5 (escala 0-10) – ALTO.

Se genera la siguiente documentación:

Informe ejecutivo INF_CIC-16_analisis_de_riesgo_2022.doc.
SOA_Declaración de Aplicabilidad de Medidas del ENS_2022.
Fichero de análisis de riesgo 2022.

Se genera también el valor del indicador de gestión de la seguridad establecido en marco con un valor de 2,87. 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 detecta una revisión necesaria para el análisis de riesgo siguiente en relación a la aprobación del nuevo ENS.

Se aprueban los niveles de riesgo en la reunión de la Comisión de Seguridad de la Información y Protección de datos de 11 de marzo de 2022.

Los valores del riesgo no 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.

Se han realizado también análisis de riesgos asociados a solicitudes de modificación de la configuración de seguridad. Estos análisis de riesgos ser realizan cuando se solicita la incorporación o modificación de nuevos sistemas integrados en la Universidad y no gestionados por el CIC, o cuando se solicita la modificación de una configuración de seguridad particular como en lo referido a al uso de usuarios genéricos para servicios de préstamo de dispositivos.

En estos casos se analiza la solicitud, se obtiene la justificación y se realiza el análisis de riesgo. La solicitud se autoriza cuando está debidamente justificado, se aplican las medidas complementarias que garanticen mantener el riesgo bajo control o los sistemas ofrecen las garantías de seguridad suficientes para su integración. Incluir un elemento no seguro, o modificar una configuración de seguridad, podría ser la puerta de entrada para un atacante y provocar un incidente que afecte a los servicios de la Universidad.

Gestión de incidencias de seguridad

En el periodo que contempla esta memoria se han registrado un total de 180 incidentes de seguridad. Estos incidentes tienen su origen:

- 7 administradores de sistemas.
- 3 CCN-CERT.
- 3 AndaluciaCERT
- 7 dirección CIC.
- 2 INCIBER-CERT.
- 1 jefe de Gestión de Seguridad.
- 1 proveedores de sistema externos.
- 2 proveedores con sistemas en la UPO.
- 9 responsables UPO externos al CIC.

- 12 sonda SAT-INET.
- 34 sistemas antispam.
- 95 usuarios UPO.
- 1 plataforma antivirus.
- 1 sistemas monitorización
- 2 otros.

En general hay una disminución de los incidentes de seguridad. Esto puede atribuirse a varios motivos:

- Mayor concienciación de usuarios.
- Periodo de inactividad de la Sonda.
- Integración de la seguridad desde el diseño atendiendo a requisitos de seguridad.
- Mejora en la protección perimetral y control de la superficie de exposición.
- Actualización de sistemas y corrección de vulnerabilidades.
- Mayor rigor en los procesos de autorización.

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 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.
- Modificación del procedimiento de gestión de cambios de datos de proveedores.

Notificación de incidentes

Se ha procedido a la notificación oficial al CCN-CERT de dos incidentes con peligrosidad alta:

- Incidente con impacto económico por la suplantación de identidad de un proveedor.
- Incidente con trabajador con acceso privilegiado a los sistemas.

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.

Alerta conflicto de Ucrania

Con motivo del conflicto de Ucrania y la elevación de los niveles de alerta ante el riesgo de incidente de ciberseguridad, el CCN-CERT, encargado de la coordinación a nivel nacional de las AAPP en lo referente a la respuesta a incidentes, ha establecido unos niveles de alertas y unas medidas a tomar en relación a la activación de un nivel u otro.

Esto ha obligado a las administraciones a implementar una serie de medidas y mantener un seguimiento activo de las mismas, dando reporte obligado al CCN-CERT.

Como consecuencia de esta situación y en relación con las medidas de seguridad se han realizado acciones coyunturales y se han impulsado, elevando su prioridad, proyectos planificados que estaban pendiente de ejecución:

- Reuniones diarias de seguimiento de acciones por parte de la Dirección del CIC.
- Bastionado de equipos terminales del CIC con acceso de privilegiado de administración de sistemas. Se ha procedido a la descarga de una nueva imagen con mayor control de la seguridad:
  - Cambio en método de autenticación en los equipos, para mejor y mayor control de la contraseña privilegiada de acceso a los sistemas
  - Retirada de aplicaciones obsoletas.
  - Unificación de aplicativos para un mayor control.
  - Retirada de Kaspersky como antivirus de equipo EndPoint.
  - Restricción de uso de cuentas de administrador.
- Despliegue de MicroClaudia (herramienta de protección anti ransomware) en servidores Windows para protección contra Ransomware.
- Apagado sistemático de equipos del personal del CIC fuera del horario laboral para reducir la superficie de exposición en periodos en los que los equipos permanecen desatendidos. Difusión de medida recomendada para los usuarios de toda la Comunidad.
- Clasificación de servidores en relación al horario disponibilidad necesaria para reducir la superficie de exposición. Implementación de encendido y apagados programados, manuales y encendidos puntuales.
- Programación de sistema de monitorización y alerta sobre equipos encendidos fuera de su horario previsto.
- Cambio de contraseñas de usuarios del CIC y de usuarios con acceso privilegiado a los sistemas.
- Llamada a la Comunidad Universitaria al cambio de contraseña para evitar el uso de contraseñas robadas con anterioridad a la fecha.
- Implantación para el CIC de perfil individual de acceso remoto con doble factor de autenticación para los accesos por VPN y actualización del software de acceso. Proyecto de despliegue de la medida a todo el personal PAS con acceso VPN a los servicios.
- Restricción de conexiones VPN de personal de apoyo al CIC de empresa externa.
- Segregación de la red del personal del CIC y personal de apoyo a los servicios.
- Distribución de soportes extraíbles y procedimiento de condiciones de uso para copia de seguridad manual por parte del personal del CIC, para garantizar una más eficiente recuperación en caso de incidente de seguridad.
- Inventario unificado de proveedores con acceso a los sistemas TIC.
- Procedimiento de actualización de portátiles de préstamo para adecuar la configuración de seguridad.
- Alta en el servicio de SinMalos de RedIris. Este servicio permite a través del análisis del tráfico de las organizaciones suscritas detectar y alimentar de forma automática el inventario de direcciones de Internet maliciosas. Esto permite crear un nivel de protección extra que bloquea el tráfico de conexiones con estas direcciones, con la ventaja de ser un sistema que se alimenta de forma automática e incrementa las capacidades de inteligencia aplicadas a la ciberseguridad.

Campaña de concienciación

Dentro del marco normativo de obligado cumplimiento y como buena práctica recogida en las normativas de referencia en gestión de la seguridad, se han llevado a cabo labores de concienciación.

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. También se ha percibido un menor número de incidentes relacionados con captura de contraseñas, lo que indica también una mayor concienciación ante la llegada de correo sospechosos.

Además de las carencias detectadas en años anteriores (personal de investigación referente a desarrollos a medidas de sus proyectos, uso de nuevas herramientas potenciadas en la pandemia, etc.) en relación a al formación y concienciación, se observan riesgos en el uso de certificados digitales personales, uso de equipos compartidos y falta de rigor en los procesos de autorización.

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.

Se está trabajando en un proyecto de colaboración (ver apartado específico) 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.

Consultoría externa

Gartnet

Durante este periodo se ha trabajado con un equipo de consultores Gartner que han hecho una aproximación a ciertos aspectos de la seguridad arrojando resultados sobre estado el estado de la seguridad en la Universidad, la identificación de factores críticos de riesgo y la priorización de tareas a realizar. Las áreas abordadas son:

- Security and Risk Management
- Security Program Priorities
- Identity & Access Management
- CCN Measures Implemented - MSE HE

Vmware

Se ha contratado un servicio de revisión del estado del sistema de virtualización basado en Vmware (Vmware Healthchecker), para revisión de configuración, seguridad y rendimiento por parte de una empresa especializada. Con este servicio se completaría la revisión a la que se han venido sometiendo los tres sistemas especialmente críticos (S.E.C.) desde el punto de vista de la continuidad de los sistemas.

- Sistema de virtualización.
- Sistema de copias de seguridad. -Revisado el año pasado -
- Sistema de bases de datos corporativas (ODA). - Revisado el año pasado -

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.

Este año se ha procedido a un cambio de versión de la sonda obligado por el CCN-CERT que ha necesitado una reinstalación completa, con nuevos requisitos. Esta instalación no ha estado exenta de incidencias con la dificultad del acceso restringido al equipo que impide realizar comprobaciones básicas. La comunicación con el soporte del CERT tuvo que derivarse a correo electrónico, ya que a través de la herramienta LUCIA para la gestión del seguimiento de actualización no obteníamos respuestas.

Durante el periodo que se contempla en la memoria se han resuelto un número de 20 incidentes notificados por la sonda. La bajada en el número de detecciones se debe al número de meses que no ha estado activa y a una mejora en los algoritmos de detección, que han minimizado las comunicaciones de incidentes.

Si bien el número de notificaciones recibidas es inferior a otros años, 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 más óptimas.

Se ha detectado un incidente de nivel medio con origen en un equipo NAS no gestionado por el CIC, que alberga una tecnología obsoleta que se ha visto comprometida y estaba estableciendo contacto con sistemas de gestión de malware que usan los atacantes.

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.

Siguiendo con los trabajos iniciados en periodos anteriores, se realiza un inventario de accesos PAM del personal técnico del CIC, para su análisis y registro.

Se auditan los trabajos realizados, abriendo líneas de trabajo que permitan continuar en la organización del inventario de usuarios y accesos.

En septiembre de 2021 se realiza el alta en el servicio Trillion que el CCN-CERT ofrece a las universidades públicas, sin ningún coste para alerta de credenciales comprometidas, que es uno de los principales vectores de entrada de posibles atacantes en los sistemas corporativos.

Esta herramienta mantiene una monitorización sobre el comercio de credenciales relacionadas con la Universidad. Haciendo análisis de los datos, se observa que muchos de los robos de credenciales corresponden con incidentes antiguos. No se puede establecer una correlación directa entre los datos que facilita este servicio y los incidentes de seguridad detectados con origen en el robo de contraseñas.

Gestión de la configuración

Se está completando la información del inventario actualizado por el personal de sistemas del CIC con la información necesaria para la gestión y control de tareas de seguridad.

Se ha generado una base de datos SEGSERV que completa los datos ya existentes en el inventario, para permitir gestionar y controlar:

- Responsables de operación y responsable de gestión del equipo
- Apagado /encendido de equipos
- Instalación de agentes de seguridad (EDR, microclaudia, antivirus, etc.)
- Gestión de actualización de equipos.

Para el parque de equipos clientes, se está realizando un proyecto piloto con la herramienta NAC Forescout de descubrimiento y control de acceso a redes. Esta herramienta permite el descubrimiento de dispositivo con acceso a la red corporativa, lo que permite contrastar los datos de inventario con los dispositivos localizados y localizar equipos desconocidos o no controlados por el CIC.

Se ha procedido a modelar la información referente a los servicios expuestos a internet, de manera que se estructura qué equipos son accesibles desde el exterior y qué servicios justifican estos accesos. Esta modelación permite una explotación ágil de la información que permite identificar de forma eficiente el riesgo asociado a estos equipos.

Se ha procedido también al la auditoria y revisión de filtros de conexión al exterior en las reglas de firewall y protección perimetral y a aumentar la información del inventario de servidores mantenido por el personal de sistemas.

Monitorización y control de equipos.

Se han realizado mejora en los servidores de nombres de dominios (DNS) que permiten mejor trazabilidad en caso de incidentes de seguridad.

Se ha iniciado un proyecto de despliegue de sistema EDR-MDR de la empresa Crowdstrike en los equipos del CIC. Los sistemas EDR son sistemas avanzados de alerta y respuesta que permiten identificar incidentes de seguridad en sus fases iniciales y permiten una respuesta más temprana y ágil ante incidentes. Estos sistemas funcionan de forma complementaria a los sistemas de antivirus especializados en la detección de malware. Además, aportan una telemetría mucho más completa que permite una mejor configuración de políticas de seguridad y un mayor control referente a los IOC (indicadores de compromiso) que puedan afectar a los dispositivos controlados. Permite saber, por ejemplo, qué equipos presentan un comportamiento relacionado con algún síntoma de ataque o si un ataque se está propagando de forma silenciosa entre equipos de la red corporativa.

Este proyecto incluye no solo equipos finales de administradores de sistema, incluye servidores tanto Windows como Linux compatibles con el sistema EDR.

En los equipos del CIC se está procediendo de forma progresiva a la retirada de Kaspersky como aplicación antimalware de punto final, tras las recomendaciones emitidas por el CCN-CERT y su sustitución por Windows Defender. Este cambio será propagado al resto de equipos gestionados por el CIC (equipos homologados) cuando se hayan adaptado las nuevas configuraciones y herramientas que apoyan al despliegue de políticas asociadas a estas herramientas (cambios de configuración, despliegue de actualizaciones, gestión desatendida de instalaciones, etc.).

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. 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 14 vulnerabilidades muchas en relación a tecnologías de publicaciones de páginas web o de virtualización. De especial criticidad fue tratada la vulnerabilidad en Apache Log4j 2, componente de java que obligó a revisar cada uno de los sistemas corporativos y aplicar las soluciones que aportaron los proveedores afectados. Supuso un esfuerzo de coordinación entre personal técnico, proveedores y servicios de respuestas a incidentes para prevenir incidentes de alto impacto en los servicios públicos.

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 2 notificaciones a OCU en relación a vulnerabilidades de sistemas nuevos puestos en producción.

Se mantienen las acciones de seguimiento de sistemas operativos obsoletos que ya no tienen soporte de manteamiento 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.

Sistemas de Copias de seguridad

Se continúa mejorando el sistema de backup, como elemento fundamental para garantizar la recuperación y continuidad del negocio. Los ataques de ransomware se están especializando en alcanzar y destruir las copias de seguridad, lo que impide la recuperación de los servicios atacados y obliga a pagar el rescate a los atacantes.

Se mejoran las capacidades de copia de primer y segundo nivel, se implementan medidas para la inalterabilidad de las copias y se destinan recursos para la realización de copias offline.

MicroClaudia y ransomware

Al despliegue ya realizado en periodos anteriores para protección de equipos finales, se ha añadido el despliegue en equipos servidores Windows que son los más afectados por los ataques de ransomware. Se ha instalado en un total de 39 equipos servidores. S eha incorporado también a la plantilla de creación de equipos virtuales de Windows para garantizar continuidad en el despliegue.

Microclaudia proporciona protección contra malware de tipo ransomware a sistemas Windows mediante la instalación de un agente ligero que despliega vacunas en el equipo. Se denomina vacuna a un mecanismo que impide que el malware se ejecute en un equipo. A diferencia de un antivirus, en donde la detección se realiza tras la ejecución de alguna acción por parte del malware, lo que se persigue con microCLAUDIA es evitar que éste ni siquiera llegue a ejecutarse en el equipo.

Actualmente se encuentran gestionados 1303 equipos con un total de 103 vacunas desplegadas y 133468 ejecutadas desde el arranque del proyecto.

Formación

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

- Configuración segura de Windows.
- Jornadas IDENTI::SIC 2021 "Cara a cara con la identidad".
- XV Jornadas STIC.
- Webinar demostración para Universidades de la solución EMMA del CCN-CERT
- TECNIRIS - Universidad Castilla la Mancha Experiencias con Ransomware.
- Sesión Continuidad de Negocio para Universidades.
- CCN-CERt: Nuevo Esquema Nacional de Seguridad.
- Webinar 'Backup & Disaster Recovery en Universidades.
- Webinar Backup en Office 365 & Azure.
- CRUE-TIC Experiencia de la URV con la integración entre su SSO basado en CAS y Azure AD.
- Jornadas SAT-INET
- Sesión formación TRILLION.
- Jornadas formativas Intune y Windows defender.
- Jornadas formativas Kaspersky.

Tras la sesión formativa sobre la experiencia de ataques graves en otras universidades, a las que asisten los administradores de sistemas, se realiza una puesta en común y una serie de propuestas de mejora en los procedimientos actuales. Esta información se recoge y se acometen acciones a corto plazo y se planifican otras para mejorar los procedimientos.

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 29,84%.
- Indicador de mejora continua 29,84%.

No aparecen datos referidos a 2021 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:
Memoria Área de TIC 2021-2022

- 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 11 de marzo de 2022.

Otras

- Actualización de portátiles de préstamos en situación de pandemia
- Bloqueo de conexiones por países a Myapp.
- Restricción a los servidores de Alma para la zona de Europa.

SERVICIO DE APLICACIONES Y SISTEMAS

Administración Electrónica y TIC

La introducción 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

Se han acometido diversas actualizaciones de otros tantos sistemas básicos de Administración Electrónica. Se enumeran a continuación los logros en torno a este grupo de actividades:

Oficina Virtual

El sistema está basado en el aplicativo Solicit@, y se compone de los siguientes módulos:

- Generador de Formularios: módulo que agrupa todas las funcionalidades necesarias para realizar el diseño y la gestión de los formularios que se presentan al ciudadano.
- Administración: gestión completa de los procedimientos publicados por la Universidad, así como de los trámites presentados por el ciudadano.
- Oficina Virtual: portal Web desde el cual, el ciudadano realiza la cumplimentación, firma y presentación telemática de los trámites publicados por la Universidad.

Dicho aplicativo, se modificó por parte de la Universidad para adaptarse a nuevas necesidades:

- Se modificó el comportamiento inicial de la Oficina Virtual para que sea posible presentar solicitudes telemáticas sin necesidad de firmarlas digitalmente, siempre y cuando estos procedimientos se hayan configurado previamente.
- Se acometió el cambio de la aplicación de pago telemático asociada a la Oficina Virtual. Debido a una imposición técnica legal, la TPV de este servicio dejaba de funcionar como lo hacía en la actualidad, para pasar a funcionar sobre la necesaria encriptación de los datos en formato SHA256.
- Se incluyeron nuevos atributos en los perfiles de usuarios para que sea posible acceder a determinados procedimientos, aunque no sean de su colectivo (PAS, PDI, estudiantes).

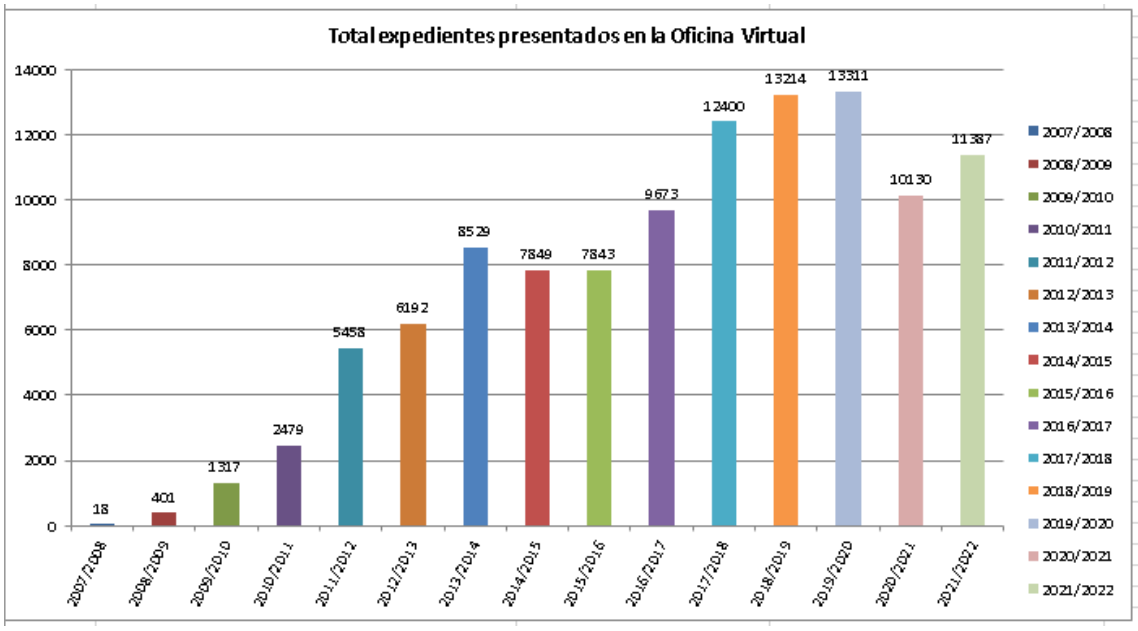
- El acceso a dicha Oficina Virtual se podía realizar inicialmente con certificado digital, con DNIe o sin certificado. Pero con la opción de acceso sin certificado no ofrece las mismas funcionalidades que con certificado electrónico o DNIe, por lo que se adaptó dicho aplicativo, para, incluir el acceso mediante integración con adAS (sistema de Single Sign On). Este nuevo tipo de acceso permite que los todos los integrantes 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 miembro de la Universidad, para acceder a la Oficina Virtual.

El acceso a la Oficina Virtual de la UPO mediante adAS UPO se considera equivalente al acceso con certificado digital, ya que se utilizan credenciales validadas y certificadas por la Universidad. Por esta razón, el acceso a la Oficina Virtual con adAS mantiene las mismas funcionalidades que el acceso con certificado digital o DNIe.

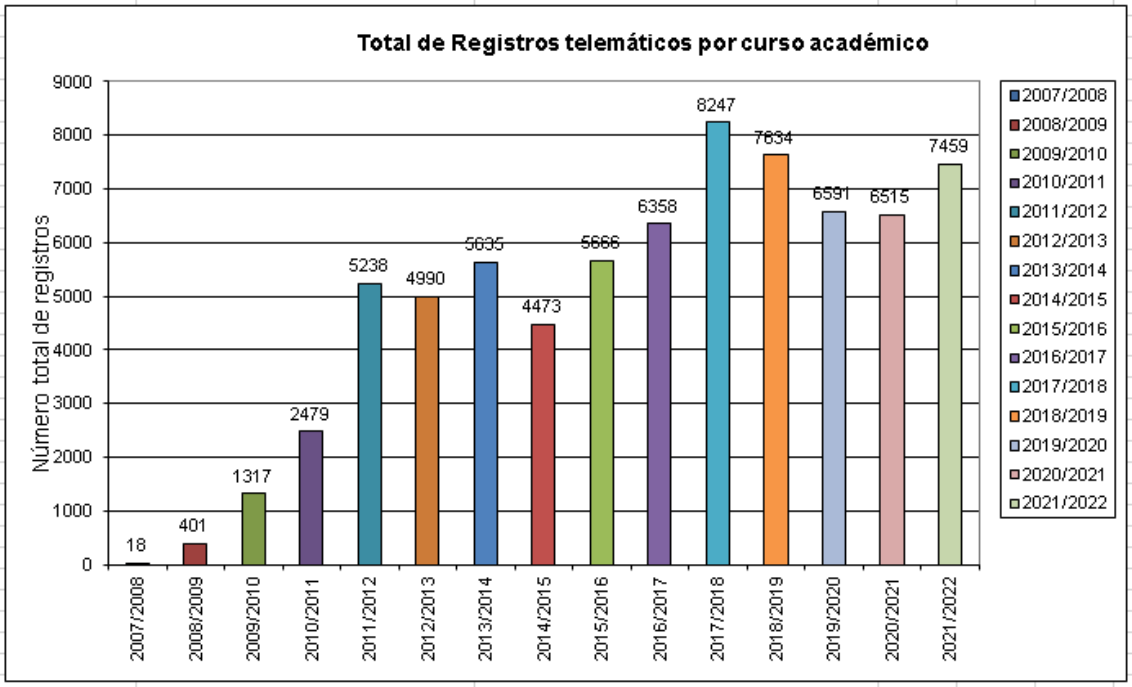
Esta acción, en definitiva, mejoró tanto la seguridad de acceso como la accesibilidad, ya que emite el acceso mediante credenciales de usuario, o mediante certificado digital, o DNIe.

Trámites presentados a través de la Oficina Virtual

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



Evolución por curso académico de expedientes presentados a través de la Oficina Virtual con registro telemático:



Oficina Funcionario Habilitado

Apoyo en la creación y mantenimiento de la oficina de asistencia al ciudadano, en su relación con la Universidad, en la que se han instalado una serie de equipos que el ciudadano podrá utilizar para presentación de trámites electrónicos y será asistido por funcionarios habilitados para este fin por la Universidad Pablo de Olavide.

@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.

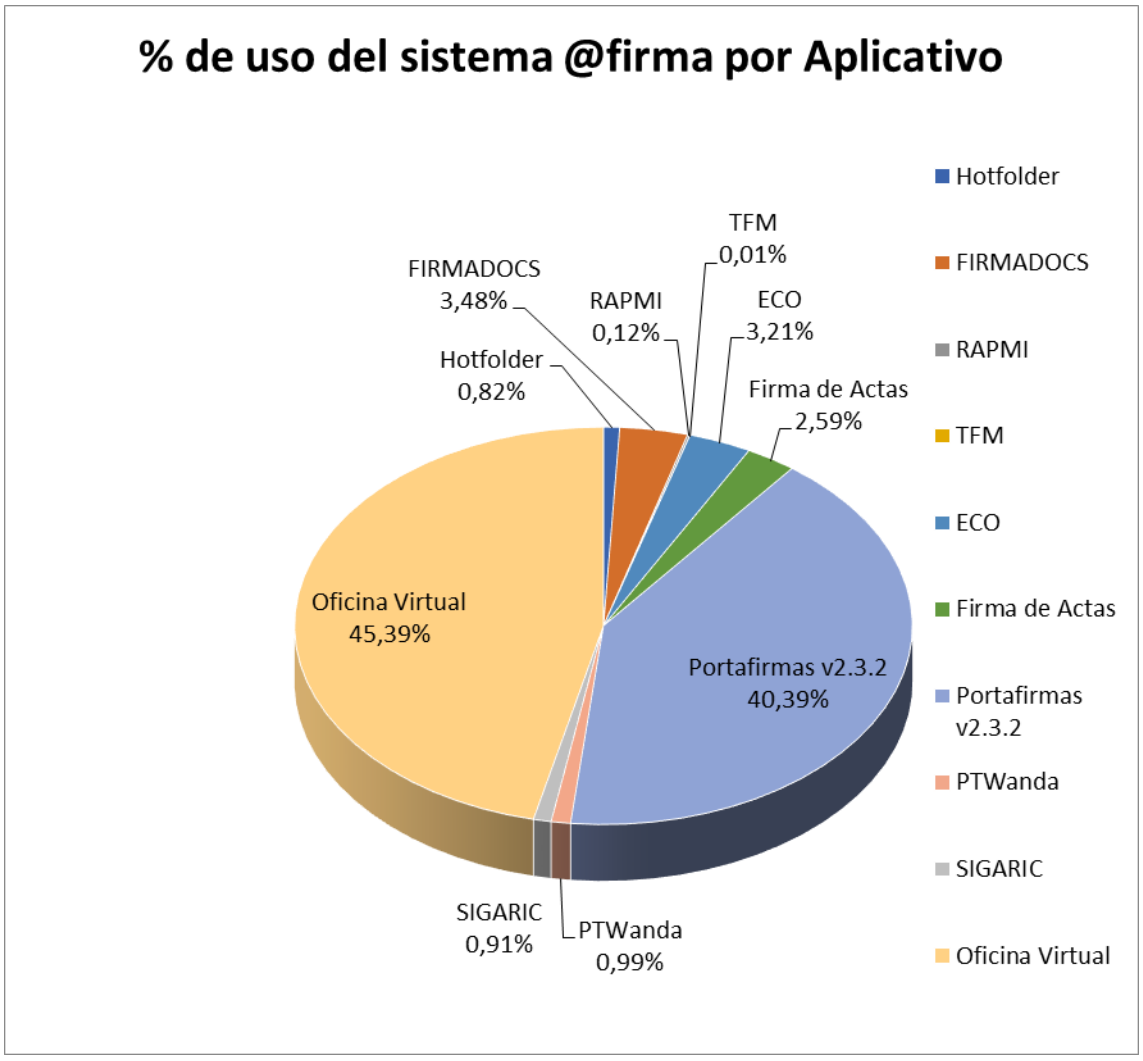
@FIRMA dispone de capacidades y funcionalidades, tales como la autenticación y firma con el DNI electrónico, firma en dos fases, uso de los formatos de firma CMS, XADES, XMLDSignature, CADES, PKCS#7..., no obligatoriedad del uso del servicio de custodia de documentos, firmas con sellado de tiempo, validación de certificados mediante OCSP, gestión de estadísticas de uso, auditoría y trazabilidad de las transacciones, etc.

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:

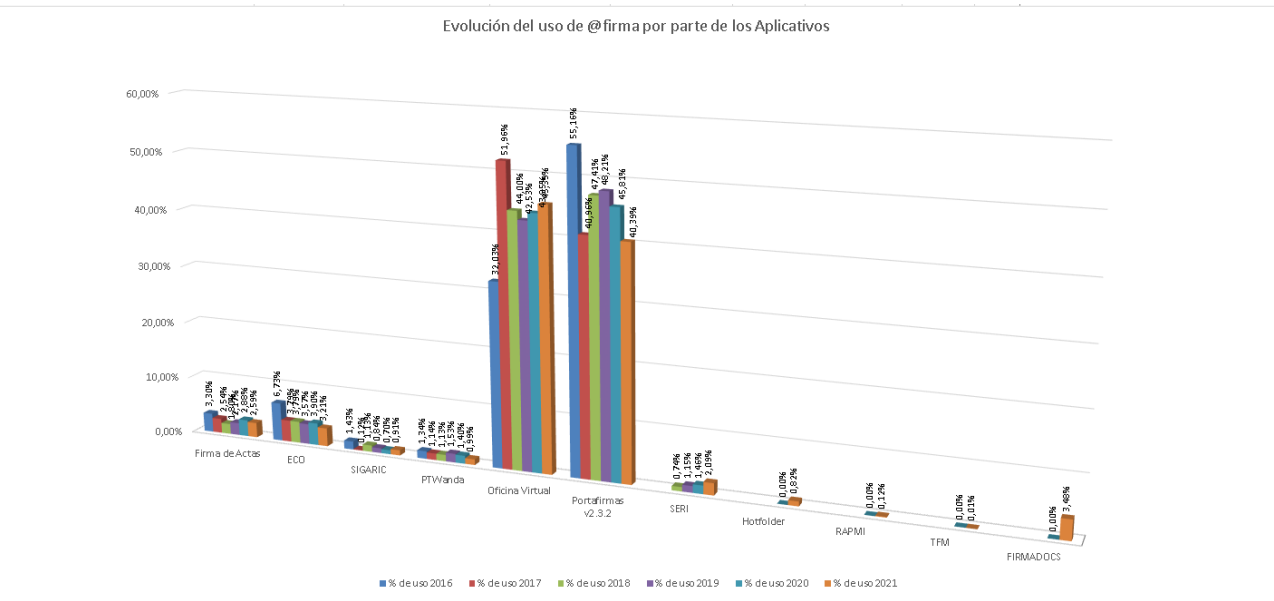
- Autenticación: Proceso que permite autenticar o identificar de forma fehaciente a una entidad basándose en la comprobación de su certificado digital.
- Validación de firmas: Proceso que permite determinar si una firma es válida o no. Se comprueba tanto la validez de la firma (formato y atributos) como 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 son Portafirmas 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.

También podemos observar en ella un aplicativo que comenzó a usarse el curso pasado, Hot Folder. 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.



Portafirm@

La aplicación Port@firmas 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 las mismas. Dicho sistema se puso en marcha el 21 de Octubre de 2008 a partir de la publicación en el BOJA num. 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.

Entre las funciones implementadas por el sistema destacan:

- **Gestión de la firma de documentos**: Consiste en una interfaz web que conocemos como 'escritorio de firma', dividida en tres partes: documentos pendientes de firma, documentos pendientes de la firma de un firmante anterior (para firmas en cascada), documentos firmados por el usuario y documentos enviados de nuevo al emisor.
- **Verificación de firmas de documentos**: Esta función consiste en una interfaz web que, a partir del código seguro de verificación del documento firmado, permite recuperar y mostrar el original para su cotejo.

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. Al poder ser ejecutada desde el navegador, permite la firma en páginas de Administración Electrónica cuando se requiere la firma en un procedimiento administrativo.

Algunas de las funcionalidades que incorpora esta nueva versión son:

- Gestión Documental: Se puede establecer como gestor Documental Alfresco, haciendo uso de los servicios CMIS/Rest que ofrece desde su versión 4.X en adelante.
- Soluciones de Movilidad: Portafirmas tiene el interfaz adaptado y optimizado para funcionar en cualquier tamaño de pantalla, al tener un diseño "responsive".
- Eliminación de los applets como requisito para firmar: La aplicación ya integra con Autofirma tanto para los procesos de autenticación como para la firma masiva de documentos (firma en lote de Autofirma).
- Certificados soportados: Todos los certificados reconocidos por el Ministerio de Industria, entre ellos, certificados AP de la FNMT, Certificados Ceres y el DNIe.
- Sustitución de la firma remota por la "firma en trámite": La nueva funcionalidad permite acceder a una petición en concreto para la firma exclusivamente de la misma. Las aplicaciones clientes pueden por tanto suprimir la tarea de firma remota y cambiar por una ventana o inclusión de la URL que ahora se ofrece.
- Perfil de supervisor: Un usuario con este perfil tendrá una nueva bandeja en la que podrá ver todas las peticiones de firma de una o varias aplicaciones.
- Custodia de certificados dentro de Portafirmas: Los certificados se almacenan encriptados dentro de sobres digitales en Portafirmas y solo se le pedirá al usuario el PIN en el instante de la firma.
- Si el usuario recibe un cargo ya existente puede ver lo que se había hecho antes su predecesor o bien al quitarle el cargo se le oculta automáticamente todo lo que tuviera por el cargo que ocupara. Es una forma de organizar el trabajo y previene en caso de cambio de personal el tener que reubicar documentos que estaban a mitad del proceso de firma.
- Varios firmantes que pueden ser personas o cargos, y que a su vez entre ellos existan reglas automáticas de delegación o incluso realizadas por los propios usuarios.
- Firma de primer firmante: Un documento es remitido a varios firmantes, pero nos basta con que uno de ellos firme el mismo, no hay que esperar a que lo firme ninguno más.
- Posibilidad de añadir un "Visto Bueno" previo a la firma: Queda registrado a nivel de historial de la petición, pero no deja marcas sobre el documento o el informe de firma.
- Rechazo Fehaciente: Trasmitir mediante una firma, marca de agua en todas las paginas "RECHAZADO", así como luego en el informe de firma se indica el motivo del rechazo de forma obligatoria.
- Delegación y Sustitución: Definir filtros automáticos de delegación, de forma que todo lo que va a una persona, pase también a un segundo cargo o usuario de forma transparente tanto a los usuarios y las aplicaciones. Esta funcionalidad estaba limitada al concepto de "cargo" en las versiones antiguas (no se podía delegar directamente entre usuarios). Se puede hacer tanto a nivel de cargo como a nivel directo entre usuarios en las últimas versiones de la aplicación.

De esta forma las peticiones ya existentes o bien las nuevas que vayan llegando al sistema se les aplicará el filtro definido de forma que se ampliará o modificará los posibles firmantes de forma automática.

Estas funcionalidades se pueden activar o desactivar en su mayor parte por configuración, lo que permite que una misma versión pueda ser usada en distintas implantaciones adaptando el comportamiento de la misma a las necesidades que cada organismo e instalación.

- Modificación de líneas de firma: Sobre peticiones ya enviadas, vía servicios web, las terceras aplicaciones pueden modificar las líneas existentes, añadir o quitar, siempre si estas última no han sido firmadas aún. Desde la administración de la aplicación se permite también modificar peticiones enviadas al sistema para los casos puntuales que haya que corregir algo puntualmente. Obviamente no será el caso más común, dado que para ello están los filtros de delegación.
- Devolución con eliminación: Opcionalmente se puede combinar el rechazo fehaciente con la devolución con eliminación, que permite a un usuario eliminar físicamente una petición.

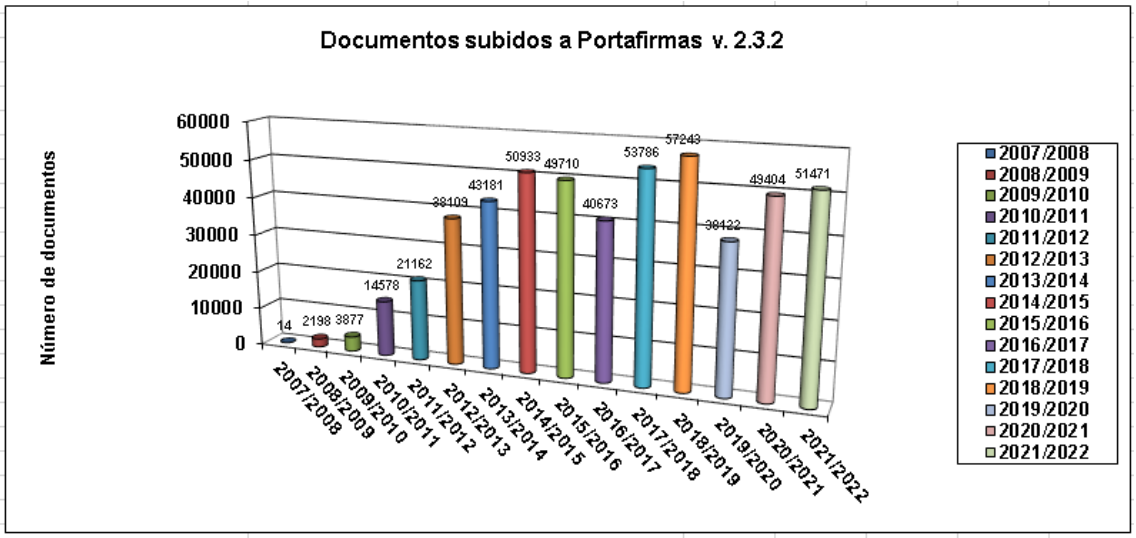
- Si el usuario recibe un cargo ya existente puede ver lo que se había hecho antes su predecesor o bien al quitarle el cargo se le oculta automáticamente todo lo que tuviera por el cargo que ocupara. Es una forma muy versátil y potente por tanto de organizar el trabajo y previene en caso de cambio de personal el tener que reubicar documentos que estaban a mitad del proceso de firma.
- Varios firmantes que pueden ser personar o cargos, y que a su vez entre ellos existan reglas automáticas de delegación o incluso realizadas por los propios usuarios

En un futuro, aparte del uso que actualmente tiene como aplicativo de firma digital de documentos, será utilizada por:

- Los elementos de la infraestructura de la nueva plataforma de tramitación G-ONCE, a la cual hacemos referencia más adelante en este documento.
- El proyecto Anot@ RCP (Registro Central de Personal), que se está implantando en la Universidad.

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

Aquí vemos la evolución del número total de documentos subidos a Portafirm@s v.2.3.2, que viene usándose en la Universidad desde el año 2007.



Desde la entrada en producción de la nueva versión de Portafirm@s (v3) el 24 /02/2022, se han subido a firma **14011** documentos a través de la misma.

Plataforma de Tramitación de Expedientes Administrativos

La Plataforma de Tramitación de expedientes administrativos, está basada actualmente en el aplicativo PTW@nda, en su última versión, y cumple con las indicaciones dadas por el ENI (Esquema Nacional de Interoperabilidad): formato de documento electrónico, expediente electrónico, etc.).

Plataforma de tramitación se basa a su vez en el motor de Tramitación Trew@, Las actividades básicas que recaen sobre Trew@ son:

- Define el flujo de trabajo de una tramitación (tareas a realizar, documentos relacionados con el trámite, circuitos de validación, etc.).
- Se utiliza como esqueleto para la puesta en marcha de nuevos procesos de gestión de expedientes.

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

.

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.

El funcionamiento de la aplicación consiste en:

1. Dentro de la configuración de la aplicación se define un directorio de entrada (Hot folder), el cual se estará observando continuamente para detectar la entrada de nuevos documentos.
2. Cuando se incluyan nuevos documentos en este directorio la aplicación los recorrerá de uno en uno y ejecutará los siguientes pasos:
   (1) Firmar el documento usando la firma de servidor configurada en el servidor @firma de la Universidad.
   (2) Una vez firmado el documento se ejecutará el procesado del documento, que dependerá del nombre del fichero. Este procesado enviará el documento firmado al destino de salida correspondiente al procesador seleccionado para el documento firmado.
   (3) Finalmente, si la firma y el procesado del documento son correctos se eliminará el documento de la carpeta de entrada y se pasará al siguiente documento.

Nuevos Procedimientos en Producción

En este periodo se han desarrollado los siguientes nuevos certificados de respuesta inmediata (SERI). Se enumeran a continuación:

- **Acreditación de abono de los derechos al Título de Grado**: A través de este servicio se proporcionará a los estudiantes un certificado acreditando el abono de los derechos al título de grado.
- **Certificado de Dirección de Tesis de Estudiantes de Doctorado en el curso académico actual**: A través de este servicio se proporciona al profesorado un certificado acreditando las tesis de estudiantes de doctorado que dirige/co-dirige o tutoriza en el curso académico actual.
- **Certificado de Curso de Formación Doctoral**: A través de este servicio se proporcionará al estudiante matriculado en los programas de doctorado de la UPO, un certificado acreditando la realización y superación de los distintos Cursos de Formación Doctoral ofertados por la Escuela de Doctorado de la Universidad Pablo de Olavide.

Sede Electrónica

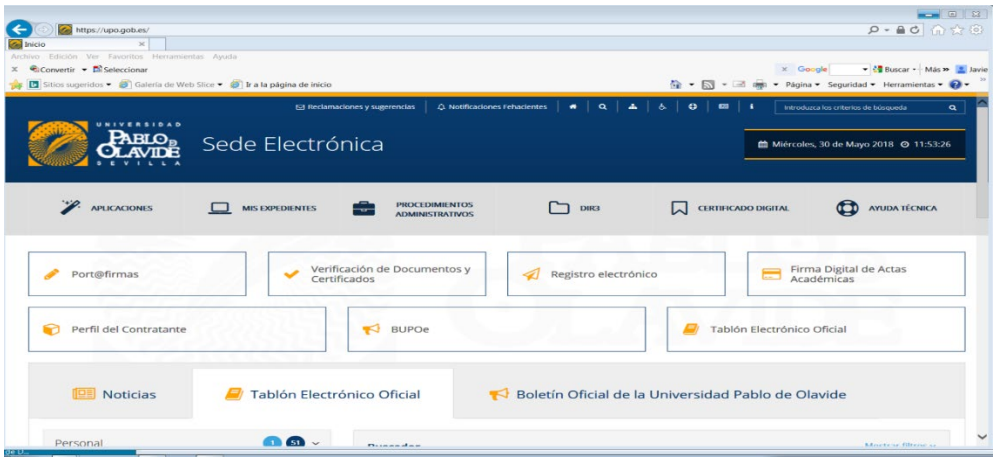
La sede electrónica de la Universidad Pablo de Olavide está disponible en la dirección web https://upo.gob.es/ desde septiembre de 2011. El Reglamento de Establecimiento y Funcionamiento de esta sede que da acceso a

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.

Se acaba de renovar el certificado de la sede emitido por la autoridad de certificación Camerfirma, vigente hasta junio de 2023. AC Camerfirma 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 que da cobertura a los requisitos legales requeridos desde el ENI y ENS.



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), con el fin de dar respuesta a los requisitos anteriores, ha puesto en marcha las medidas adecuadas para, con una capa de servicios, asegurar la adecuada gestión del mismo, garantizando:

- El acceso a la información, 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.
- La actualización y la coherencia de la información, disponiendo de mecanismos técnicos y formales que permitan mantenerla actualizada frente a los cambios que ésta pueda sufrir. En este sentido, el Directorio Común se enmarca en un modelo cooperativo de corresponsabilidad, aglutinando los datos de las diferentes Administraciones colaboradoras a través de una red de fuentes responsables, que

envían la información en base a un acuerdo bilateral de colaboración entre la DGMAPIAE y la Administración participante.

- 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 a las condiciones que se establezcan con las Administraciones proveedoras.
- La gestión de la codificación única de las unidades y oficinas reside en el propio Directorio.

Los organismos dados de alta para la Universidad Pablo de Olavide, de Sevilla, se encuentran publicados en la Sede electrónica de la Universidad en la siguiente dirección:

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

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 31 de mayo de 2021.

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.

Durante este tiempo se han llevado a cabo las siguientes actuaciones:

- Revisión de aplicación para detectar mejoras y cambios.
- Revisión de manuales y guías.
- Apoyo técnico para la elaboración de vídeos explicativos.
- Preparación de aulas para las sesiones de formación con todos los involucrados.
- Revisión de imagen del Sistema Operativo de los equipos nuevos para la Unidad de Registros de la UPO.
- Migración de equipos informáticos en la Unidad de Registros de la UPO.
- Despliegue masivo de acceso para GEISER para su comunidad de usuarios dentro de UPO.
- Integración de Instancia Genérica de UPO con GEISER.
- Integración de todos los procedimientos electrónicos de la Administración Electrónica con GEISER.

GEISER ha quedado 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.

Anot@

Implantación del componente de generación de Anotaciones y su integración con el servicio web de 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@.

Para ello se han llevado a cabo las siguientes actividades:

- Integración con la Firma digital de Anotaciones.
- Configuración y despliegue del API de firma.
- Configuración de la integración entre UXXI-RRHH y el API de firma.
- Pruebas técnicas de certificación de la integración.
- Integración con los servicios web de Anot@: EditaRCP y AnotaRCP del MINHAP
- Configuración de la integración entre UXXI-RRHH y los servicios de Anot@
- Formación a los usuarios de UXXI-RRHH: Integración con Anot@

Proyectos en desarrollo

G-ONCE (Plataforma de Tramitación).

G-ONCE es la 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.

G-ONCE se ofrece como solución básica, paquetizada, de forma modular y con los en componentes habilitantes de Administración Electrónica sobradamente probados en multitud de organismo públicos.

Actualmente nos encontramos en un proceso de licitación conjunta a nivel interuniversitario, habiendo hecho ya aportación de los procedimientos telemáticos en los que la Universidad tiene especial interés.

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 DNIe empleando plataformas de firma electrónica avanzada.
- Catálogo de procedimientos: se incluye una serie de procedimientos comunes plenamente operativos que pueden ser parametrizados y ampliados.
- Asistente guiado de trámites que permite guiar paso a paso a los ciudadanos y usuarios en las solicitudes.
- Firma electrónica de documentos, formularios, solicitudes etc.
- Portafirmas electrónico.
- 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.
- Digitalización certificada homologada por la AEAT.

Alfresco (Gestor Documental).

La situación actual de la Universidad incluye dos implantaciones de Alfresco distintas:

- - Alfresco CE 3.3 (para la plataforma de tramitación actual, PTWanda)
- - Alfresco Enterprise 5.1.2, para:
    - Firma de Actas (Firma de Actas Académicas)
    - Expedientes PDI (Personal Docente e Investigador)
    - Aplicación RAPMI (Gestión de solicitudes de movilidad nacional e internacional)
    - Documentación de usuarios internos de la Universidad
    - Documentación migrada de la antigua versión de Alfresco de SGIC (Sistema de Garantía Interna de Calidad). Cuando termine de desarrollarse el nuevo aplicativo este repositorio quedará como histórico.
    - SGIC (Sistema de Garantía Interna de Calidad)
    - TFM (Trabajos Fin de Master)
    - Varias aplicaciones que se están desarrollando:
        - Automatrícula Fundación
        - TFG
- Alfresco Enterprise 7.1 y 7.2
    - Se tiene previsto acometer la migración de la versión 5.1.2 a las 7.x de la plataforma.

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.

El intercambio de datos entre AAPP es por tanto una tarea fundamental a la hora de prestar servicios avanzados de administración electrónica a los ciudadanos, mejorando la eficiencia y eficacia de las *organizaciones*.

Se usa en otros organismos, en muchos servicios, como: Consulta de estar al corriente de Deuda con la TGSS Consulta de estar al corriente de pagos con la AEAT Servicio de Comunicación del Cambio de Domicilio Servicio de Consulta de la Renta Servicios de Verificación de Datos de Identidad y de Residencia, Servicios de consulta de estar dado de alta en la TGSS1.

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 se ha seguido avanzando en la mejora de las prestaciones que ofrece la plataforma Docker. El número de aplicaciones hospedadas en espacios de base contenedor ha seguido creciendo, respondiendo la plataforma de manera muy satisfactoria. Se ha podido ensayar con éxito la actualización de imágenes antiguas y la incorporación de otras nuevas. También en el ámbito de la seguridad, sigue siendo de interés la ausencia de incidentes en comparación con la tecnología precedente.

Se ha incidido también en parametrizar y definir los procesos administrativos de migración de contenidos procedentes de terceros (típicamente empresas externas de diseño web). Los desarrollos cada vez son más sofisticados, con los que este mecanismo parece haberse establecido como la opción de preferencia para el desarrollo web en proyectos de investigación y algunos contenidos institucionales. Se han seleccionado plugins específicos para exportación/importación y definido el alcance del proceso por cada parte (universidad-empresa), lo que agiliza bastante el tiempo de puesta en producción.

Por otro lado, se ha finalizado la fase de implantación y puesta en producción de la segunda plataforma basada en contenedores. La idea para esta segunda instancia era desarrollar un sistema de alojamiento web no centrado específicamente en WP. Se está utilizando para el alojamiento de ficheros, aplicaciones dockerizadas por terceros, aplicaciones web corporativas especiales (biblioteca, administración electrónica), etc...

A diferencia de la plataforma WP, que dispone de una configuración específicamente orientada a este tipo de contenedores, en esta nueva instancia, la configuración se realiza a nivel de contenedor, no de plataforma, con lo que puede adecuarse a cada caso de manera más individualizada, proporcionando igualmente todas las facilidades que ofrece la tecnología.

Durante este año también se ha procedido a la retirada de las antiguas instancias de base OpenCms (migradas a los nuevos sistemas en producción) y de los servidores LAMP de la tecnología precedente (salvo algún aplicativo residual cuya migración también es inminente).

Con respecto al servidor proxy web HAProxy, comentar que ha seguido operando sin novedad durante el presente curso. Se estudia la posibilidad de realizar una nueva actualización (no prioritaria por el momento) una vez valorado el calendario de liberación de versiones del desarrollador.

Correo electrónico

El sistema de correo de la Universidad Pablo de Olavide, está basado en software libre y se adapta a las necesidades de usabilidad, capacidad, disponibilidad y seguridad actuales.

Se trabaja de forma activa en el servicio para implementar mejoras y actualizaciones que permitan mantener al día este servicio.

En el momento actual es imprescindible redoblar esfuerzos en lo que a seguridad se refiere. En este contexto, se sigue aplicando una mejora continua tanto en los protocolos de actuación como en las salvaguardias que protegen el sistema de correo ante los nuevos y diversos tipos de ataques, adaptándolos y mejorándolos tras

cada nuevo incidente. Se mantiene la eficacia y la rapidez con la que se detectan ataques por captura de credenciales, logrando detenerlos de forma rápida y efectiva. También se sigue colaborando de forma activa con el Instituto Nacional de Ciberseguridad para mejorar la gestión y tratamiento de los diversos incidentes de seguridad, así como contenerlos de forma adecuada.

Gestión de identidades

El servicio de Gestión de Identidades facilita el acceso a diferentes servicios mediante usuario y contraseña, tarjeta inteligente o DNI electrónico. Es la puerta de entrada tanto para el acceso a SIR (Sistema de Identidad Federado de las Universidades Españolas) como para un creciente número de servicios ofrecidos por la Universidad, entre los cuales destacan “Aula Virtual, “Oficina Virtual”, “Firma automatizada”, “Repositorio Seguro”, “Formación Plan Docente”, “Laboratorios Virtuales”, “Servicio de Biblioteca”, etc. También es la puerta de entrada a determinadas aplicaciones, que gracias a la integración de nuestro servicio de Identidad con el sistema de Identidad Electrónica para las Administraciones “@Clave”, permite y facilita el acceso a determinados usuarios externos a la Universidad a dichas aplicaciones.

Se han aplicado las últimas actualizaciones disponibles para mejorar tanto la seguridad como las funcionalidades de este servicio.

Se ha verificado la importancia de haber implementado nuevos controles de seguridad para evitar diversos ataques al servicio, en especial los de fuerza bruta. Estos controles han evitado de forma efectiva los numerosos intentos de ataque que sufren los servicios informáticos de forma generalizada.

Por otra parte, seguimos trabajando en un nuevo proyecto de mejora global del servicio de Gestión de Identidades, que pretende evolucionar los actuales procedimientos y sistemas de gestión de las identidades y accesos, incorporándolos en un diseño global con objetivos ampliados y definidos.

Almacenamiento

Se ha seguido trabajado tanto en la actualización de los sistemas de almacenamiento de la Universidad como en la retirada de sistemas más antiguos. De esta forma se garantiza una mejor seguridad y disponibilidad en el acceso a los datos.

Se está trabajando en sustituir la tecnología actual de conexión a nuestros sistemas de almacenamiento, de tal forma que se modernice, flexibilice y facilite la ampliación y mejora del servicio en el futuro.

Debido a la gran demanda de espacio de almacenamiento por los diferentes servicios de la Universidad, se ha seguido trabajado en la ampliación de la infraestructura de almacenamiento. De esta forma, se logra ofrecer todo el almacenamiento requerido por los diferentes servicios que lo requieren.

En especial y debido a los recientes ataques sufridos por entidades públicas y privadas del tipo ransomware (un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos), hemos seguido aumentando el espacio disponible para alojar copias de seguridad, así como implementando medidas de protección sobre dichas copias para asegurar la inmutabilidad de las mismas ante cualquier evento.

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 para gestionar las solicitudes de movilidad nacional e internacional (antiguo RAPMI) En marzo de 2022 se puso en marcha una aplicación, desarrollada en lenguaje PHP y base de datos Oracle, que ayuda a la gestión de solicitudes del alumnado que quiere realizar estancias de movilidad tanto ERASMUS, internacional, como nacional (SICUE), desarrollada por la empresa Cibernos. La gestión abarca desde el mismo momento en que el estudiante realiza la solicitud como hasta cuando regresa de su estancia y se le reconocen las calificaciones obtenidas, incorporándose éstas a su expediente.
  La plataforma incluye validaciones por parte del tutor académico, consultas y gestiones por el Área de Relaciones Internacionales, y consultas por parte del Área de Gestión de Matrícula y Expediente Académico.
- Se amplía la funcionalidad de la aplicación de Horarios y se crea una nueva versión para los horarios de postgrado independiente de la de Grado.
- Se comienza el piloto de una nueva aplicación de generación y gestión de horarios de la empresa Bullet: Bullet Calendar y Bullet Time Tabler.
- Se comienza la implantación del componente de Preinscripción de Estudios Propios de UXXI-Académico.
- Se comienza la implantación y validación de un nuevo tablero de datos con la tecnología de Oracle BI para la obtención de datos de alumnos.
- Se inicia un piloto con Microsoft para la automatización de procesos que se hacen manualmente.
- Se ha terminado la migración de todas las bases de datos a la versión Oracle19c RAC y alguna residual en Oracle 12c RAC..

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

- Etempo: actualización de versión, parches de seguridad, migración de base de datos, evoluciones, mejoras, etc.
- Etempo Pruebas: instalación de cero de entorno de pruebas para el aplicativo etempo.
- Gescontrat@: actualización de versión y parches de seguridad. Trabajándose en la migración a Windows Server 2022.
- Nice: Actuaciones de seguridad en la aplicación i2a Cronos de reservas deportivas.
- Eurowin: Actuaciones de seguridad en la aplicación SAGE.
- Eit: Evolución de la plataforma, migración de servidor y actuaciones de seguridad sobre la aplicación de Datio.

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 la integración de este aplicativo con UXXI-Investigación.
- Se acometen mejoras en UPOCompra en el tratamiento de compras con las agencias.
- Se va a actualizar la versión de la aplicación de control horario etempo

Aula Virtual

Durante el curso académico 2021-2022, el servicio de Aula Virtual ha estado trabajando intensamente en la migración de la plataforma de docencia virtual, Blackboard Learn, a la nube. A pesar de que la experiencia de usuario es similar a la de la versión anterior, esta migración proporciona una mejora tecnológica muy

importante respecto a la accesibilidad, el soporte, las actualizaciones, el mantenimiento y, sobre todo, la seguridad. El acceso a la plataforma se sigue realizando desde https://campusvirtual.upo.es

Como cada año, 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, plataforma de docencia virtual institucional. Como consecuencia del paso a la nube, hemos tenido que adaptar todos los procesos relacionados con las tareas de gestión de la plataforma.

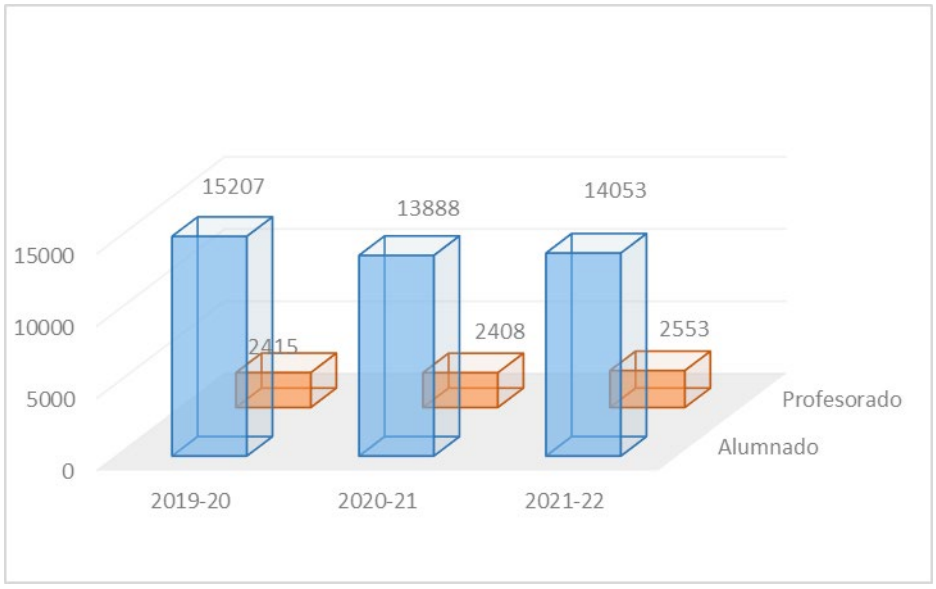
Desde el servicio de Aula virtual se ha procedido de oficio, a crear todos los espacios virtuales de docencia virtual del curso académico 2021-22, tanto de estudios de Grado como de Postgrado. A petición del CUI se han creado todos los espacios virtuales necesarios para el apoyo a la formación de los alumnos internacionales. Del mismo modo se han creado los espacios virtuales para la actividad docente de los cursos de Formación Permanente.

Durante el curso académico 2021-2022 las tareas planificadas dirigidas a la mejora del rendimiento de la plataforma y a la satisfacción de los usuarios han sido:

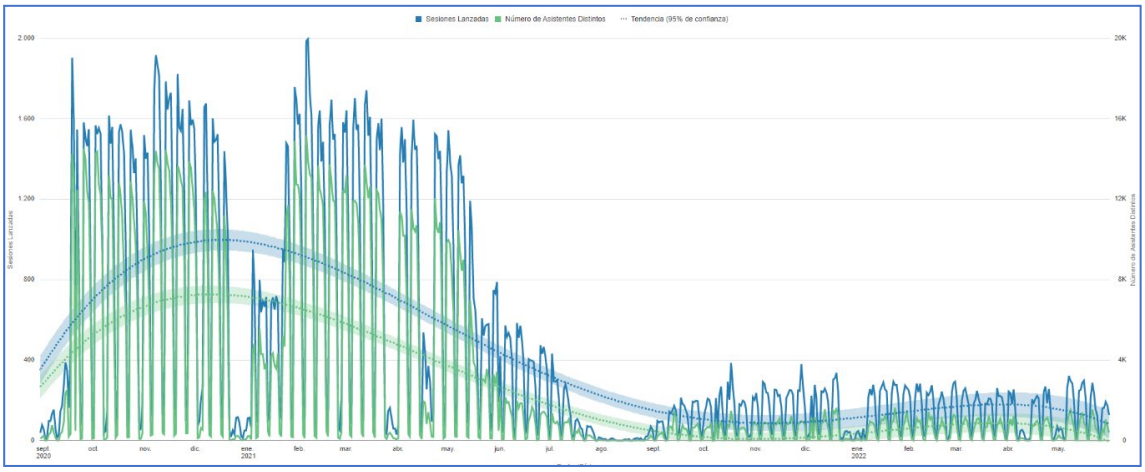
- Se han eliminado de los espacios del curso 2020-21 de la plataforma Blackboard Learn, así como los usuarios que no tenían ningún espacio virtual asignado en el curso 2021-22, con el objetivo de mejorar el tiempo de respuesta de la plataforma al usuario y reducir el espacio de almacenamiento, reduciendo así costes de mantenimiento.
- Se ha actualizado la integración de Turnitin, a LTI 1.3, aumentando las funcionalidades y seguridad en el uso de la herramienta. Recordamos que Turnitin es una herramienta que comprueba la originalidad de los trabajos entregados por los alumnos y está disponible en los espacios virtuales destinados a los trabajos fin de grado y trabajos fin de máster.
- Se ha mejorado la gestión del profesorado en los espacios virtuales de los cursos de Formación Permanente automatizando el alta y baja de estos. Para ello, ha sido necesario integrar distintas fuentes de datos, tanto internas como de aplicaciones de Formación Permanente.
- Se ha empezado a dar apoyo al área de Doctorado para el desarrollo de sus curso de formación, creando los espacios virtuales necesarios así como la gestión de profesorado/alumnado a dichos cursos.
- Se ha continuado proporcionando usuario supervisor de Collaborate a las áreas/unidades en las que se ha justificado su necesidad, para que puedan crear y gestionar las salas que estimen necesarias para la realización de reuniones, seminarios, jornadas, … Se han proporcionado manuales funcionales 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 un importante cambio en la integración de la herramienta de laboratorios virtuales Labster con la plataforma del Aula Virtual. Esta herramienta está disponible en determinados espacios virtuales de los estudios del Área de Experimentales. Con esta nueva integración, al profesorado le será mucho más sencillo, seleccionar y enlazar los laboratorios en el espacio virtual, poniéndolos así disponibles al alumnado.
- Dado que la herramienta “Lista de Alumnos” proporcionada por Blackboard no ofrece la imagen de perfil del alumnado de una manera suficientemente visible, se ha incorporado a los espacios virtuales una nueva herramienta “Lista de Clase” desde la que no solo se ven las imágenes correctamente, sino que permite personalizar la lista atendiendo a criterios de grupo y rol.

Datos estadísticos del Aula Virtual

A continuación, se muestra una gráfica con el total de usuarios agrupados por perfiles con acceso al Aula Virtual. Se puede observar un ligero aumento tanto en el profesorado como en el alumnado.



En la siguiente gráfica observamos como al ser la docencia presencial en el curso 2021-22, el uso de Collaborate Ultra ha descendido considerablemente sobre el uso que hubo en el curso 2020-21 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 del 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 en relación 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 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 124 vídeos.

Se han actualizado los manuales, documento de requisitos técnicos y compatibilidad y casos de uso sobre la herramienta Blackboard Collaborate Ultra, para incorporar las nuevas funcionalidades ofrecidas por esta herramienta. Hacemos una mención especial a los casos de uso en los que se ha pretendido proporcionar al profesorado una guía de cómo utilizar Blackboard Collaborate Ultra. Toda esta información está recogida en la página web dentro de la web de docencia virtual https://www.upo.es/docencia-virtual/aula-virtual/collaborate-ultra/

Se han añadido videotutoriales relacionados con las herramientas de evaluación en la página web dentro de la web de docencia virtual https://www.upo.es/docencia-virtual/aula-virtual/herramientas-de-evaluacion/ , así como otras FAQs sobre estas herramientas.

Se han impartido dos ediciones de formación de ocho horas de duración repartidas en horarios de mañana y tarde, 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. Se ofertaron 30 plazas por edición, cubriéndose un tercio de ellas en cada una de las ediciones.

SERVICIO DE REDES Y EQUIPAMIENTO

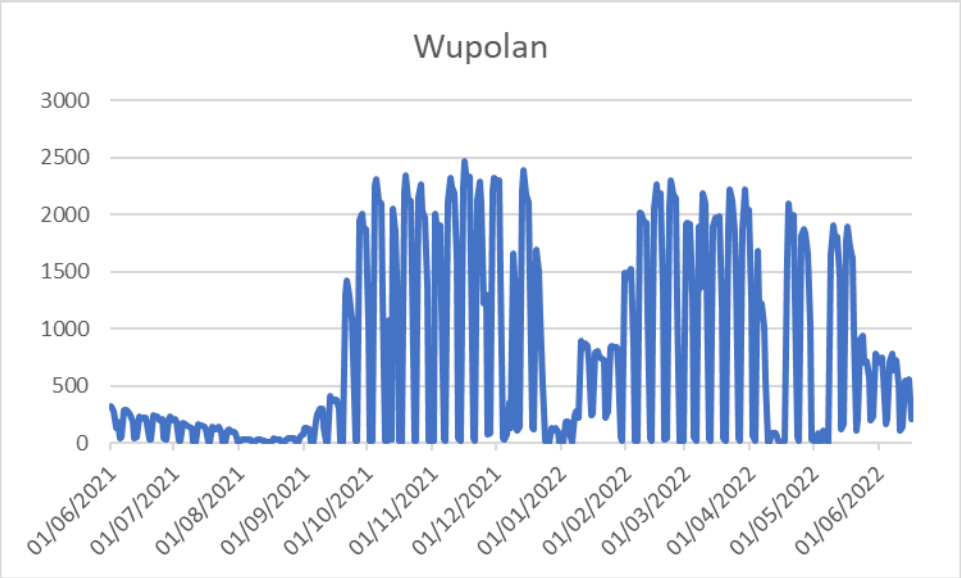
Redes, comunicaciones e infraestructura.

WIFI

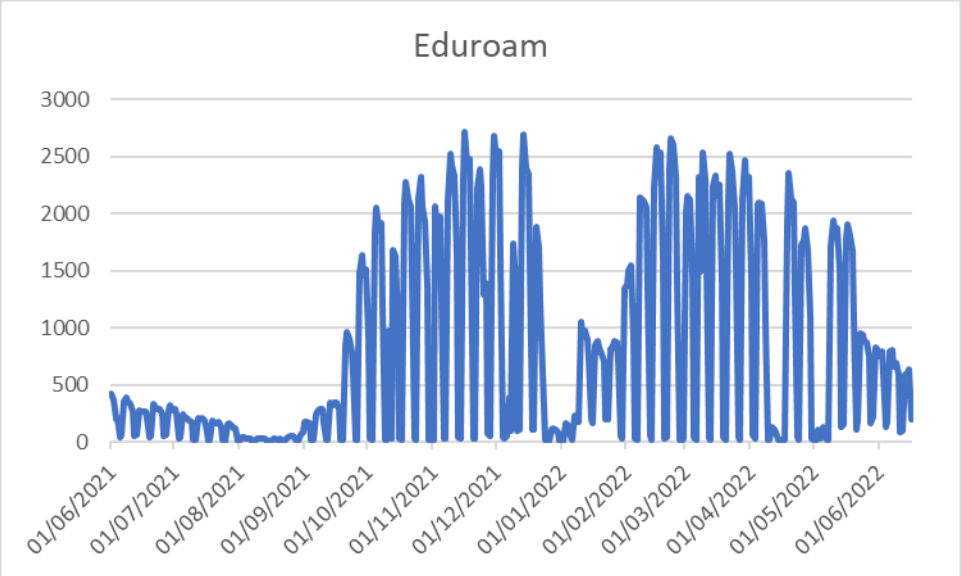
En este curso, aunque la presencialidad ya ha sido importante, no se han registrado grandes diferencias en cuanto a usuarios conectados a la red wifi.

CLIENTES

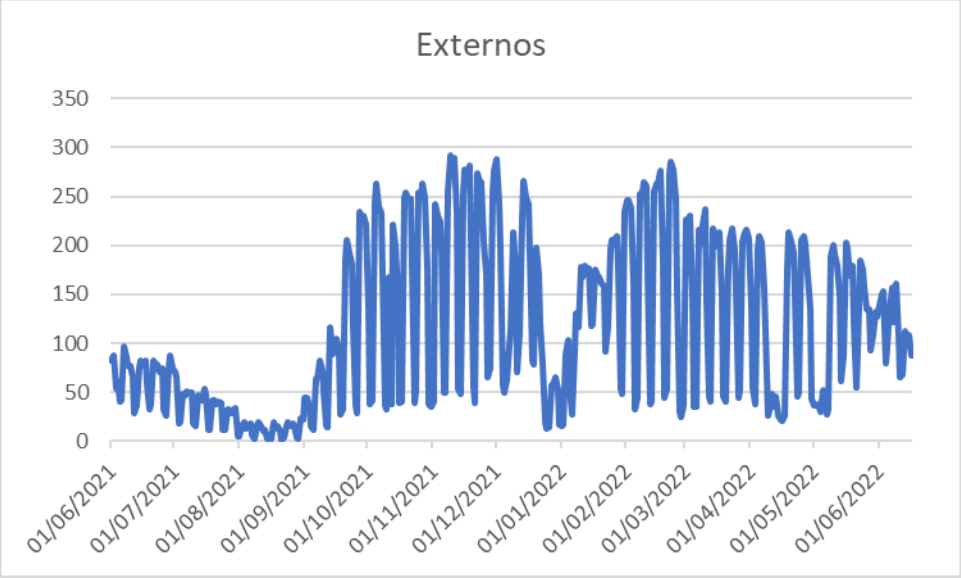
CLIENTES WUPOLAN



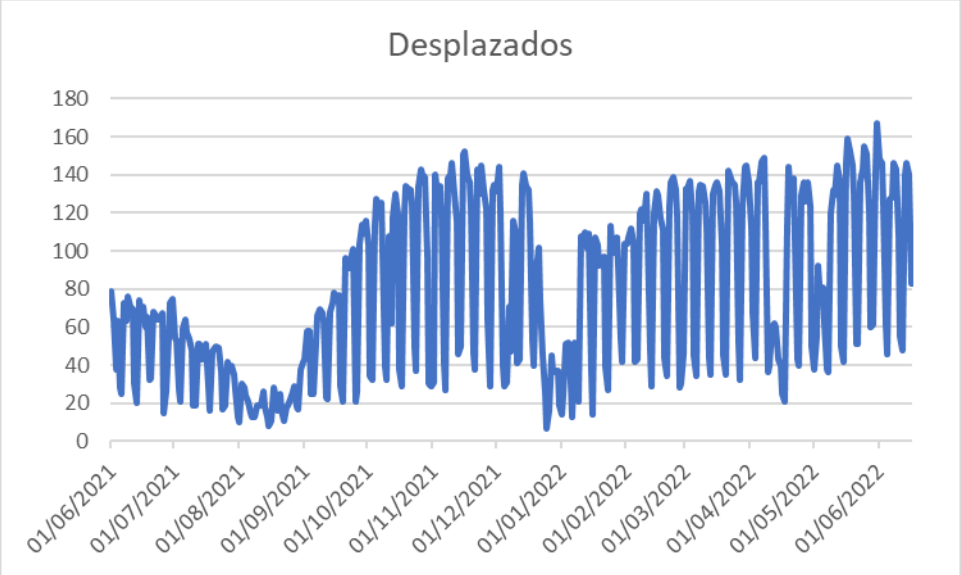
CLIENTES EDUROAM



CLIENTES DE OTRAS UNIVERSIDADES DESPLAZADOS A LA UPO



CLIENTES UPO DESPLAZADO A OTRAS UNIVERSIDADES



Como novedad, se aporta un nuevo sistema que facilita la configuración de los clientes móviles de la red wifi Eduroam. Este sistema permite realizar la configuración de los clientes de forma automática con tan solo leer el código QR correspondiente.

TELEFONÍA

Centralita

Durante este curso se ha realizado la migración del sistema de tarificación (cálculo del gasto de centralita en función de las tarifas telefónicas personalizadas) y gestión de la facturación (comprobación del gasto y distribución a los diferentes centros de coste). Los nuevos sistemas se basan en servidores con sistema operativo Linux virtualizados, mucho más seguros.

Algunos datos interesantes se exponen a continuación:

Renovaciones de terminal al equipo de Gobierno actual.

	Renove 2022
Equipo de gobierno	16 Tel

Número de líneas móviles instaladas este curso:

	Nuevas altas
Líneas móviles	32

Número de líneas fijas instaladas este curso.

	Nuevas altas
Líneas fijas	10

Proyecto Piloto movilidad

A raíz del establecimiento del teletrabajo en la UPO debido a la pandemia originada en 2020 se ha intentado facilitar la movilidad de los trabajadores. En el CIC se ha llevado a cabo un proyecto piloto consistente en utilizar únicamente el dispositivo telefónico móvil, tanto en casa cuando se está en modo teletrabajo como en la UPO cuando se trabaja en modo presencial. El piloto ha sido todo un éxito, ya que ha permitido comunicar con el personal del CIC a través de un único número de contacto, permitiendo, además, el desplazamiento dentro y fuera del campus. El número total de personal que utiliza este sistema es de 19.

SEGURIDAD EN LAS COMUNICACIONES

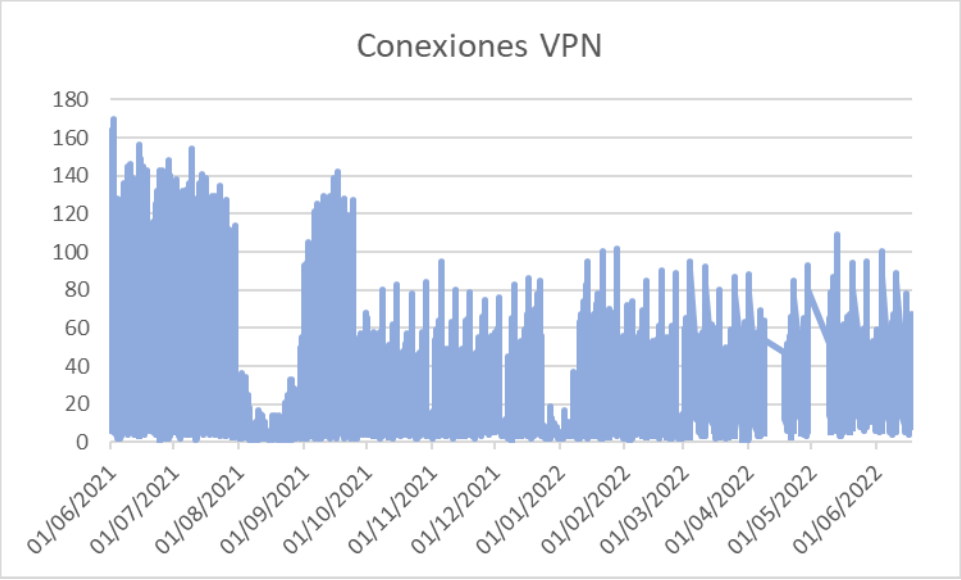
Securización de sedes

Durante los últimos años el número de ataques informáticos a grandes instituciones ha tenido un crecimiento exponencial. Entre las instituciones atacadas se cuenta con varias universiades españolas, ataques de tal gravedad que han tenido incluso que dejar temporalmente de dar servicio. Con objeto de reforzar la seguridad en la UPO, en este curso académico se han instalado un sistema cortafuegos para cada una de las sedes externas de la UPO, complementando el ya existente en la sede central. . De este modo se refuerza la seguridad de las personas usuarias de estas sedes, pudiendo filtrar y prevenir ataques y amenazas provenientes de Internet.

Conexiones VPN

Durante el curso 2021/2022 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) siguiendo la evolución que se muestra en la figura. Se puede observar una disminución en el uso y la frecuencia debido a la vuelta progresiva al trabajo presencial.



Para aumentar la seguridad de las conexiones VPN se está haciendo un piloto para probar la implementación del **doble factor de autenticación**. Consiste en el envío de SMS al teléfono que se designe, con un código que debe ser introducido una vez que el usuario se ha identificado. De este modo, nos aseguramos de que la persona que está identificándose es quien dice ser. El piloto está realizado en el CIC con todos sus integrantes y en el área de Área de Contabilidad, Ingresos y Patrimonio de la UPO.

Seguridad Perimetral

El CIC se ha unido al proyecto liderado por RedIris "SinMalos". En este proyecto, cada institución afiliada analiza y detecta en el tráfico que recibe las direcciones IP que tienen un comportamiento malicioso, como pueden ser escaneos, ataques de fuerza bruta, intentos de explotación de vulnerabilidades, etc. Con esta información, se genera una lista de direcciones potencialmente peligrosas que es recogida por el sistema central de SinMalos, situado en RedIRIS. Este sistema analiza y agrupa la información de cada una de las fuentes para proporcionar a la comunidad una serie de listas de reputación IP que contienen la información agregada y enriquecida.

Las listas de reputación IP se descargan en los dispositivos de seguridad perimetral de la UPO para bloquear el tráfico malicioso, a la vez que la UPO contribuye a detectar IPs maliciosas con las que alimentar las listas.

Red de datos

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

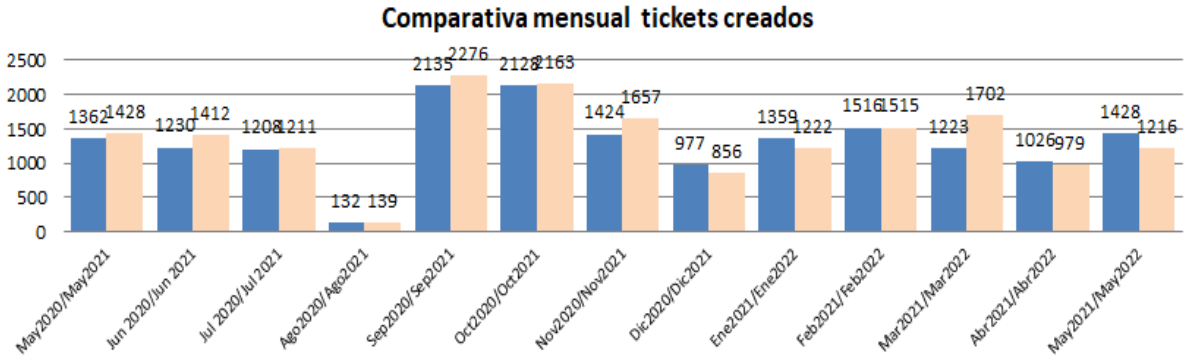
- Renovación de equipamiento obsoleto: se han cambiado por obsolescencia un total de 20 equipos de red de puesto de trabajo sin afectación a servicio.
- Enlace del nuevo edificio "Nuevo Animalario" para la conexión a la red de datos, mediante fibra mono y multimodo.

CENTRO DE SERVICIOS

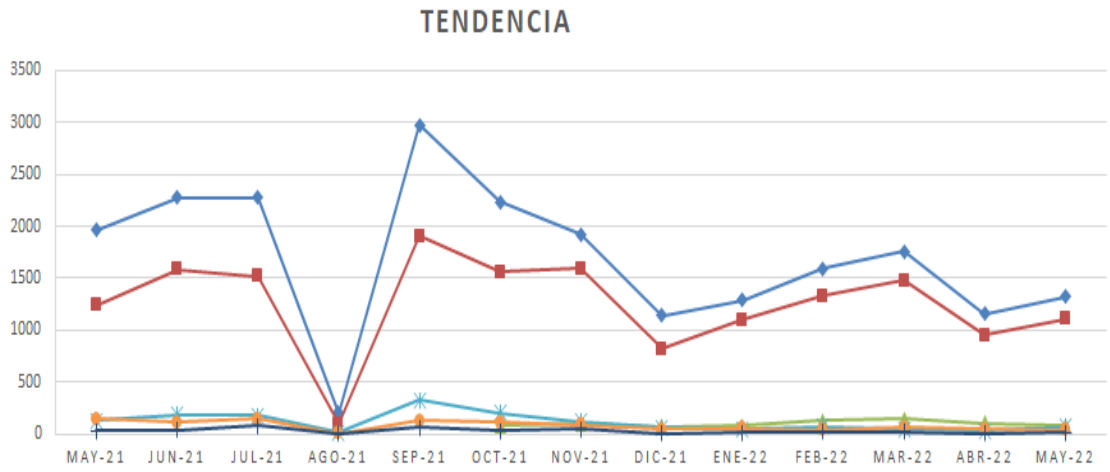
El Centro de Servicios del CIC continua su actividad este curso ya de modo normalizado. La actividad se ha visto incrementada con la incorporación de las actividades de teletrabajo, a las que hay que atender en modo remoto, además de con el mantenimiento y asesoramiento del uso de las nuevas dotaciones de audiovisuales realizadas en las aulas de docencia y laboratorios de docencia y seminarios.

Datos del servicio 2021/2022

Tikets creados: El número de tikets se mantiene en la misma línea del pasado año, con ligera tendencia al alza en determinados meses.

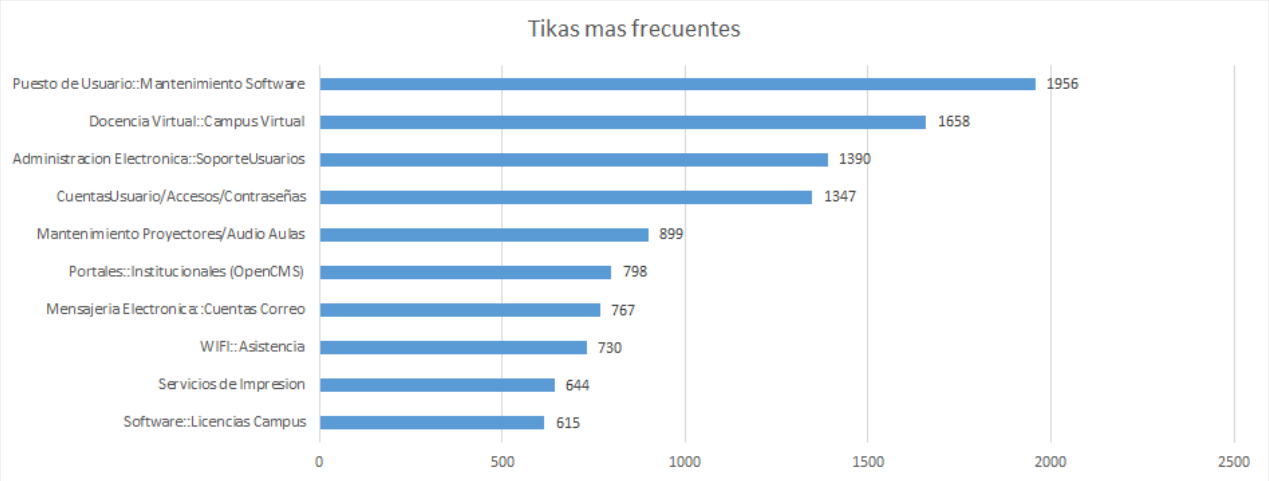


Atención telefónica: la media del número de llamadas ronda sobre las 1600 mensuales, con picos en septiembre, comienzo de curso e inicio de la docencia con los nuevos sistemas audiovisuales.



	may-21	jun-21	jul-21	ago-21	sep-21	oct-21	nov-21	dic-21	ene-22	feb-22	mar-22	abr-22	may-22
RECIBIDAS TOTALES	1963	2280	2278	200	2976	2239	1920	1139	1289	1592	1756	1156	1322
ATENDIDAS CSU	1237	1581	1521	99	1908	1558	1589	818	1097	1331	1478	952	1105
ATENDIDAS AULAS						75	92	72	76	127	145	106	77
DESBORDADAS	127	182	180	12	327	202	118	59	46	72	47	31	69
INCOMPLETAS	141	109	146	1	125	112	87	47	51	40	65	42	41
PERDIDAS	30	38	79	5	58	25	46	8	10	24	20	7	14

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



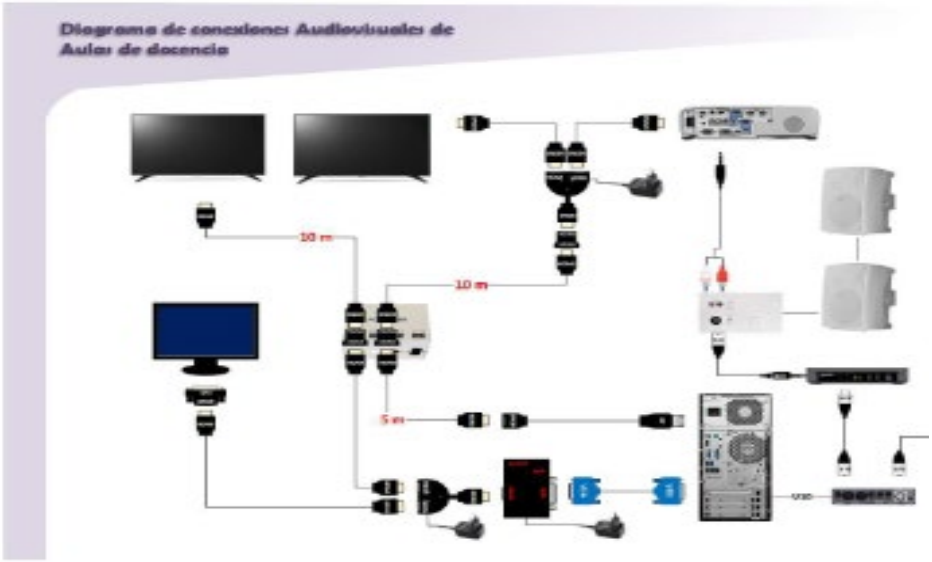
MULTIMEDIA

En el nuevo escenario surgido por la pandemia, con la finalidad de no interrumpir las funciones propias de nuestra Universidad (eminentemente presenciales) y garantizar, a su vez el obligado cumplimiento de las medidas sanitarias, entre ellas, fundamentalmente, el distanciamiento social, la Universidad, con el incondicional impulso del Vicerrectorado Transformación Digital y Calidad , ha desplegado y sigue desplegando modelos innovadores que permitan a los docentes impartir docencia según dos paradigmas esenciales:

- - 100 % online. Modelo según el cual el docente (sólo él de manera presencial en el aula) puede impartir la docencia a todos los alumnos que siguen la clase desde sus respectivos domicilios o ubicaciones personales. La interacción docente ↔ estudiante será, mediante las adaptaciones tecnológicas aplicadas, bidireccional y total.
- - Dual. Modelo a través del cual un determinado grupo de estudiantes asisten presencialmente a clase con garantías, gracias a la escasez de su número, de mantenimiento de la distancia de seguridad entre ellos mientras que el resto del grupo podrá seguir la clase desde sus diferentes ubicaciones personales con plena garantía de participación e interacción, no sólo con el docente, sino con el resto de sus compañeros presentes en el aula.

Con tal fin, la Universidad Pablo de Olavide ha ejecutado un ambicioso plan de adaptación tecnológica que abarca la transformación de la práctica totalidad de las instalaciones docentes que adapta y democratiza el acceso a sus servicios a un total aproximado de 17.000 usuarios directos entre estudiantes, docentes y personal de administración y servicios además del acceso general de cualquier ciudadano que requiera de sus servicios.

Estas se han desarrollado sobre un total de 121 aulas de docencia, 30 aulas de informática, 23 laboratorios de docencia y 30 seminarios. Los espacios docentes con mayor dotación son las aulas de docencia que se componen de cámara, proyector y pantalla, micrófonos de petaca y de ambiente y tabletas, todo ello gestionado por un sencillo mecanismo.

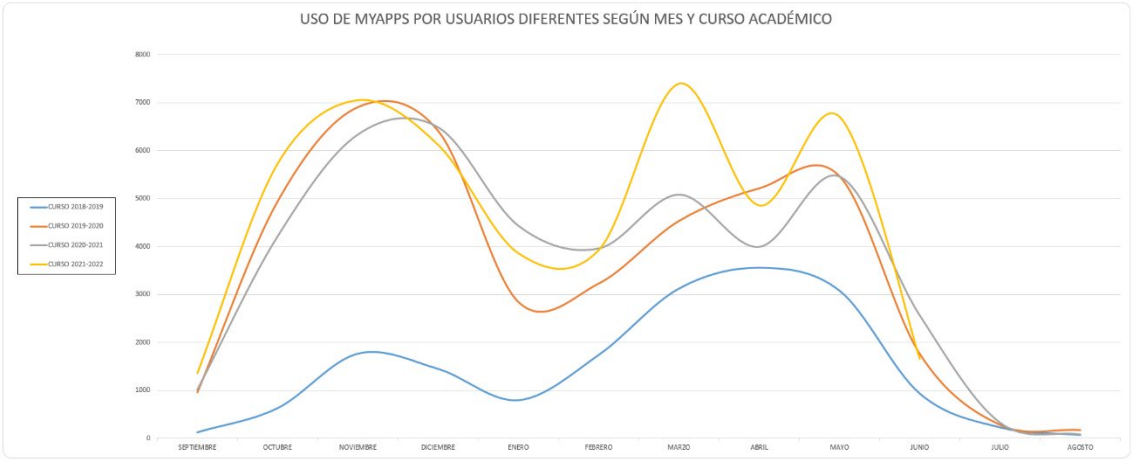


Esquema físico de la conexión de los dispositivos audiovisuales en las aulas de docencia

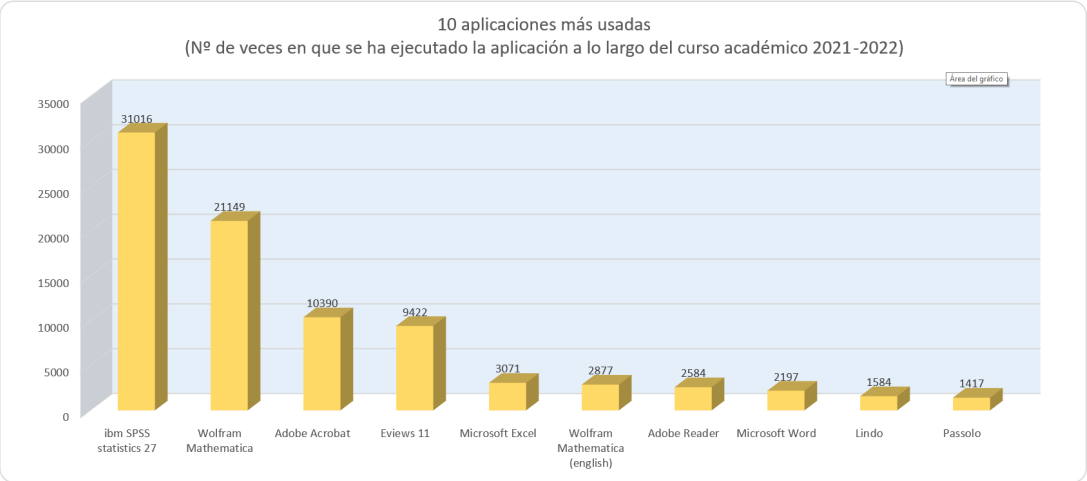
Vista del equipamiento multimedia de un aula de docencia

MyAPPS

El servicio de aplicaciones de aulas de informática en la nube MyApps se ha consolidado hasta formar ya parte indispensable de la docencia en la UPO. Este servicio ofrece a los y las estudiantes todo el software necesario para sus estudios. En el siguiente gráfico se puede observar como el uso del servicio aumenta, sobre todo, en periodos pre-exámenes.



Otro gráfico con interés es el siguiente, que muestra las 10 aplicaciones más utilizadas en el curso 2021/2022, de entre más de 190 aplicaciones existentes en la plataforma.



Equipamiento, Aulas y Laboratorios

Puesto de usuario.

La actual gestión del puesto de usuario está siendo sustituida por una administración moderna, mediante el producto Intune de Microsoft.

- Imágenes para instalación de sistema operativo y software corporativo.
  Se ha incorporado una nueva imagen genérica al catálogo actual (39 imágenes y 344 variantes), 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.
- Renovación de Equipos.
  Este curso se han renovado 40 equipos de Personal Docente e Invertigador y 183 equipos de Aulas de Informática.

Servicio de Impresión

El servicio de impresión del PAS, mediante pago por uso, ha sufrido un incremento en el número de impresiones respecto al curso anterior:

- 2021: Impresiones BN 491.612 Impresiones color 90.603
- 2020: Impresiones BN 430.520 Impresiones color 63.106

No así en el número de usuarios, que se mantiene en 520

El parque de impresoras instaladas es de

- Multifunción: 70 Taskalfa 356ci
- Color grupos reducidos: 10 Ecosys P6230CDN

Samba

Memoria Área de TIC 2021-2022

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 7.5 TB
- Número de Grupos 171
- Número de Usuarios 623

Uno de los cambios en la forma de trabajar del Personal de Administración y Servicios derivados de la pandemia, ha sido la incorporación del Teletrabajo, que a su vez lleva a replantear el modelo actual de PCsobremesa asignado en un despacho por el de ordenador Portátil con acceso a los mismos servicios desde el despacho como desde casa.

El inicio de una prueba piloto con este modelo, tiene como consecuencia directa replantear el cambio de algunos servicios, de modo que se está trabajando en sustituir el actual servicio Samba por Sharepoint, que está disponible independientemente de que el equipo del usuario esté conectado a la red de la UPO o a la wifi de su casa.

BSCW

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

- Usuarios 8290
- Volumen de datos 539.5 G

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.

Protección puesto de usuario

Microclaudia

Se ha consolidado el sistema complementario al antivirus tradicional llamado Microclaudia.

Este sistema, desarrollado por el Centro Criptológico Nacional, está especializado en la protección contra ataques del tipo ransomware, mediante mecanismos de vacunación, haciendo creer al atacante que el equipo ya está infectado.

Kaspersky

La actual situación de inestabilidad mundial ha hecho saltar numerosas alarmas en relación a la idoneidad de mantener instalado el actual sistema antivirus: Kaspersky.

De forma prioritaria aunque controlada, se está migrando al producto Microsoft Defender for Endpoint Plan 1.

Dado que el servicio Kaspersky incluye no solo la protección de los puestos finales, sino el despliegue de aplicaciones, inventario de aplicaciones, gestión de actualizaciones de Windows, inventario hardware, etc. la desinstalación del mismo no es algo trivial, y es preciso disponer de herramientas alternativas que cumplan con las funciones que actualmente recaen sobre Kaspersky Security Centre.

Estas nuevas herramientas son Intune (administración moderna del puesto de usuario), Microsoft Defender for Endpoint (sistema de protección del punto) y WSUS (herramienta de actualización centralizada de sistemas operativos Windows).

EDR

Como sistema avanzado de protección, se está desplegando en puestos de usuario clave y en servidores un sistema de Endpoint Detection Response, capaz de responder a comportamientos de riesgo mediante mecanismos alternativos a los sistemas tradicionales de antivirus, antimalware, firewalls, etc.

Licencias Campus

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

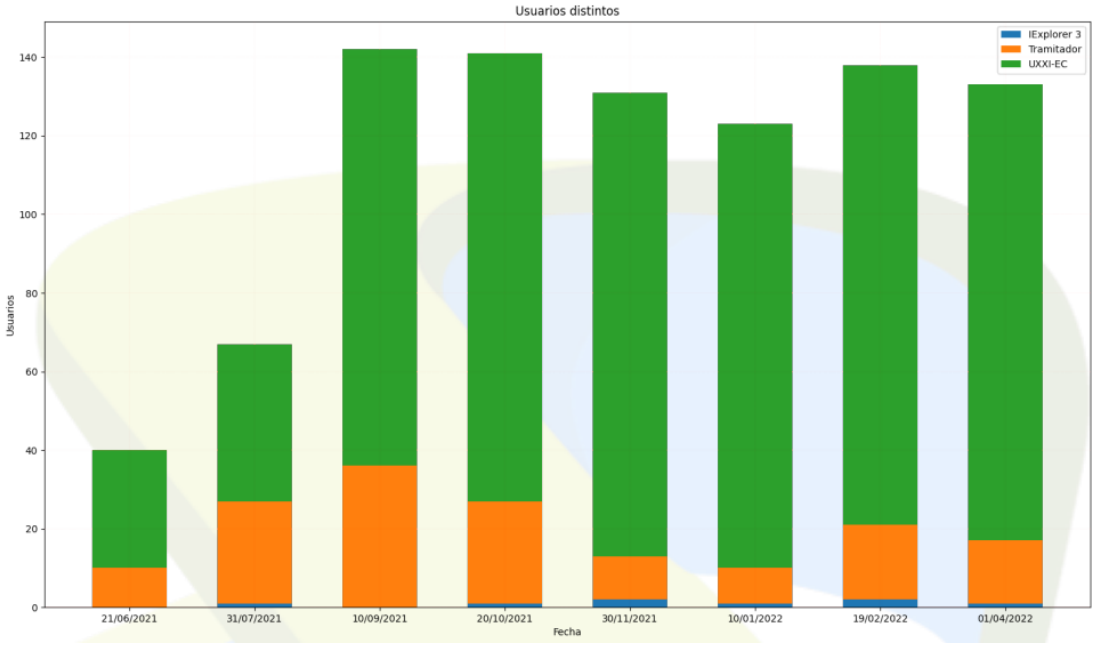
El número de usuarios con acceso a Microsoft 365 (antes Office 365) es de 18.021 teniendo asignadas las siguientes licencias.

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

Microsoft 365 A3 for students use benefit	52000	18021

Aplicaciones virtuales UDS.

Este sistema de aplicaciones virtuales está orientado al uso por parte del PAS, si bien algunos usuarios con equipos Mac lo utilizan para acceder a páginas que aún requieran acceder con Internet Explorer.



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 2021/2022 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: 39,29 % (11 de 28)
- ✓ Nº horas formación TI 2021/2022: 137 horas, 45 minutos
- ✓ Coste total: 7.745,05 €

Detalle actividades formativas TI realizadas:

Nombre actividad formativa	Duración (horas)	Nº de Participantes

Veeam Availability Suite v11: Configuration and Management	21,00	1
OTRS7: Novedades más importantes	4,00	2
Architecting on AWS	21,00	2
microCLAUDIA, centro de vacunación contra el ransomware	1,50	2
Mejores prácticas de Veeam Agent for Windows/Linux/MAC	1,00	1
Jornadas IDENTI::SIC 2021 "Cara a cara con la identidad"	9,00	1
Sophos Professional Services	8,00	3
Turnitin Feedback Studio for Blackboard	2,00	1
Oracle19c. Administración ASM y Clusterware	25,00	1
Oracle19c. Backup y recuperación con RMAN	10,00	1
Microsoft Power Platform Virtual Training Day: Fundamentals	3,25	1
Nuevo Esquema Nacional de Seguridad (ENS)	20,00	1
Ansible	12,00	3

Resto actividades formativas.

Se presenta a continuación un resumen de las actividades formativas a las que ha asistido el personal del Área a lo largo del curso 2020/2021 y que están incluidas dentro del Plan de Formación anual del PAS.

Resumen de datos:

- ✓ Nº actividades formativas distintas: 5
- ✓ Modalidad de actividad formativa:
  - Presencial: 3
  - Virtual: 2
- ✓ % participación personal CIC: 14,29 % (4 de 28)
- ✓ Nº horas formación 2020/2021: 207 horas, 30 minutos
- ✓ Coste total: 0,00 €

Detalle actividades formativas realizadas:

Nombre actividad formativa	Duración (horas)	Nº de Participantes
Estadística aplicada con SPSS: Nivel I	12,00	3
Formación en igualdad, prevención, actuación y mediación ante la violencia de género	180,00	1
Taller sobre Naturaleza del Gasto en la Gestión de Facturas	3,00	1
Inglés. Nivel B2	10,00	1
Geiser	2,50	1

Resumen participación en actividades formativas.

Acciones formativas TI por participante:

- Participantes en 1 actividad formativa: 5

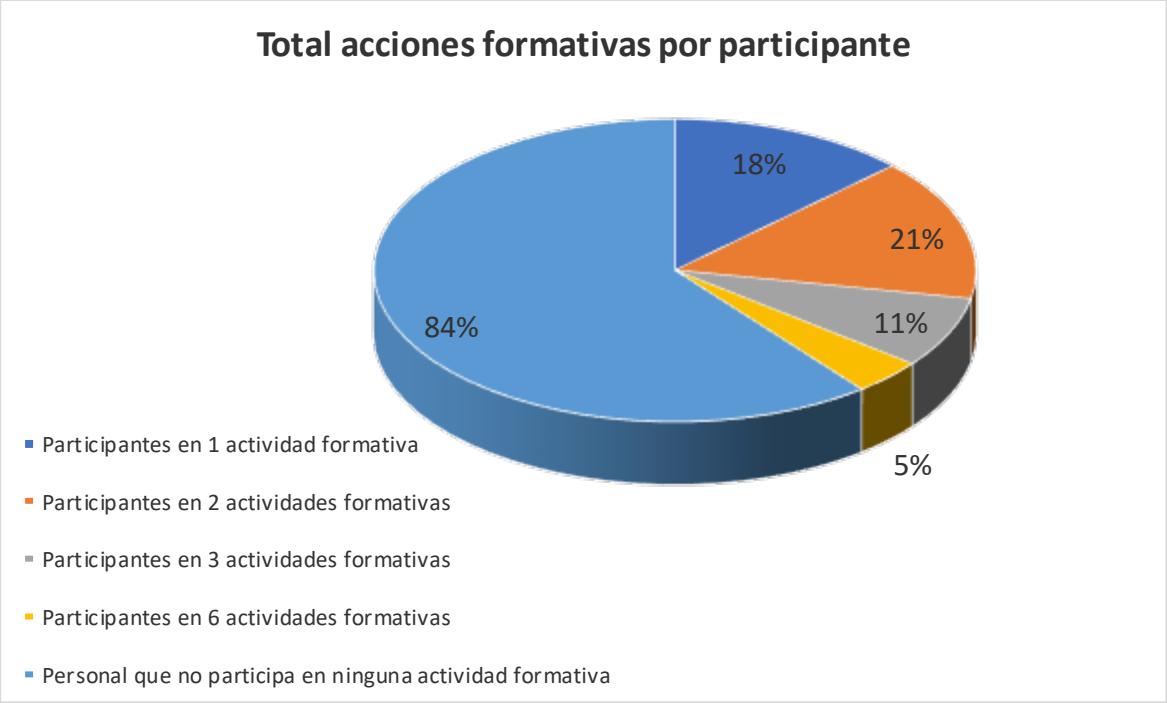
- Participantes en 2 actividades formativas: 2
- Participantes en 3 actividades formativas: 1
- Participantes en 6 actividades formativas: 1

Resto acciones formativas por participante:

- Participantes en 1 actividad formativa: 2
- Participantes en 2 actividades formativas: 1
- Participantes en 3 actividades formativas: 1

Total acciones formativas por participante:

- Participantes en 1 actividad formativa: 5
- Participantes en 2 actividades formativas: 4
- Participantes en 3 actividades formativas: 2
- Participantes en 6 actividades formativas: 1
- Personal que no participa en ninguna actividad formativa:16



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