TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Reuniones de la Comisión de seguridad y Protección de datos

El 14 de noviembre de 2018 se reúne la Comisión de Seguridad de la Información y Protección de Datos con el siguiente orden del día:

1) Plan de adecuación al RGPD.
2) Informe de incidentes relevantes.
3) Plan de mejora de la seguridad.

Durante el desarrollo de la reunión se informa sobre las actividades realizadas y la hoja de ruta en referencia al plan de adecuación al RGPD y el plan de mejora de la seguridad.

Se presenta ante la Comisión el informe de incidentes relevantes, donde se pone de manifiesto el número de incidentes de seguridad ocurridos en 2018, un análisis por tipos y el impacto potencial de los mismo. De esta manera se informa a la Comisión sobre la gestión de incidentes y se trabaja sobre la concienciación en referencia a los riesgos de la organización.

Se presenta un informe sobre el problema del phishing como uno de los incidentes más frecuentes con impacto en la organización. De esta forma se da visibilidad al problema y sobre todo a la necesidad de concienciación como defensa ante ataques basados en ingeniería social.

Como resultado de esta reunión:

Se acuerda la colaboración para la realización de trabajos conjuntos en materia de seguridad de la información y protección de datos. Se trabajará en espacios comunes para compartir información a nivel interno y para exponer información a la comunidad.

El 12 de junio de 2019 se reunió la Comisión de Seguridad y Protección de datos con el siguiente orden del día:

1) Propuesta de revisión de la Política de Seguridad de la Información, y de modificación de la misma para la incorporación de la Política de Protección de Datos de la Universidad.
2) Propuesta de revisión de la Política de Privacidad en Internet (Web UPO).
3) Informe de situación del plan de adecuación de la Universidad al Reglamento General de Protección de datos y a la nueva LOPDGDD.
4) Planificación de próximas actuaciones.

En el desarrollo de la reunión se exponen los cambios propuestos para la nueva Política de Seguridad de la información. Además de actualizar dicha política, se incorpora en este mismo documento la Política de Protección de Datos, pasándose a denominarse Política de Seguridad y Protección de Datos.

Además, la Política se ha revisado conforme a la nueva versión de la Guía 801 del ENS sobre responsabilidades y funciones, que viene a establecer cómo deben repartirse los roles dentro de una organización y cómo debe ser la estructura en materia de seguridad de la información y privacidad.

Dicha política viene a satisfacer el cumplimiento de requisitos normativos, marca los principios y directrices que deben regir la gestión de la seguridad y la protección de datos y pone de manifiesto el compromiso de la Universidad en ambos ámbitos.

Con este acto se da por cumplido el requisito normativo de revisión de la Política de Seguridad y el de creación de la política de privacidad. Se ratifica en el seno de la Comisión quien elevará al Rector para su aprobación.

Se aprueba también la Política de Privacidad de la web, que surge al amparo de esta política y que es de obligada publicación en los portales corporativos.

Se expone el avance del plan de adecuación al RGPD y los avances en el plan de mejora de la seguridad, estableciéndose un grupo de trabajo en el seno de la Comisión, para operar a corto plazo en la elaboración del RAT (registro de Actividades del Tratamiento) y la aprobación de normativas de desarrollo de la Política.

Como resultado de esta reunión:

1. Queda propuesta la nueva Política de Seguridad de la Información y Protección de Datos para que el Rector la apruebe.
2. Queda aprobada la Política de Privacidad de la web.
3. Queda acordada la creación de un grupo de trabajo, para planificar y acometer las tareas de creación del RAT y elaboración de normas de desarrollo de la Política.

Normas, procedimientos e informes

En el marco del Plan de mejora de la seguridad se ha estado trabajando en los borradores de las distintas normativas y procedimientos. Una vez aprobada la Política, se procederá a la aprobación de estas normativas. Estas normativas integran, cuando procede, aspectos de la gestión de la seguridad y la privacidad, siendo elaboradas de forma conjunta por parte del CIC y la Delegada de Protección de Datos.

- Política de Seguridad y Protección de Datos.
- 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.

Se han generado los siguientes informes:

- Informe de phishing octubre 2018: este documento recoge información referida a los ataques de suplantación de identidad, mediante técnica de phishing, que afectan a la Universidad. Se trata de poner de manifiesto su incidencia, su evolución y las acciones que se llevan a cabo encaminadas a la prevención y contención de estos incidentes. Así como para el desarrollo de las medidas recomendadas.
- Informe de Control de Acceso Áreas Seguras TIC: el presente informe recoge los fundamentos y obligaciones legales recogidos en las normativas de aplicación en todo lo referente al control de acceso a área seguras TIC.

- Informe de requerimientos en el uso de claves criptográficas: es objeto último de este informe poner en conocimiento las principales normativas de aplicación y los requerimientos exigidos en todo proceso donde intervengan claves criptográficas, como lo es en particular en la autenticación de servicios web y las comunicaciones seguras.
- Informe de trabajo en almacenes: objetivo de este documento es poner de manifiesto el estado de aquellas instalaciones destinadas al almacenamiento de equipamiento informático y las deficiencias que observan aquellos trabajadores del Centro de Informática, tanto externos como internos, que tienen que realizar trabajos en estas instalaciones.
- Informes sobre cero eléctrico con impacto en sistemas TIC: documentos que recogen el detalle de los incidentes donde se ha producido una caída a cero del suministro eléctrico que afecta a las infraestructuras que alojan los sistemas informáticos que dan soporte a los servicios TIC de la organización y que tuvieron consecuencias en las disponibilidad y continuidad de los mismos:

    - Incidente 29 de agosto de 2018.
    - Incidente 7 de diciembre 2018.
    - Incidente 16 de diciembre 2018.

- Incidentes de seguridad ti relevantes y presentación divulgativa: divulgación sobre incidentes de seguridad ti, poniendo de manifiesto las características de los mismos y el impacto en la organización.
- Informe máquina EPS.UPO.ES: el objetivo del este informe es poner de manifiesto las evidencias de infección detectadas por los sistemas de monitorización en relación a la máquina EPS.UPO.ES identificada con la IP 192.168.10.234. Estas evidencias constituyen en sí un incidente de seguridad, que más allá de confirmar que la máquina se encuentra comprometida, pone en riesgo otros sistemas de información de la organización.
- Informe incidente 'Digital Research Team' - 11/02/2019: recoge el detalle del incidente relacionado con el grupo 'Digital Research Team' que inició una campaña de divulgación en twitter de presuntas fugas de información y vulnerabilidades en webs de la UPO. El informe da a conocer la naturaleza del incidente, las actuaciones realizadas durante su gestión, así como su valoración definitiva. Con esta información, los responsables podrán determinar si llevan a

cabo medidas adicionales para restablecer el posible daño de imagen, así como promover cualquier otra medida conducente a mitigar los riesgos asociados al incidente.

- Informe sobre control de acceso y credenciales: el informe recoge los fundamentos y obligaciones legales donde se establecen requisitos mínimos de seguridad y principios en lo referente al control de acceso y a las credenciales corporativas.
- Informe incidente de seguridad SEGUPO 818: el objetivo de este informe es dar respuesta a la información solicitada por parte de la Policía Local de Alcalá de Guadaira referente a un incidente se seguridad ocurrido el 5 de abril relacionado con la captura y posterior suplantación de identidad de un usuario en la plataforma de correo corporativo.

Se han generado las siguientes presentaciones:

- Presentación gestión de incidencias – EDNON: exposición divulgativa del sistema de notificación y la gestión de incidentes para proyecto de herramienta integradora.
- Presentación gestión de incidencias: exposición divulgativa para informar a la Delegada de Protección de Datos del procedimiento de gestión de incidentes de seguridad en la UPO.
- Presentación de Política de Seguridad y Protección de Datos: exposición divulgativa referente a los cambios de la Política de Seguridad en su revisión anual y la creación de la Política de Protección de Datos.

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

- Procedimiento de detección de ataque de spam desde la UPO: modificación de los scripts de detección para que permita herramientas como my.com y no se produzcan falsos positivos; revisión del correo de notificación al usuario del incidente con recomendaciones de actuación; revisión de oficio de modificación de identidad web por técnicos de tercer nivel.
- Procedimiento de actuación frente a llegada de spam: habilitar de oficio los controles web de plataforma antivirus para el bloqueo de url maliciosa; denuncia sistemática a los certs, plataformas para la identificación y etiquetado de correo spam; denuncia en los navegadores de url maliciosas y propuesta de modificación de clasificación de dominios en Fortinet. Se ha habilitado permiso de acceso a las notificaciones de usuario en TIKA de la cola de spam a la

Jefa de Gestión de Seguridad para acortar los plazos de respuesta. Nueva clasificación de estos incidentes como brechas de seguridad.

- Gestión de contraseñas en ADAS: se ha incorporado de oficio en el sistema, fechas de renovación de contraseñas para que caduquen las contraseñas de usuarios que no hubieran cambiando nunca las contraseña a través de ADAS.

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, 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): 3,6 (escala 0-10) – ALTO.

Se genera la siguiente documentación:

- Informe ejecutivo del análisis de riesgo.
- SOA_Declaración de Aplicabilidad de Medidas del ENS_2019.
- Fichero de análisis de riesgo 2019.

Se genera también el valor del indicador de gestión de la seguridad establecido en marco con un valor de 3.03. 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.

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.

En línea con la campaña iniciada en años anteriores, se han seguido publicando consejos de seguridad en las pantallas informativas y se han publicado consejos y alertas por twitter.

Si bien no se ha llevado a cabo la impresión de folletos y la distribución en mano al personal, durante este periodo se ha llevado a cabo una labor intensa de concienciación a través de mail desde la cuenta de seguridadti@upo.es.

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 el Jefe de Gestión de Seguridad, 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).

Se han recibido un total de 289 correos de usuarios a la cuenta y se han emitido un total de 227 correos desde la cuenta, relacionados con incidentes denunciados por los usuarios o notificaciones a usuarios, de incidentes en los que se han visto involucrados.

Se ha notado un aumento significativo en el nivel de concienciación, manifestándose en un incremento importante de las denuncias de incidentes por parte de usuarios. También se ha aumentado este nivel de concienciación en unidades con un impacto potencial alto, como gestión económica, quienes consultan de forma preventiva un mayor número de correos sospechosos.

Trabajos de coordinación Seguridad de la Información y Protección de Datos de Carácter Personal

Tras los acuerdos adoptados por la Comisión de Seguridad de la Información y Protección de Datos, se ha establecido un equipo de trabajo formado por la delegada de protección de datos, el responsable de sistema y la Jefa de gestión de seguridad para el desarrollo de actividades que afectan a ambos ámbitos:

- Estudios de las medidas de seguridad exigibles a proveedores externos con encargo de tratamiento.
- Definición del procedimiento común de gestión de incidencias y adaptación de la herramienta de gestión.
- Procedimiento de extracción de datos de equipos corporativos.
- Generación de clausulado.
- Integración de la política de seguridad y política de protección de datos.
- Análisis conjunto de brechas de seguridad.
- Intercambio de información sobre los sistemas TIC que soportan los datos de carácter personal, proceso de gestión de contraseñas, de gestión de incidentes, de control de acceso, etc.
- Estudio de posible herramienta de gestión de Registro de Actividades.

Servicio SAT-INET

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

Durante el periodo que se contempla en la memoria se han resuelto un número de 70 incidentes notificados por la sonda.

El mayor número de incidencias recibidas son referentes a:

- Tráfico relacionado con posible infección de equipos con malware dridex, coin miner, dns Sinkhole.
- Intentos de explotación de vulnerabilidades en equipos servidores.

Un gran número de incidentes estaban relacionados con dos equipos athenea y sierra-db, que han podido ser retirados y sustituidos por un nuevo sistema.

Se han recibido un total de 70 incidentes catalogadas de peligrosidad Media – Alta.

Auditoría técnica para detección de vulnerabilidades

Se han realizado las siguientes auditorías técnicas para la detección de vulnerabilidades en sistemas Web. Estos análisis son parte de las acciones de prevención y, en algunos casos, de contención de incidentes de seguridad:

- Sistemas de preproducción en la subred 10.
- Sistema eps.upo.es en relación con vulnerabilidades publicadas en foros públicos e incidentes de seguridad detectados.
- Sistema upo.gob.es.
- Sistema Histiarte.upo.es.
- Sistemas de aplicaciones OCU.
- Sistema Marco.upo.es.

Los informes han dado lugar a acciones de mejora que han corregido las vulnerabilidades catalogadas como altas, cuando ha sido posible, o a planes de actuación para el reemplazo de los sistemas vulnerables.

Gestión de incidencias de seguridad

Dentro de la gestión de operativa diaria de seguridad se han desarrollado acciones para la resolución de 408 incidentes de seguridad (frente a los 260 del periodo anterior) encaminados a corregir vulnerabilidades o ataques sufridos en los sistemas.

Se han registrado un total de 408 incidentes de seguridad. Estos incidentes tienen su origen:

- 42 notificados por el INCIBE-CERT (antes CERTSI).
- 3 notificados por AndaluciaCERT.
- 39 notificados de oficio.
- 70 notificados por la sonda.
- 100 registrados por la herramienta solicitud de servicio al CIC.
- 62 notificados por las herramientas de detección automáticas antispam.
- 92 otros (por usuarios a correo electrónico a seguridadti@upo.es, presenciales, etc.).

Cabe destacar el incremento de denuncia de los usuarios y del número de usuarios que notifican de forma sistemática siguiendo el procedimiento para facilitar el máximo de información posible.

Por tipo de incidente:

- 72 Contenido abusivo – spam, phishing, extorsión.
- 37 Código dañino - infecciones por malware.
- 64 Disponibilidad – pérdida en la disponibilidad de los servicios, problemas con credenciales de acceso a los servicios, pérdida de información.
- 81 Intrusiones – Escaneo de vulnerabilidades, intentos de ejecución de código remoto, cross-site. Scripting (XSS), defacement (desfiguración).
- 8 Obtención de información – escaneo de vulnerabilidades.
- 6 Política de la Información.
- 84 fraude – emisión de correo spam desde la UPO.
- 56 Otros – vulnerabilidades.

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.
- Se han corregido vulnerabilidades detectadas en equipos expuestos a internet mejorando los algoritmos de cifrados, filtrado puertos de acceso y eliminando servicios bajo el criterio de configuración mínima.

Incidentes de sistemas comprometidos

Se han producido incidentes de peligrosidad alta en relación con dos sistemas de la Universidad. En ambos casos con notificaciones externas por parte de los equipos CSIRT:

- Página Web Revistas.
- Página Web EPS.upo.es.

En ambos casos la causa raíz de los incidentes era la falta de mantenimiento de dichos sistemas, permitiendo la explotación a los atacantes de vulnerabilidades conocidas no corregidas. Ambos sistemas mostraban evidencias claras de estar comprometidos y comprometer, por tanto, la seguridad de la organización.

En ambos casos se realizaron los informes necesarios y se estableció la coordinación con los responsables funcionales de estos sistemas para el apoyo en la migración de estos sistemas a otros actualizados.

Incidentes con impacto reputacional

Se han producido incidentes con impacto reputacional:

- Inclusión en listas negras de la IP de la Universidad por envío de correo sospechoso.
- Desfiguración de páginas web con la inclusión de contenido no legítimo.
- Redirecciones de páginas no autorizadas.
- Caída de sistema web eps.upo.es.

Notificación de incidentes

No se ha realizado ninguna notificación obligatoria de gestión de incidentes de seguridad ni de brechas de seguridad.

Apoyo en los equipos CSIRT

Para el análisis forense de ciertos incidentes se ha solicitado la ayuda de los CSIRT para la determinación del impacto o la peligrosidad del mismo. Se les ha enviado la información que nos han solicitado y han procedido a informarnos.

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 relacionados con otros organismos:

- Se ha denunciado la detección por parte del antivirus corporativo de páginas de otros organismos que habían sido comprometidas.
- Se ha procedido a la comunicación al servicio de LAVADORA de un aumento importante del número de spam recibido en determinados periodos.

- Se ha procedido a la comunicación al servicio de LAVADORA de reiteración de correo spam de un mismo tipo que no estaba siendo marcado como spam, aportando colección de correos para su análisis.
- 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:

    - Problemas de confidencialidad en Myapps y problemas de niveles de permisos sobre recursos.
    - Vulnerabilidades detectadas con OpenVAS sobre sistemas webs de OCU.

Herramienta de gestión de incidentes

Se ha mejorado la herramienta de gestión de incidentes para la integración con la gestión de brechas de seguridad y generación de informe completo sobre cada incidente.

Procedimiento de gestión de incidentes

Se ha acordado una gestión de conjunta de incidentes de seguridad y brechas de seguridad con un único punto de contacto común. Se elabora una propuesta de procedimiento para recoger la forma de actuación y establecer las comunicaciones.

Tal y como se ha mencionado en el apartado de normativa, se han desarrollado los procedimientos de gestión de incidencias (a la espera de aprobación formal) y los procedimientos de actuación en caso de llegada de correo spam. Esta procedimentación ha sistematizado la respuesta ante este tipo de incidentes y ha minimizado los tiempos de respuestas.

Proyecto de mejora de control de acceso a salas físicas

Se ha elabora un proyecto de mejora del control de acceso a salas físicas que permitirá ir mejorando el control de acceso a áreas seguras, asegurando el cumplimiento normativo y mejorando la operatividad.

Esta mejora en el sistema permitirá la coexistencia del sistema actual con el nuevo sistema para la protección de la inversión realizada hasta el momento y migración progresiva conforme a recursos y necesidades.

El sistema permitirá el registro activo de acceso y la notificación de posibles incidentes de seguridad relacionados con el acceso.

Además, se ha elaborado la normativa y procedimiento de acceso a áreas seguras y normativa de buen uso de áreas seguras, todas en espera de aprobación formal.

Proyecto de implementación de herramienta de gestión de Incidentes

Actualmente la UPO dispone de una herramienta de trabajo de gestión de incidentes de seguridad que permite el registro de los incidentes y dar cumplimiento normativo a este procedimiento.

El sistema actual permite incorporar toda la información necesaria para gestionar todo el ciclo de vida del incidente desde su registro, seguimiento, actuaciones, comunicaciones e informe final.

Se elabora un proyecto para el estudio de mejora de esta herramienta con el objetivo de sustituir la herramienta por LUCIA, herramienta de gestión que el CCN-CERT pone a disposición de las administraciones públicas. Esta evolución permitiría:

- Asegurar la adecuación de la herramienta a los cambios normativos.
- Integración con la herramienta de notificación de SAT-INET.
- Integración con INES – Herramienta de elaboración de informe anual sobre el estado de la seguridad.

- Centralizar la gestión de comunicaciones de incidentes con autoridades de control.
- Automatizar las notificaciones de incidentes provenientes de distintas fuentes como el correo electrónico o la herramienta de gestión de incidentes (TIKA).

El proyecto se elabora con la empresa EDNON y ha generado un informe que permitirá valorar la idoneidad de la sustitución de la herramienta, valorando los recursos necesarios, las mejoras que se obtendrían y lo que se perdería con respecto al sistema actual.

Formación

Se ha realizado las siguientes acciones formativas en materia de seguridad:

CIC

- El factor humano como primera línea de defensa. 5 horas

Jefe de Gestión y Colaboradores de Coordinación de Seguridad

- Taller PILAR de gestión de riesgos. 25 horas.

Administrador web

- Asistencia a jornada Día Mundial de la Ciberseguridad. Riesgos de seguridad en portales web: ¿tu sitio es seguro o crees que no te han atacado?.

Jefa de Gestión de la Seguridad

- Gestión de incidentes CCN-CERT. CCN. 9 horas.
- Concienciación seguridad wifi. CCN-CERT. CCN. 3 horas.
- Incidentes complejos -captura de evidencias. CCN-CERT. CCN. 3 horas.
- Auditoria enfocada ENS. CCN-CERT. CCN. 3 horas.
- Herramienta PILAR 7.2 – CCN-CERT. 3 horas.

- Herramienta INES 2.O. CCN-CERT. 3 horas.
- Introducción al hacking ético. AndaluciaCERT. 40 horas.
- Asistencia a jornadas “Novedades legislativas en materia de privacidad y seguridad de la información”. 5 horas.
- Asistencia a SEDIAN Day, Cybersecurity Conferences. 8 horas.

Realización anual del informe INES como requerimiento del 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:

- Indicador de Madurez del ENS 23.23%.
- Indicador del cumplimiento del ENS 26.21%.
- Organización de la Seguridad 79%.

Se genera la siguiente documentación:

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

Otros

Desde el punto de vista de la seguridad se han realizado acciones encaminadas a la mejora:

- Alta disponibilidad en firewall de aulas de informática.
- Alta disponibilidad en conexión a la salida de internet.
- Mejora de la alta disponibilidad en el core de red.
- Desactivación de protocolos vulnerables de cifrado web.

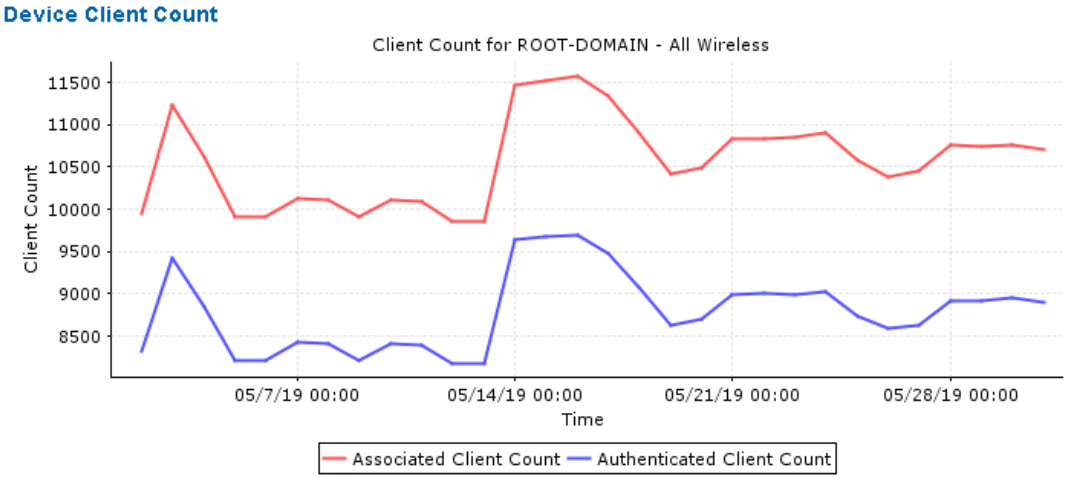
- Eliminación paulatina de sistema web con acceso http.
- Cambio de versión en la plataforma antivirus que permite nuevos módulos de control.
- Activación de cortafuego de aplicaciones en equipos finales a través de la plataforma de antivirus.
- Sustitución de estafetas de correo con la mejora de cifrado de correo saliente.
- Virtualización en DMZ que permite mejor control de medidas de seguridad como backups o actividades de mantenimiento.
- Incorporación de nuevos servicios a Adas para mejor control de acceso y gestión de contraseñas.

SERVICIO DE REDES Y EQUIPAMIENTO

Campus Inalámbrico

Red inalámbrica

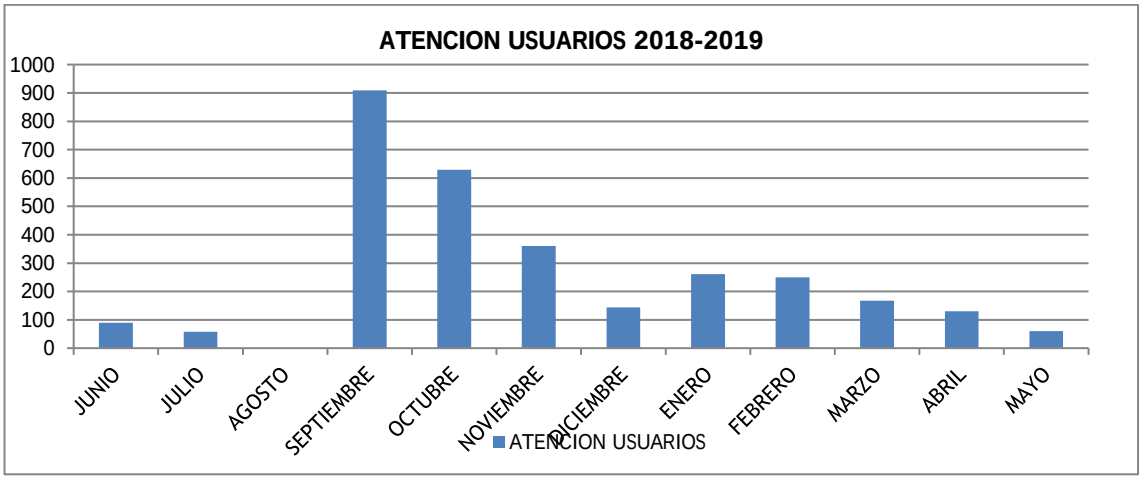
Durante el curso 2018-2019 se han reforzado dos edificios aularios cuya dotación inalámbrica estaba obsoleta: los edificios 13 y 16. A su vez, se ha renovado toda la infraestructura WiFi de la sede de Olavide en Carmona, quedando la cobertura no sólo más extendida sino capaz de dar soporte de más calidad y mayor ancho de banda a los usuarios de la sede. Estas mejoras han supuesto un aumento en la satisfacción de los usuarios de dichos edificios y en general de todos los usuarios de la red inalámbrica de la UPO.



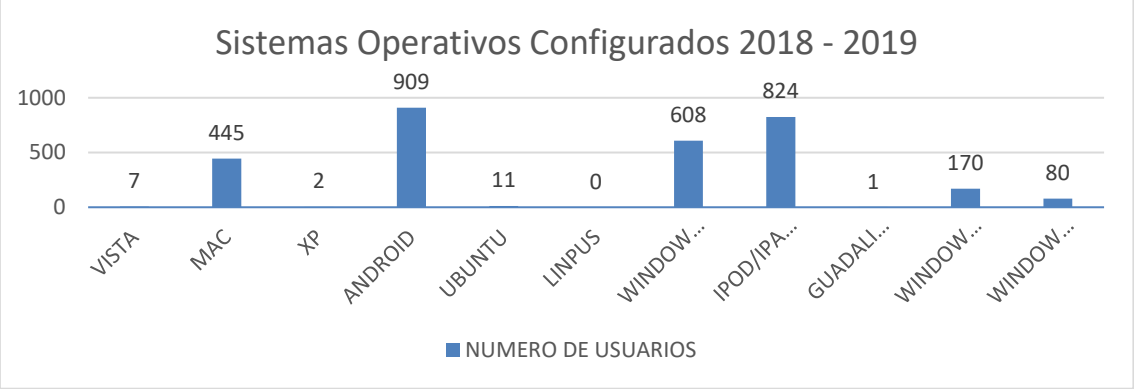
Como muestra de la dimensión que supone el acceso a la red wifi hemos tomado el mes de mayo de 2019. En este gráfico podemos observar dos líneas, la que está más abajo (color azul) indica el número de clientes conectados (autentificados) a la red wifi de la UPO. Se puede observar que hay picos de casi 10.000 usuarios sostenidos durante varios días. La línea superior (color rojo) indica el número de clientes asociados a la red, es decir, dispositivos que 'ven' un punto de acceso, pero no están autentificados, ocupando, sin embargo, espacio en el espectro aéreo y en el enlace de control, ya que se están comunicando continuamente. En esta situación encontramos unos 12.000 dispositivos, que es una carga bastante elevada.

Servicio de atención a usuarios Wifi

En el siguiente gráfico puede verse la evolución mensual del servicio de atención a usuarios. Como suele ser habitual, la mayor actividad corresponde con el comienzo del curso académico.



Con respecto a los sistemas operativos de los dispositivos en los que se ha configurado el servicio de conexión wifi tenemos la siguiente gráfica:



Se observa un aumento del uso de dispositivos Android y Apple con respecto a los sistemas operativos Windows que siempre han destacado como de uso personal.

Desde el servicio de Atención a Usuarios Wifi se ha atendido este año a un total de 26 eventos (congresos, conferencias y otros), en los que se ha dado soporte a los usuarios externos a la UPO que asisten a estas actividades.

Infraestructura de Red

Enlaces Sedes UPO

Con objeto de mejorar el acceso a internet en las sedes de Sevilla (Centro y Residencia Flora Tristán) y Carmona, la conexión al exterior se han aumentado a 100 Mbps síncronos. Esto significa que los usuarios de dichos centros tendrán 100Mbps en subida y 100 Mbps en bajada asegurados, con un ancho de banda real de 200 Mbps.

Core de red

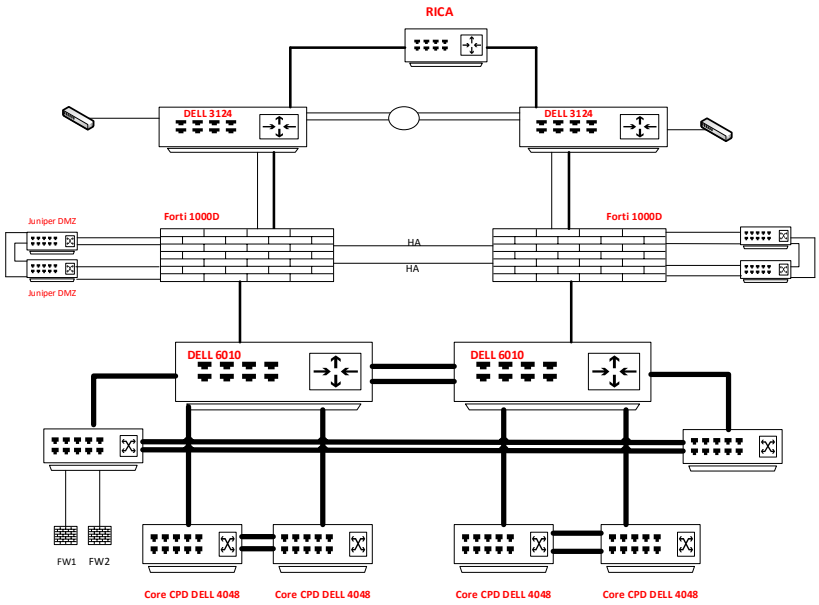
En el verano de 2018 se llevó a cabo la renovación del core de la red de datos. En el core se encuentran los nodos de red que dan servicio a toda la universidad, del que parten las fibras ópticas que enlazan a todos los edificios y a donde se conectan los servidores con las aplicaciones que utilizamos diariamente. Igualmente se ha actualizado el core de acceso a internet. Así disponemos de un core de 40

Gbps, siendo la primera Universidad en tener un troncal de alta velocidad. Otras características son la redundancia y continuidad de negocio que facilita la configuración elegida. Por otra parte, los equipos elegidos están preparados para implementar redes dirigidas por software (SDN).

Este proyecto ha sido presentado en dos jornadas de difusión:

- Cádiz, marzo de 2019, Evento Dell/EMC.
- Sevilla, mayo de 2019, Jornadas Técnicas de RedIris.

A continuación, se muestra un esquema general que muestra cómo queda el core una vez finalizada su implantación.



Seguridad en aulas: En el verano de 2018 también se llevó a cabo la renovación del sistema de seguridad de la zona de aulas de informática, que estaba obsoleto y daba problemas de gestión. Este sistema, un firewall en alta disponibilidad, permite securizar la parte de aulas aislándola de la red de la UPO, permitiendo analizar en cada momento las aplicaciones a las que se accede y evitando ataques informáticos procedentes de esta zona.

CPD1

Este curso se ha reformado el CPD1, situado en la planta superior del edificio 1.

Este CPD se utiliza como respaldo del CPD32, pero en sus inicios fue el primer CPD que tuvo la UPO. Desde sus inicios permanecía casi inalterable, por lo que era necesario actuar para que los equipos de respaldo situados allí tuvieran unas condiciones seguras.

Las áreas en las que se actuado, junto con el área de IMEE, han sido iluminación, refrigeración, control de incendios, instalación de suelo técnico, electrificación y acondicionamiento del espacio con armarios tipo Rack para instalación de los equipos de red y servidores de alta disponibilidad.

Telefonía

Durante este año el servicio de telefonía se ha caracterizado por su estabilidad de funcionamiento. Cabe señalar la caída del uso del sistema fax como consecuencia de la existencia de otros modos de transmisión de documentos.

Como actuaciones destacadas pueden citarse:

- Migración de centro de atención telefónica del área de gestión de grados a un call center con agentes.

Multimedia

Salas de Juntas del Rectorado

En las salas de juntas del Rectorado se han realizado varios proyectos multimedia:

- Proyección: en cada una de las salas de juntas 1, 2 y multiusos se ha instalado un sistema de visionado en monitor de 70 “con soporte móvil, conectado a través de un sistema de proyección inalámbrico.
- Grabación de sonido: en las salas de juntas 1 y 2 se ha instalado un sistema de grabación de sonido de sala con microfonía de ambiente integrada en una placa omnidireccional, con un sencillo sistema de puesta en marcha, pausa y parada.

- Visualización: en la sala de juntas 3 se ha instalado un sistema capaz de permitir el visionado de la proyección desde distintos ángulos a toda la mesa de conferencias, que pueda retirarse en un momento dado. La proyección se realiza a través de un sistema de transmisión

inalámbrica. Toda la sala ha quedado integrada con el sistema de conferencia y grabación ya existente.

- Proyección en la sala del Rector: se ha dotado esta sala de proyección con una pantalla de 2x1.50, un proyector de alta resolución, ambos escamoteables en techo, y todo conectado a través de un sistema de proyección inalámbrica.

- Colaboración con coworking de Biblioteca tanto en relación al equipamiento multimedia instalado allí como a la infraestructura de red (cableada y wifi) necesaria para el correcto funcionamiento de la sala.

Aulas

En este año se ha finalizado la ejecución del procedimiento de dotación multimedia de las aulas de docencia iniciado el pasado año. Un total de 145 aulas han quedado renovadas en la dotación multimedia, consistiendo ésta en sistema de audio y video integrados.

Laboratorios de Docencia Avanzada (active learning)

Estas aulas/laboratorios de docencia avanzada se ponen a disposición de la comunidad con objeto de ofrecer una enseñanza más participativa y con mayor aportación tecnológica que en la docencia tradicional.

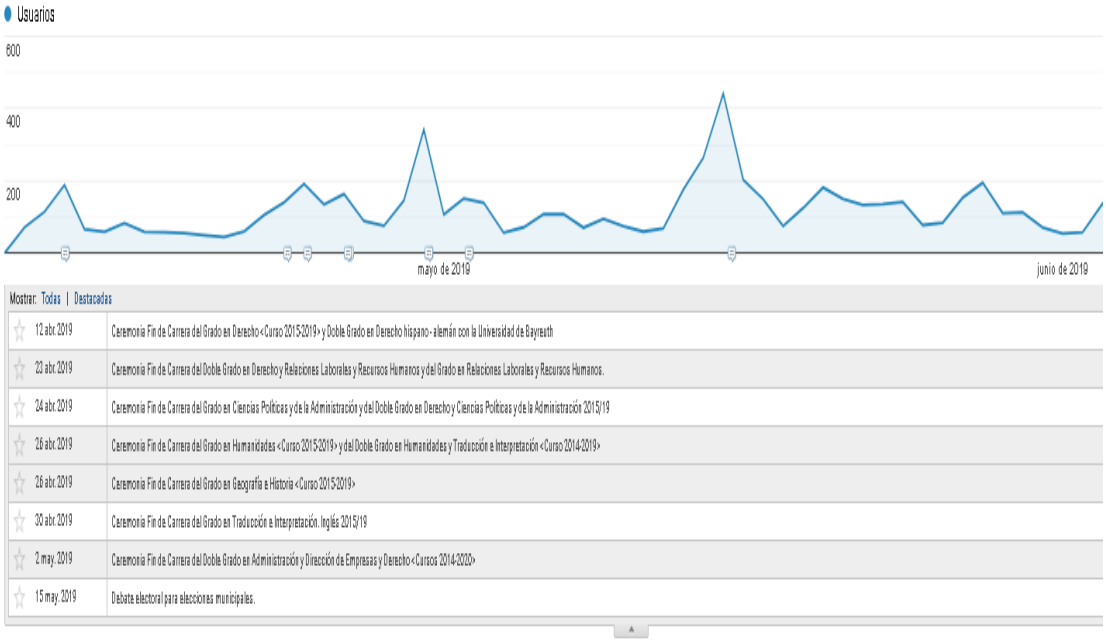
Consta de:

- Una pantalla táctil en la que es posible proyectar tanto desde un ordenador como desde un móvil, escribir en ella, guardar lo escrito, etc.
- Sistema de grabación de clases autónomo.
- Cámara de grabación.
- Videoconferencia.

Los laboratorios cuentan, como puede verse en la foto inferior, de un mobiliario versátil y actual, que puede disponerse tanto en forma individual como de grupo, permitiendo configurar diferentes dinámicas educativas.

UPOTV

El sistema de almacenamiento de vídeo de la UPO va creciendo uniformemente y cada día son más las personas que se conectan para ver los vídeos producidos en nuestra Universidad. Como dato curioso, el pico más alto de conexiones a nuestro sistema se tuvo el día 15 de mayo, cuando se celebró el debate electoral por parte de los candidatos al ayuntamiento de Sevilla, con un máximo con 442 usuarios.



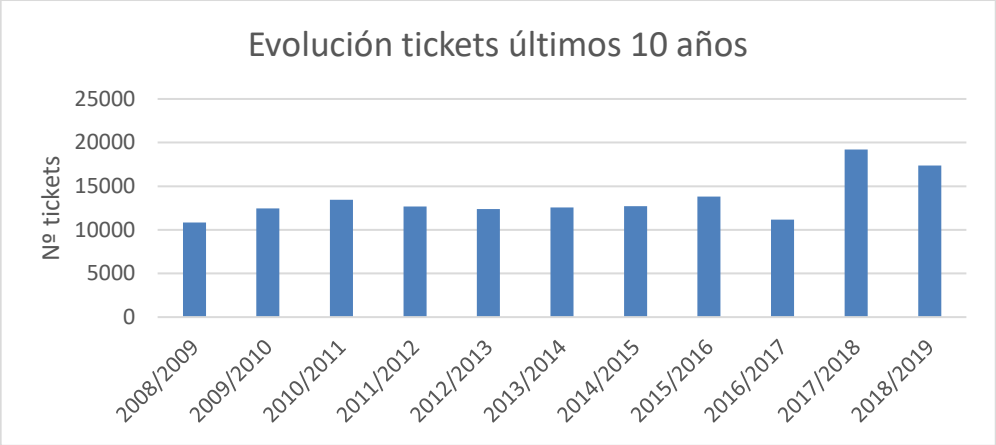
Centro de Servicios al Usuario/a (CSU), Puesto de Usuario y Aulas

Centro de Servicios al Usuario/a (CSU)

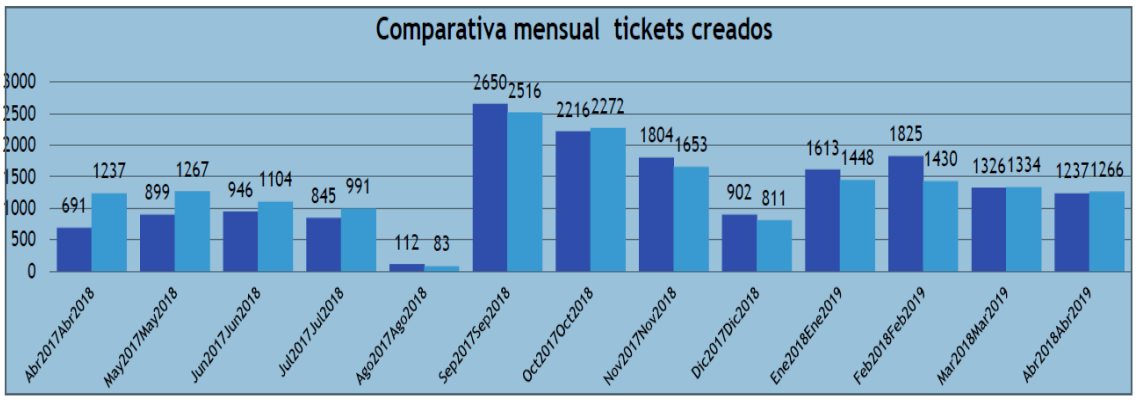
El CSU es uno de los pilares del CIC. Da respuesta cada mes a más de un millar de solicitudes e incidencias relacionadas con las TIC. Ubicado en el edif. 9, además del presencial, dispone de estos canales de entrada: teléfono, correo electrónico y web (herramienta de gestión de incidencias).

El CSU recibe tickets de servicio que luego clasifica y asigna a los distintos agentes. A continuación, se muestra un gráfico de la evolución del número de tickets entrantes en el CSU al año. Este número ha crecido durante los dos últimos años, debido al aumento de servicios que se ofrecen desde el CIC.

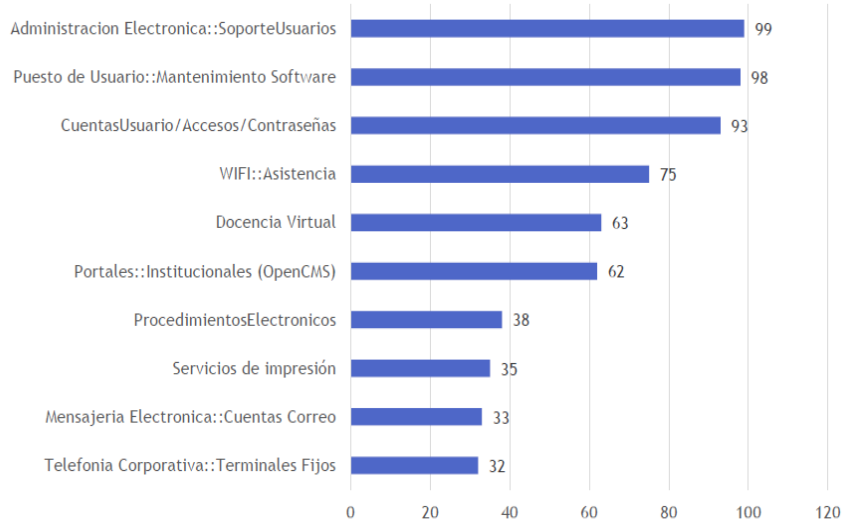
Evolución anual del número de tickets de servicio registradas



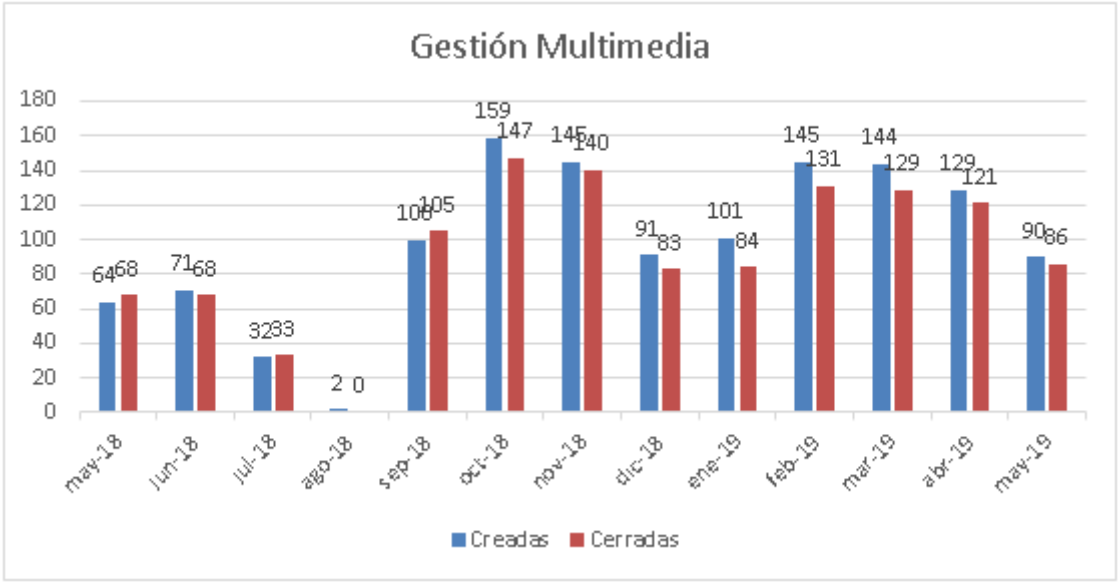
A lo largo del curso también se observa como la mayoría de los tickets se concentran en el inicio de curso. Este patrón se repite cada año.



A continuación, se muestra un gráfico en el que puede observarse la distribución mensual de las categorías de incidencias y peticiones. Esta categorización permite un estudio más profundo de la problemática de usuario.



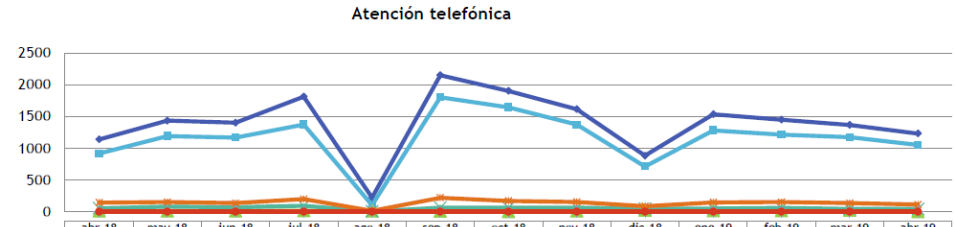
Cabe destacar, dentro de la gestión de CSU, el importante aumento de la gestión multimedia, que día a día cobra más relevancia en la Universidad.



En comparación con el año pasado, las solicitudes de asistencia multimedia han crecido un 14%.

Por último, respecto a la atención telefónica, se muestra una gráfica donde se observa la evolución anual del número de llamadas, acompañando a esta información algunos datos sobre su tratamiento, como el número de llamadas perdidas o el número de llamadas que se desvían a la central remota (desborde).

Cabe destacar el elevado número de llamadas que se atienden, debido al eficaz sistema de call center existente.

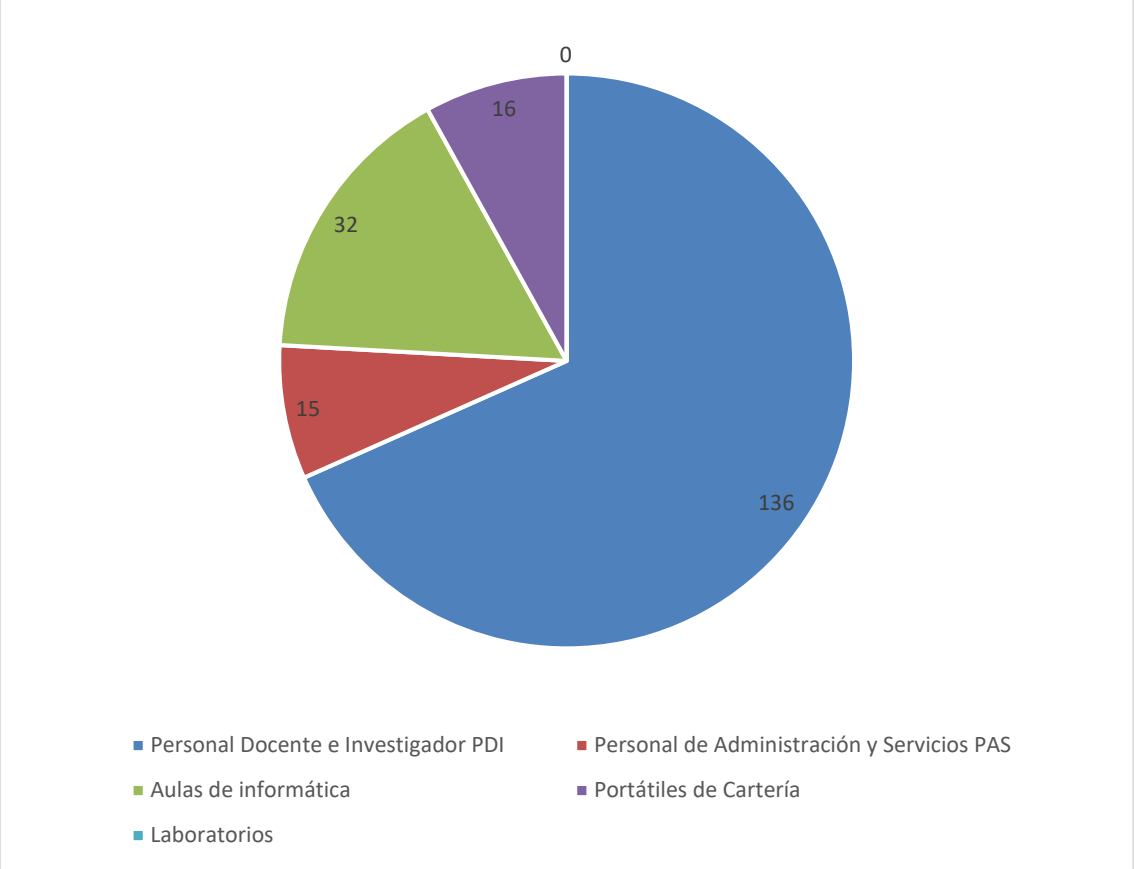


	abr-18	may-18	jun-18	jul-18	ago-18	sep-18	oct-18	nov-18	dic-18	ene-19	feb-19	mar-19	abr-19
RECIBIDAS	1138	1433	1401	1811	223	2148	1901	1613	882	1535	1448	1366	1231
ATENDIDAS CSU	916	1191	1166	1372	104	1800	1644	1371	712	1281	1215	1173	1052
PERDIDAS	15	13	14	16	14	10	3	15	22	18	16	22	4
DESBORDE	55	81	70	94	6	66	64	65	47	53	61	45	44
INCOMPLETAS	145	153	137	200	15	221	171	155	88	149	153	136	113
%DESBORDE	5%	6%	5%	5%	3%	3%	3%	4%	5%	3%	4%	3%	4%
% INCOMPLETAS	13%	11%	10%	11%	7%	10%	9%	10%	10%	10%	11%	10%	9%

Puesto de Usuario

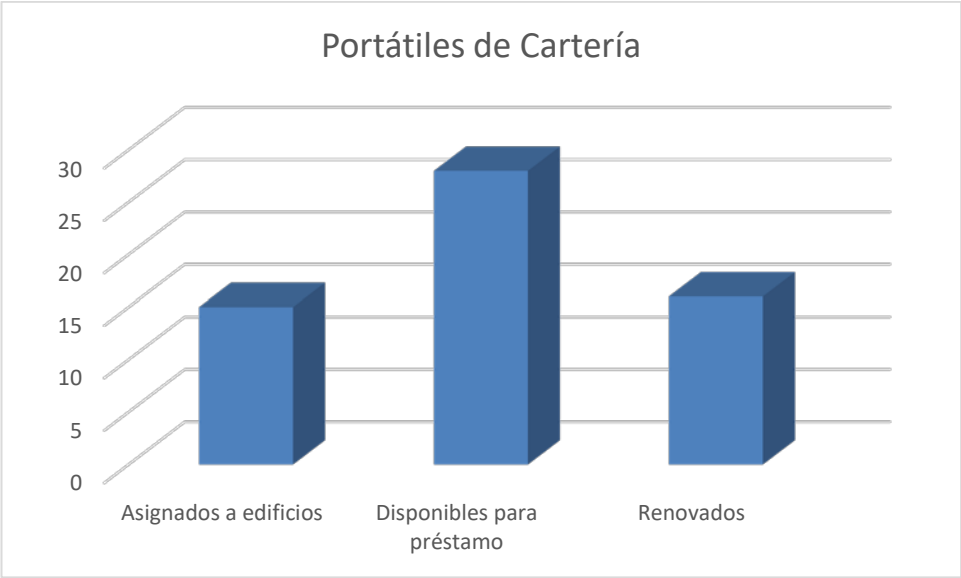
Este Servicio es el encargado tanto de la renovación anual de equipamiento (Personal de Administración y Servicios y Personal Docente e Investigador), como de la instalación de nuevos equipos en caso de incorporación de personal a la Universidad, además de los cambios de configuración derivados de la movilidad de éste.

La resolución del concurso del pasado curso, ha permitido la renovación de los siguientes equipos personales (PCs):



Los nuevos equipos de PAS y PDI ya utilizan el sistema operativo Windows 10, y en el caso de PAS, el usuario no tiene permisos de administrador, lo que aumenta la seguridad del sistema, minimizando el número de incidencias y consecuentemente la pérdida de tiempo derivada de su resolución.

Los datos referentes al mantenimiento y renovación de portátiles cuyo préstamo gestiona el Área de Campus, comúnmente llamado “Portátiles de Cartería” son los siguientes:



Impresión

Este año se ha desplegado un nuevo parque de impresoras de grupo en todas las áreas de PAS, pasando del modelo tradicional de adquisición y mantenimiento de equipos por parte del CIC y compra de consumibles por parte de las áreas, a un modelo de pago por uso, proporcionado por Coanda, la adjudicataria del concurso. En dicho modelo se paga una cantidad prefijada que puede variar en función del uso que se le dé a cada máquina.

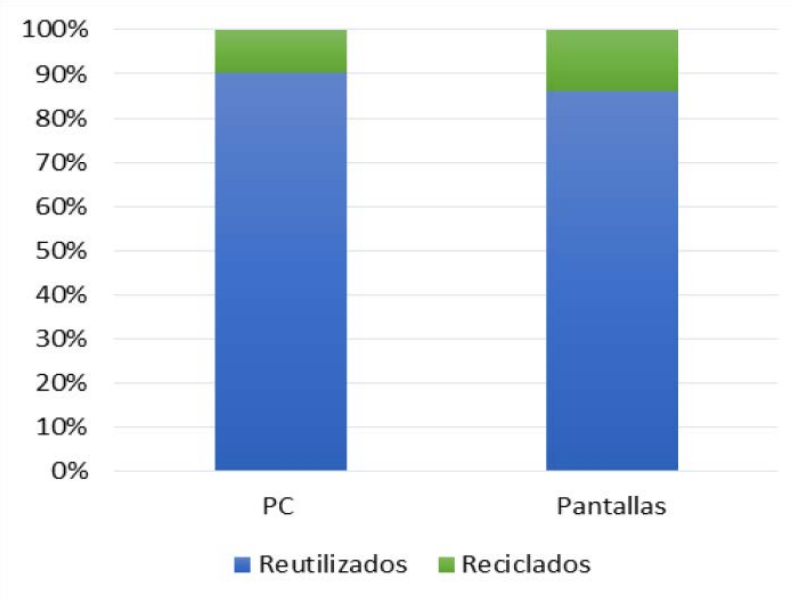
El número total de impresoras distribuidas es de 90, utilizadas por 499 usuarios. Cada impresora se comparte por un máximo de 15 usuarios.

Reciclaje

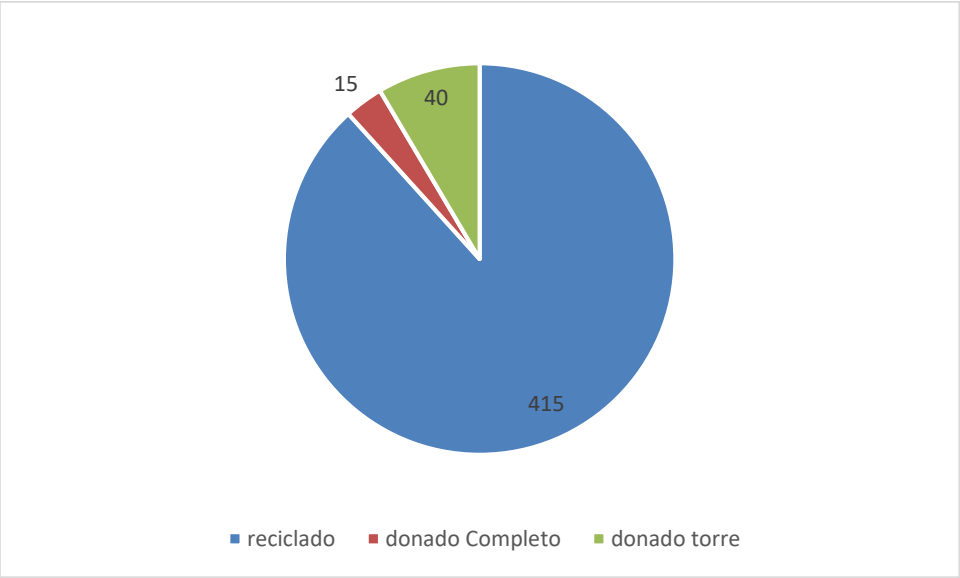
Este año se ha reciclado un algo más de 9.000 kilos de residuos electrónicos. A continuación, se muestra un gráfico donde se muestran las cantidades retiradas y la tipología.

Entidad productora	Universidad Pablo de Olavide	
Centro	Revertia Porriño	
Nº Recogidas	1	
Tipo de RAEE	Uds.	Kg.
01 - PC de sobremesa	470	5.640
03 - Servidores	3	90
99 - Otros	34	2.065
Total general	507	7.795

El equipamiento que no ha podido ser objeto de reutilización ha sido enviado a plantas de reciclaje para su adecuada gestión y valorización.



Un porcentaje de estos equipos reutilizados se ha dedicado a donaciones. La empresa de reciclaje, en nombre de la UPO, ha enviado a 12 centros públicos solicitantes un total de 15 equipos completos y 40 torres de pcs, suponiendo un 10 % del total.



Imágenes de Equipos Homologados

La instalación del software y sistema operativo en los nuevos equipos, renovados y reubicados se lleva a cabo mediante un sistema de despliegue de imágenes propio del CIC.

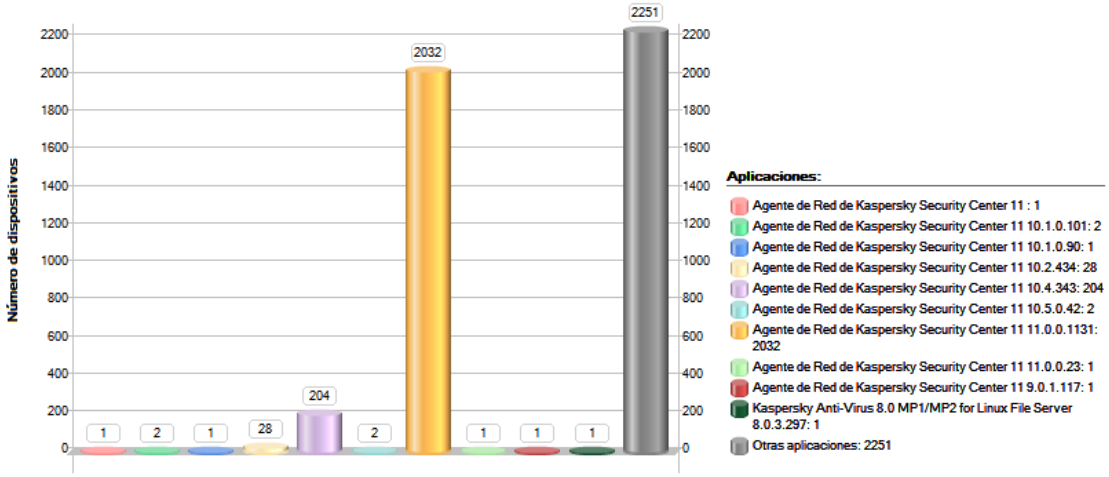
Actualmente hay disponible el siguiente número de imagen y variantes:

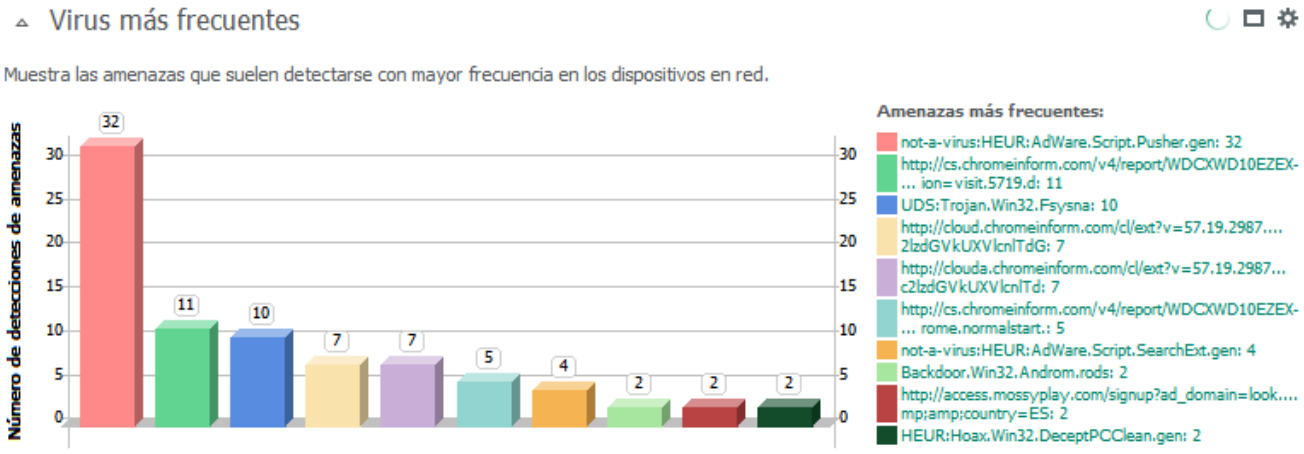
- Windows 7: 16 imágenes – 213 variantes
- Windows 10: 10 imágenes – 69 variantes

Servicio de Prevención, Detección y Eliminación de Virus Informáticos y Malware

La protección antivirus de puesto de usuario y servidores se gestiona mediante Kaspersky Security Center.

El estado actual de despliegue y la relación de virus más más detectados es el siguiente:



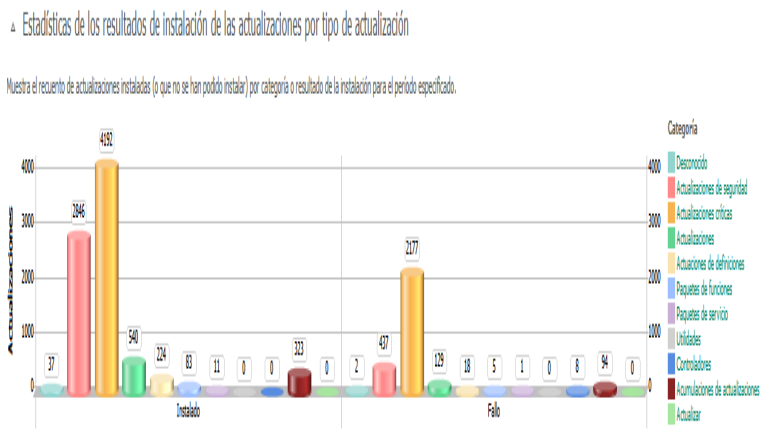


Servicio de Actualización de Sistemas Windows

Este sistema automatizado permite optimizar la descarga de las actualizaciones de Microsoft, utilizando servidores propios y evitando así el acceso a Internet de cada uno de los PCs para descargar cada nuevo parche.

El incremento del número de actualizaciones disponibles y el control previo al despliegue se refleja en el número constante de equipos pendientes de actualizar. No obstante, este control previo garantiza la interacción de los nuevos parches con las aplicaciones ya existentes.

Estas actualizaciones se gestionan mediante la herramienta Kaspersky Security Center. En el siguiente gráfico pueden observarse diferentes tipos de actualizaciones realizadas en los equipos personales de la UPO.



Programas Office 365, Imagine (antiguo Dreamspark)

En base al acuerdo alcanzado entre Microsoft y la CRUE, todas las Universidades con Office correctamente licenciado para sus PAS/PDI (tanto en modalidad Campus como Select u Open), podrán conseguir para sus alumnos/as/PAS/PDIs, licencias gratuitas de Office Pro, para uso personal en sus PCs, Macs, Portátiles, Móviles y Tabletas.

- Microsoft Office 365 (Windows, Mac, IOS, Android): 5.034 usuarios/as.

Por otra parte, se mantiene el programa Microsoft Imagine (antiguo Dreamspark), que permite el uso de software orientado al desarrollo de aplicaciones a los/as alumnos/as de determinadas Facultades.

Software de Microsoft (Microsoft Imagine). Para PDI y alumnos/as de los Grados en Biotecnología; Grado en Ciencias Ambientales; Grado en Geografía e Historia; Grado en Ingeniería Informática en Sistemas de Información; Grado en Nutrición Humana y Dietética y Grado en Trabajo Social (condición del proveedor) (uso en equipos personales).

- 2.375 alumnos/as.
- 440 profesores/as.

Servicio de Almacenamiento, compartición y ejecución de archivos en red: Samba

Servicio centralizado de almacenamiento de archivos que permite el acceso a documentos de uso diario por parte de todos los integrantes de un área de administración.

Actualmente hay definidos 204 grupos y están registrados 642 usuarios en el servicio.

Se están utilizando 5.5 Tbytes de espacio, de un total de 7.9T.

Este año el servicio ha pasado a un servidor virtual, de este modo, la continuidad del servicio basada en cluster pasa a depender de los mecanismos de continuidad del sistema de virtualización.

Herramienta de Trabajo en Grupo BSCW

Esta herramienta web colaborativa para grupos de trabaja ha sido actualizada a la versión 5.1.8, además se ha realizado una purga de usuarios inactivos.

Número de usuarios activos: 4.406.

Volumen de datos: 461,4 Gb.

Como novedad, el acceso a la herramienta se hace ahora a través del portal de autenticación centralizada.

Aulas de Informática

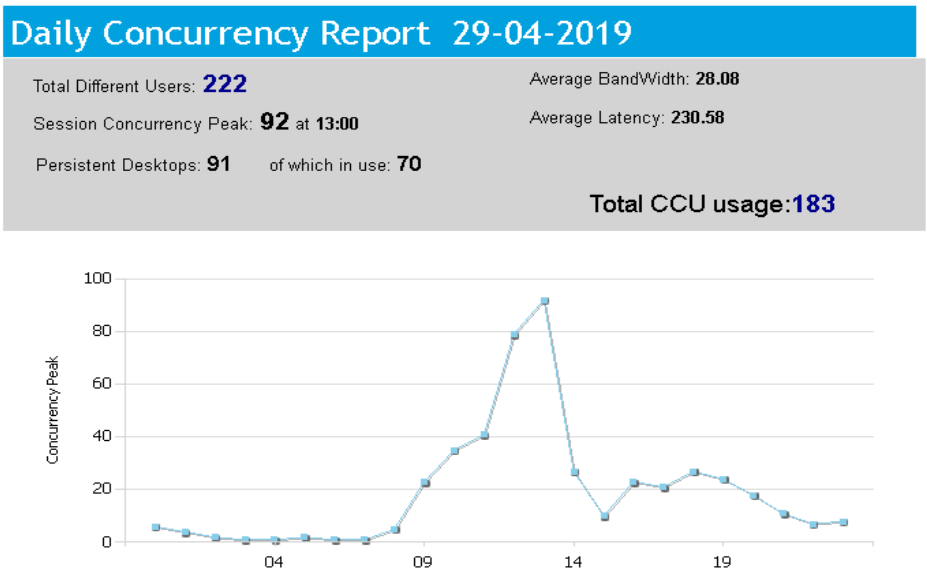
Los datos de PCs, aulas y aplicaciones de docencia gestionadas son estos:

- Número de PCs gestionados: 791.
- Número de aulas de informática: 34.
- Número de aplicaciones software: 279 (aprox. 60% es software libre).

Estas aplicaciones deben solicitarse de forma anual, de modo que el software no solicitado se elimina y así no interfiere con el que queda instalado.

Escritorios Virtuales

En las aulas de informática y, en especial, fuera de ellas, se ha impuesto mayoritariamente el uso de MyApps como herramienta de acceso al software de docencia. Las conexiones han ido en aumento a la vez que la herramienta ha ido consolidándose, hasta tener más de 200 usuarios diarios con picos de más de 100 conexiones simultáneas.



Total Applications Available in Production: 180

Total Different Users during this Period: 258

Max Concurrency peak: 32 (on 30-May-2019 11:05)

Top 30 Applications

Application	Count
IBM SPSS STATISTICS 25	683
GOOGLE CHROME	184
WOLFRAM MATHEMATICA	92
WOLFRAM MATHEMATICA_ENG	90
MICROSOFT WORD_ARABIC	79
EVIEWS	57
BLEND FOR VISUAL STUDIO	50
ARCMAP	43
MICROSOFT EXCEL_ENGLISH	37
VINA	33
LIGAND EXPLORER	31
_INTERCAMBIADOR DE FICHEROS	30
LINDO	24
ADOBE_ACROBAT	21
ATLAS.TI	16
CHIMERA	16
GOOGLE EARTH	14
ARCGLOBE	14
MICROSOFT POWERPOINT_ARABIC	13
AUTODOCK	9
LINUX_CLOUD	8
MICROSOFT WORD	8
MOZILLA FIREFOX	8
BIOINFORMATICA_RNASEQ	6
7-ZIP	6
LINUX-DTI	6
WOLFRAM MATHEMATICA 2012_ENG	6
OPENOFFICE WRITER	5
ARCCATALOG	4
LINUX-CAP	4

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

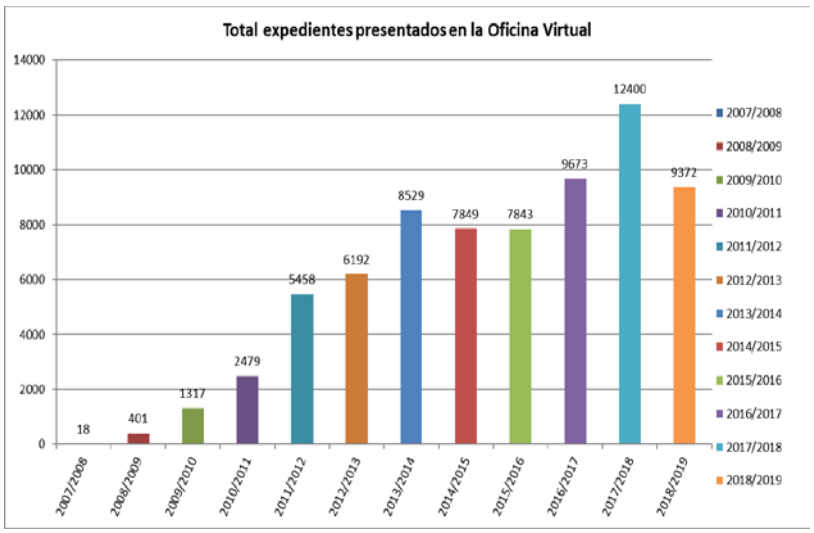
aplicativo, para, incluir el acceso mediante integración con adAS (sistema de Single Sign On). Este nuevo tipo de acceso permite que los todos los integrantes de la comunidad universitaria de la UPO (PAS, PDI y estudiantes) puedan utilizar sus credenciales de la Universidad, es decir el usuario y contraseña, 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.

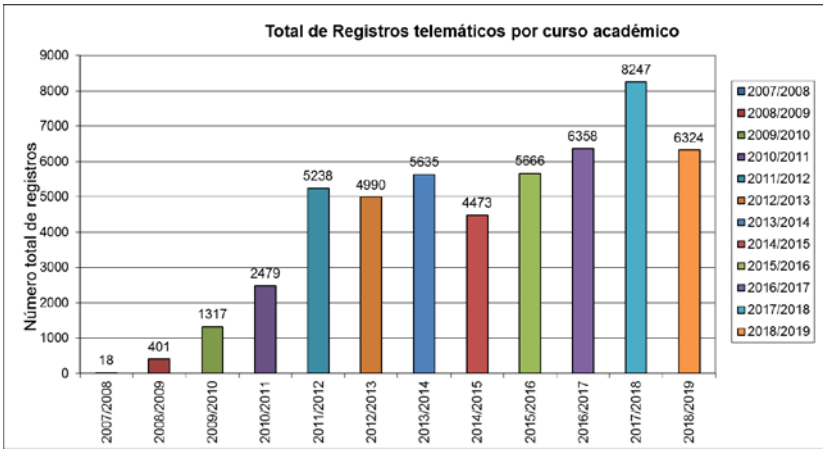
Esta acción, en definitiva, mejoró tanto la seguridad de acceso como la accesibilidad, ya que emite el acceso mediante credenciales de usuario, o mediante certificado digital, o DNIe.

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

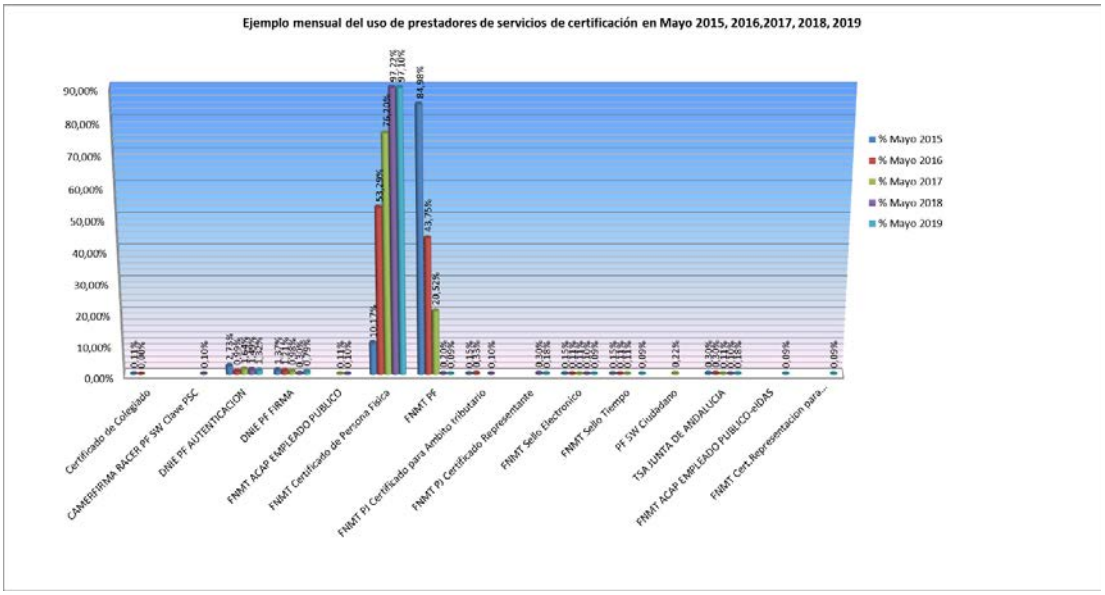
Apoyo en la creación y mantenimiento de la oficina de asistencia al ciudadano, en su relación con la Universidad, en la que se han instalado una serie de equipos que el ciudadano podrá utilizar para presentación de trámites electrónicos y será asistido por funcionarios habilitados para este fin por la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

@FIRMA

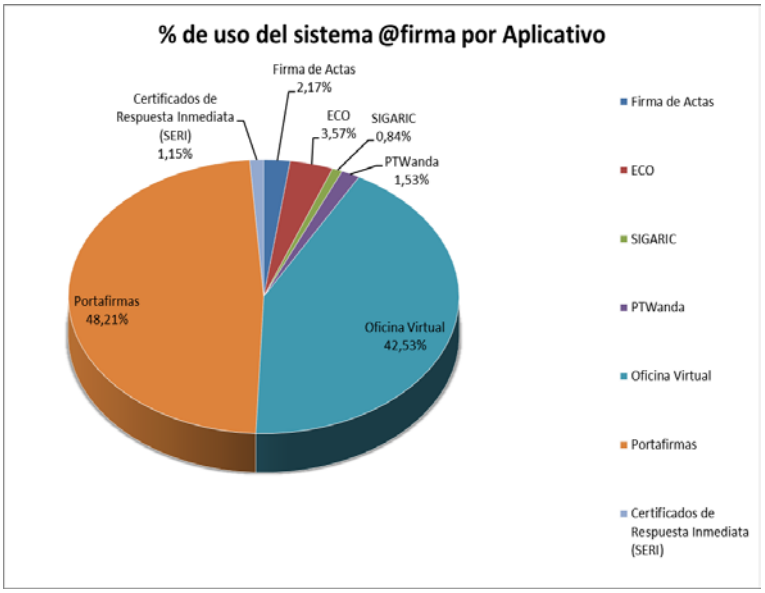
A principios de 2015, a partir del 2 de marzo, la FNMT empezó a emitir un nuevo tipo de certificado electrónico de identidad de persona física de la FNMT-RCM, que mejora la seguridad y que también implicó cambios en la infraestructura de @firma instalada en la Universidad. Durante un tiempo convivirán tanto el certificado antiguo como el nuevo.

En el siguiente gráfico se muestran los tipos de certificado por parte del firmante que se han utilizado para la firma de documentos en la infraestructura existente en la Universidad. Se puede observar que ya un 97,10% de los certificados utilizados pertenecen al nuevo tipo que empezó a expedir la FNMT

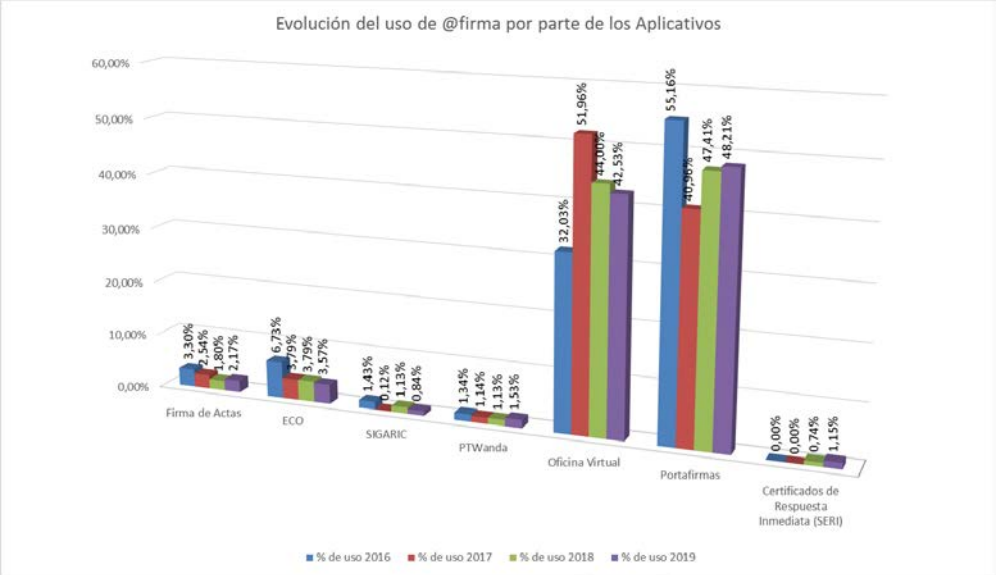
(Certificado Persona Física), frente al 10%,53%,76% y 92% de los años anteriores y que el anterior FNMT PF apenas se usa ya (0,09%). Y que el DNIE PF tanto de autenticación, como de firma, respecto a sus inicios ha descendido su uso al 1,32% y 0,799% respectivamente.



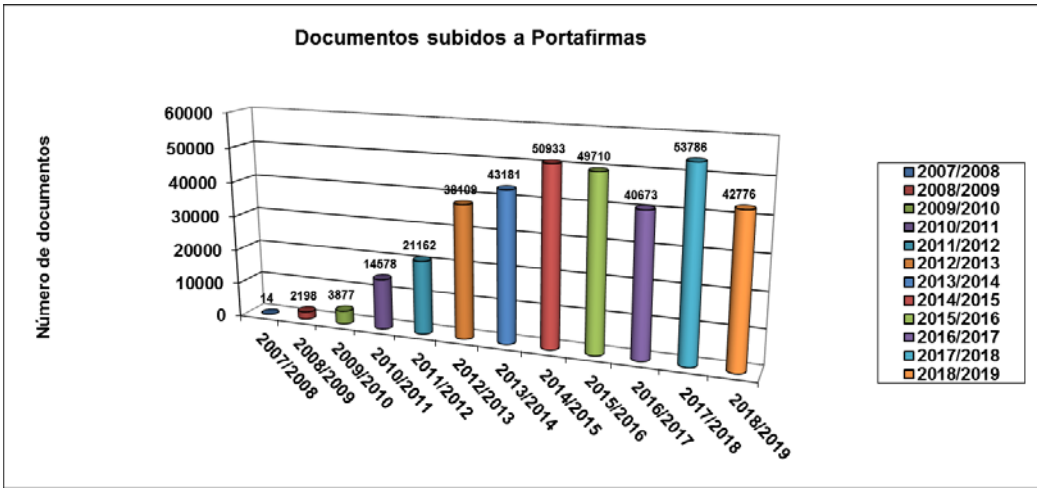
En el siguiente gráfico se muestra el uso del sistema @firma por aplicativo:



En el anterior gráfico podemos ver que las aplicaciones a través de las cuales se realizan firmas electrónicas son Portafirmas y Oficina Virtual. También observamos respecto a los Certificados de Respuesta Inmediata que ha aumentado su uso con respecto al pasado año como podemos observar en la siguiente gráfica.



Evolución de número de documentos firmados en @firma a través del aplicativo Port@firmas



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, lo cual responderá a las exigencias tecnológicas actuales, con vistas al cumplimiento del 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.

Nuevos Procedimientos en Producción

En este periodo se ha desarrollado el siguiente procedimiento, es decir, estudio; desarrollo; implantación; prueba; puesta en producción; presentación; soporte; y mantenimiento, en estrecha colaboración con diversas Áreas Administrativas. Se enumeran a continuación:

- Reconocimiento Académico de Programas Movilidad Internacional (ERASMUS): Tramitación de Reconocimiento Académico para participantes en Programas de Movilidad Internacional (ERASMUS) con validación académica por parte del Centro.

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 Asignaturas Matriculadas en Grado: A través de este servicio se proporcionará a los estudiantes un certificado acreditando las asignaturas matriculadas en el curso académico.
- Certificado de Asignaturas Matriculadas en Máster Universitario: A través de este servicio se proporcionará a los estudiantes un certificado acreditando las asignaturas matriculadas en el máster universitario que estén cursando.
- Certificado de Asignaturas Matriculadas en Doctorado: A través de este servicio se proporcionará a los estudiantes un certificado acreditando su matrícula en el Programa de Doctorado que estén cursando.

Procedimientos sobre los que se han desarrollado evolutivos

En este periodo se han desarrollado evolutivos, es decir, estudio; desarrollo; implantación; prueba; puesta en producción; presentación; soporte; y mantenimiento, sobre diversos procedimientos electrónicos en estrecha colaboración con diversas Áreas Administrativas. Se enumeran a continuación:

- Procedimiento de Solicitud de Equipamiento Informático Descatalogado (EID). Proyecto de donación de material obsoleto a los diferentes estamentos que lo soliciten para uso educativo, o como donación a países necesitados. En ninguno de los casos se podrá utilizar el material entregado con ánimo de lucro.
- Procedimiento de Selección Personal de Administración y Servicios (SPAF_S Y SPAF_C). Tramitación de solicitudes presentadas por los candidatos a plazas de concurso de acceso, entre acreditados.
- Procedimiento de Solicitud de Reconocimiento y transformación de Créditos (Grado) (RDC). Permite a los estudiantes de Grados solicitar de forma telemática los Reconocimientos/Transferencias de créditos de asignaturas (RDC).
- Procedimiento de Solicitud de Títulos Oficiales (Grado). (STOG). Permite a los estudiantes de Grados solicitar de forma telemática los Reconocimientos/Transferencias de créditos de asignaturas (RDC).
- Procedimiento de Solicitud de Certificado Académico Personal (SCAP). Permite a los estudiantes de Grados, Licenciaturas, Diplomaturas e Ingeniería Técnica solicitar y recoger

de forma telemática las certificaciones donde conste cualquier dato solicitado de su expediente académico.

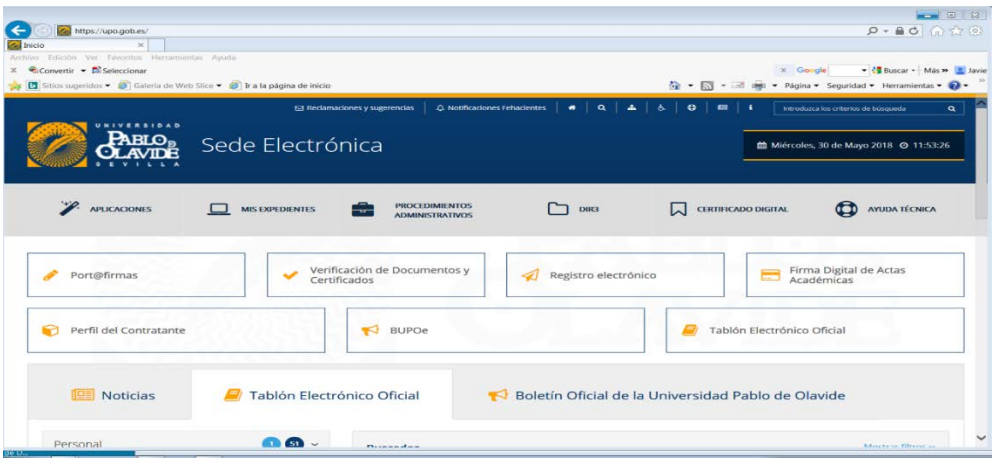
Sede Electrónica

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.

En 2016 se dotó a la sede de un nuevo certificado emitido por la autoridad de certificación Camerfirma. 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.

Proyectos en fase de desarrollo

- *GEISER* (Gestión Integrada de Servicios de Registro).

  Se está llevando a cabo la implantación en las oficinas de Registro General de la Universidad, de 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 tareas:

  - Elaboración de un plan de pruebas exhaustivo, que ha permitido testear la herramienta en su conjunto.
  - Configuración y adaptación del aplicativo a las necesidades la UPO.
  - Alta de usuarios y configuración de Unidades asignadas.
  - Sesiones de concienciación y estrategia con todos los usuarios involucrados.

- Configuración de equipos de trabajos (imágenes de sistema operativo).
- Configuración de impresoras selladoras (pegatinas) y escáneres de alta capacidad.

Se prevé que su entrada en producción se produzca en noviembre.

- *TangramGO!* (Plataforma de Tramitación).

El proyecto de implantación de la nueva plataforma de tramitación está caracterizado por:

- Provisión de la plataforma de Tramitación Electrónica TangramGO!.
- Configuración de look&feel según guía de estilo de la Universidad Pablo de Olavide.
- Integración con Geiser.
- Integración con la actual Sede Electrónica de la Universidad Pablo de Olavide.
- Puesta en marcha de los 25 procedimientos administrativos previamente modelados en la plataforma TangramBox V2.X.
- Paquete de formación en TangramGO! V3.0 a los usuarios tramitadores, administradores y desarrolladores de la Universidad Pablo de Olavide. Se realizará un plan de formación presencial para el colectivo de PAS y PDI más un curso online que estará operativo durante todo el tiempo que esté en servicio la plataforma TangramGO! en la Universidad Pablo de Olavide.

TangramGO! está compuesta por un conjunto de módulos escalables y reutilizables, con el fiel reflejo de la reutilización de componentes entre administraciones públicas:

- Permite el acoplamiento entre subsistemas. Incluye un bus de interoperabilidad que permite dicho acoplamiento de una manera muy efectiva.
- Es totalmente escalable. Cualquiera de los componentes que conforman la plataforma puede escalar para soportar el volumen de expedientes, usuarios o documentos que necesite procesar la Universidad Pablo de Olavide. Como ejemplo de ello está el almacén de expedientes en el Gestor Documental Alfresco, que puede escalar desde una instancia básica

al principio, hasta una implantación en alta disponibilidad con numerosos volúmenes y réplicas.

- Seguridad. TangramGO! ha sido certificado en el cumplimiento con el Esquema Nacional de Seguridad (RD 3/2010). Mediante el cumplimiento de las medidas de protección para cada una de las dimensiones de seguridad puede conseguirse un nivel de seguridad elevado.

    - Disponibilidad. Dispone de scripts de copias de seguridad con una política de rotación configurable. Por otro lado, la infraestructura de virtualización permite la realización de snapshots que ayudan a reducir de forma considerable los tiempos necesarios para una posible recuperación del sistema.

    - Autenticación. La plataforma provee estos criterios de autenticación:

        - Certificado electrónico reconocido por @firma, inclusive certificados nuevos eIDAS, en dispositivos Software o Hardware (tarjetas criptográficas, DNIe, HSM). La autenticación no se realiza mediante applet Java.
        - Ldap / Single Sign-On SAML 2. Por medio de usuario y clave de los ciudadanos y trabajadores públicos, en integración a sistema de la Universidad Pablo de Olavide.
        - Cl@ve. sistema clave-usuario.

    - Firma electrónica. Cada documento administrativo oficial requiere de al menos una firma. En TangramGO!, todas las firmas se realizan en formato CAdES, XAdES y PAdES usando de certificados digitales X509v3 y componentes de firma oficialmente reconocidos (Autofirma). La firma puede realizarse desde la Sede, el Escritorio de Tramitación o el Portafirmas y puede comprobarse desde el validador de firmas "valide.redsara.es".

      La plataforma TangramGO! soporta la actualización de las firmas a formatos longevos.
    - Integridad. Se garantiza la integridad de los documentos de los expedientes administrativos por la disponibilidad de las firmas en formatos oficialmente reconocidos y la posibilidad de poder validar cualquier documento firmado. La

plataforma ofrece funciones adicionales para proteger la integridad de la información, como la separación de los roles funcionales y la protección de documentos y expedientes.

- Confidencialidad. Toda la plataforma hace uso de conexiones seguras HTTPS con algoritmos adaptados a los últimos estándares. La calidad de las conexiones puede comprobarse fácilmente mediante test públicamente disponibles. Por otra parte, se protege la confidencialidad mediante la limitación de acceso a los datos: por una parte, cada interesado sólo puede acceder a los datos de sus propios expedientes, y por otra, los tramitadores sólo pueden ver y acceder a los expedientes en los que participan en su tramitación o a los superiores de los mismos.
- Trazabilidad. Todas las operaciones que avanzan los procedimientos o que generen documentos y cualquier otro tipo de información son registradas, así como los accesos a expedientes y documentos. Estos registros pueden protegerse mediante la copia de seguridad o el envío de los mismos a otros sistemas.

Actualmente se ha instalado y configurado la infraestructura de servidores necesaria para soportar a todos los componentes de la plataforma. Ya se encuentra desplegada en el entorno de desarrollo, con la hoja de estilos adecuada a la Sede Electrónica de la UPO y ya se ha realizado una primera validación de la misma.

También se han comenzado las reuniones con las Áreas para el "remodelado" de los procedimientos y su implantación en la nueva plataforma:

- Instancia Genérica
- Solicitud de Certificado Académico Personal
- Reconocimiento de Créditos
- Traslado de Expedientes
- Solicitud de Título Oficial de Grado
- Reconocimiento Académico de Programas Movilidad Internacional (RAPMI)

- *Alfresco (Gestor Documental)*.

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

  * Alfresco CE 3.3 (para PTWanda)

  * Alfresco 4.0.d (para documentación de usuarios internos de la Universidad)

  * Alfresco Enterprise 5.1.2

    - Firma de Actas
    - Expedientes PDI (Personal Docente e Investigador)
    - Varias aplicaciones que se están desarrollando:

      - FDA (Firma de Actas Académicas)
      - BUPO (Boletín oficial de la Universidad Pablo de Olavide)
      - TEO (Tablón Electrónico Oficial de la Universidad Pablo de Olavide)
      - SGIC (Sistema de Garantía Interna de Calidad)
      - TANGRAM
      - Oficinavirtual
      - TFM (Trabajos Fin de Master)

  Se están realizando una serie de actuaciones junto a la empresa keensoft, sobre las diversas versiones del Gestor Documental Alfresco, existentes en la Universidad.

  De ellas ya se encuentran finalizadas:

    - Auditoría del entorno 5.1.2. Esta ya se encuentra finalizada.
    - Configuración de un entorno de pruebas para 5.1.2.

  Y se tienen previsto acometer:

    - Actualización de la versión 5.1.2 a 6.x.
    - Migración de los datos existentes en el aplicativo con la versión 4.0.d al aplicativo con la versión 5.1.2.

- *Port@firmas* (gestor centralizado de documentos que permite la firma digital). Se está trabajando en la implantación de una nueva versión del aplicativo que sustituirá al actual. Se ha optado por la versión ofrecida por el Ministerio de Hacienda y Administraciones Públicas que finalmente estará integrado dentro de la infraestructura de TangramGO.

- Nueva aplicación para solicitar publicaciones en el *Tablón Electrónico Oficial (TEO) y el Boletín Oficial de la UPO (BUPO)*, que sustituirá a las actuales. Se encuentra actualmente a falta de las últimas correcciones para entrar en producción lo antes posible. Ya está validada por los usuarios.

- *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

Se han realizado trabajos de optimización en el sistema de proxy frontal (basado en HAProxy) Dichas mejoras se orientan a facilitar los trabajos de operación, mantenimiento, configuración y seguridad de la plataforma.

Se insiste en la política de actualización de cifras, certificados y https para los servidores web para mejorar la seguridad general del servicio.

Se continúa con el proceso de renovación de las infraestructuras web más antiguas, controlando la obsolescencia de contenidos y actualizando la infraestructura de servidores que ofrece este servicio con nuevas máquinas instaladas en entornos virtualizados. De esta forma se mejora tanto la seguridad como la disponibilidad del servicio.

Se consolida el uso de la nueva plataforma OpenCms de Facultades, Departamentos y portal de profesorado, quedando planificadas nuevas incorporaciones de contenidos y actualización de nuevas titulaciones.

Se han incorporado a la infraestructura de nuevas máquinas virtuales para dar servicio a nuevas versiones de software en uso, como por ejemplo Limesurvey (encuestas), OJS (plataforma de revistas de Biblioteca) y aplicaciones corporativas basadas en PHP.

Se ha procedido a actualizar el portal que contiene la Sede Electrónica con el paquete empresarial OCEE de OpenCms, lo que ha derivado en una mejora sustancial del rendimiento y por tanto de la experiencia de navegación por parte de los usuarios.

Se publican los nuevos portales de las Facultades de Derecho, Facultad de Empresariales, Faculta de Ciencias Sociales y Facultad de Humanidades. En breve se publicará también la Facultad de Experimentales.

Se comienza con la elaboración de la nueva estructura para los portales de los departamentos.

Se publica el nuevo portal del profesorado. Este portal muestra información académica de la docencia del profesor, datos de contacto, proyectos de investigación y datos adicionales que el profesor puede añadir como su currículum, links de interés, …

Correo electrónico

El sistema de correo está basado en software libre y se adapta a las nuevas necesidades de usabilidad, capacidad, disponibilidad y seguridad. Hemos seguido trabajando en implementar nuevas mejoras y actualizaciones para mantener al día este servicio, mejorando algunos aspectos relativos a la usabilidad y sobre todo la seguridad. Por otra parte, se han instalado nuevas estafetas de correo entrante y saliente en un entorno virtualizado que permite mejorar la disponibilidad y seguridad de este servicio.

Se sigue confirmando el beneficio de la apuesta realizada a la adhesión de nuestro servicio de correo al proyecto de infraestructura común para el servicio de correo electrónico en la comunidad RedIRIS (Servicio Lavadora), que se encarga de filtrarlo antes de llegar a nuestras estafetas, reduciendo el número de mensajes de spam que llega a las mismas de forma considerable, y mejorando, en consecuencia, la calidad del servicio con un evidente ahorro de costes en su gestión.

Se sigue aplicando una mejora continua tanto en los protocolos de actuación como en las salvaguardias que protegen el sistema de correo ante nuevos y diversos tipos de ataques, adaptándolos y mejorándolos tras cada nuevo incidente. Se ha conseguido aumentar la rapidez con la que se detectan

ataques por captura de credenciales, logrando detenerlos de forma rápida y efectiva. También se está 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

Hemos aplicado las últimas actualizaciones disponibles a nuestro Proveedor de Identidad e incrementado el número de aplicaciones que están protegidas por este sistema. Este Proveedor de Identidad facilita el acceso a diferentes servicios mediante usuario y contraseña, tarjeta inteligente o DNI electrónico. Mejora el control de acceso de los servicios y, por tanto, la seguridad. 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.

Almacenamiento

Se ha trabajado en la actualización de los sistemas de almacenamiento de la Universidad. De esta forma se garantiza una mejor seguridad y disponibilidad en el acceso a los datos. También se ha trabajado en su ampliación, debido a la gran demanda de espacio de almacenamiento por parte del creciente número de servicios ofrecidos a la Universidad.

Se ha seguido trabajado en la ampliación de la infraestructura de almacenamiento necesaria para poder modernizar el servicio de copias de seguridad, de tal forma que las copias de seguridad se almacenen en disco y no en cinta. De esta forma se logra que tanto las copias de seguridad como las recuperaciones de datos sean mucho más ágiles y eficientes.

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:

- Firma Digital de Actas Académicas, se han realizado mejoras y correcciones en la aplicación de Firma de Actas relativas a las diligencias.
- En UXXI-INV se consolida la migración económica con UXXI-EC y se comienza a explotar el módulo de "TimeSheets" en el Portal del Investigador. Se está evaluando diferentes alternativas para comenzar a explotar la gestión de convocatorias de la investigación de manera telemática.
- La aplicación UPOAvisos se migra de servidor actualizando su tecnología hacía PHP 7, mejorando las funcionalidades que ofrece con la visualización de documentos resúmenes de los envíos realizados que facilitan procesos posteriores de calidad.
- Se han realizado mejoras y correcciones en el aplicativo para la evaluación de los Trabajo Fin de Grado de la Facultad de Empresariales.
- Se han realizado mejoras de programación (haciéndola más eficiente) en la aplicación EnvíaSMS encargada de enviar SMS en la Universidad.
- Migración del SID (Sistema de Información para la Dirección) de Oracle Discoverer 10g a Oracle Business Intelligence 12c (OBI 12c).

  Previamente se hizo una migración de Discoverer 10g a Oracle Business Intelligence 11g (OBI 11g) que no llegó a ponerse en producción. Después se acometió la migración de 10g a la 12c y está a punto de ponerse en producción.

  Las principales tareas de este proyecto son:

  - Instalación y configuración del software de Oracle Business Intelligence 12c.
  - Migración del repositorio y catálogo desde la versión OBI 11g a la versión 12c.
  - Actualización del método de autenticación al corporativo (OAM y adAS).
  - Actualización de la versión de la base de datos.

- PCI (Portal de Consulta de Indicadores)

  Se ha hecho un nuevo desarrollo de la aplicación Web de PCI para la gestión de los indicadores de calidad. Se actualiza la aplicación, tanto funcional como tecnológicamente, y se mejora la usabilidad.

- LOPD

  La Disposición Adicional 7.ª de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, establece un método para la publicación del número del documento identificativo de los interesados cuando esta sea necesaria en el caso de anuncios y publicaciones de actos administrativos.

  Ante las numerosas consultas recibidas, las autoridades de control en materia de protección de datos han elaborado de forma conjunta unas orientaciones provisionales para la aplicación de la mencionada Disposición Adicional para tratar de evitar que la adopción de fórmulas distintas pudiera dar lugar a posibilitar, ante publicaciones diversas, la recomposición íntegra del número de dicho documento identificativo.

  Se ha elaborado un documento Excel y otro Word que realiza el enmascarado de los documentos identificativos en base a las orientaciones proporcionadas por dichas autoridades de control.

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).
- SGIC (Sistema de Garantía Interna de Calidad).
- TFM (Trabajos Fin de Master).
- Docentia.
- Actualización Sistema Integración de Datos del Data Warehouse.

  El proyecto consiste en la migración y actualización del Sistema de Integración de Datos del Data Warehouse a la herramienta Oracle Data Integrator 12c. Las principales tareas son:

  - Instalación y configuración del software de Oracle Data Integrator 12c.
  - Migración de los procedimientos ETL al nuevo entorno de integración ODI 12c.
  - Actualización y optimización de los procedimientos ETL.

- Se comienza con la migración de las bases de datos a la versión Oracle 12c y Oracle12c RAC para las bases de datos del ERP.

- Se acometen mejoras en UPOCompra para el tratamiento de contratos menores.
- Cambio de la plataforma Elavon a Redsys para el pago mediante TPV de recibos de UXXI-AC.

Aula Virtual

Durante el curso académico 2018-2019, la sección dedicada al Aula Virtual ha estado trabajando en distintas líneas. Como es habitual y necesario, se han venido realizando labores propias de soporte y seguimiento del servicio en cuanto a atención (personal, telefónica, etc.) a los/as usuarios/as y sus correspondientes solicitudes de servicio; mantenimiento y actualización diaria de profesores-as/alumnos-as/asignaturas que utilizan el Aula Virtual y su acceso a la plataforma de docencia virtual institucional. El acceso a la plataforma se realiza desde https://campusvirtual.upo.es

Desde el servicio de Aula virtual se procede, de oficio, a crear todos los espacios virtuales de docencia virtual del curso académico que comienza.

Esta plataforma, como se ha recogido en ocasiones anteriores, está a la vanguardia del aprendizaje telemático y tiene una especial orientación hacia el usuario final (estudiantes/profesores). Entre sus múltiples ventajas frente a otros modelos de Docencia Virtual cabe resaltar que:

- Dispone de una interfaz más intuitiva y amigable. La nueva interfaz presenta una herramienta actualizada, flexible y abierta pues incorpora funcionalidades de Web 2.0, e integración con redes sociales.
- Permite personalizar la interfaz con la tecnología web 2.0 para seleccionar, arrastrar y mover y así configurar los elementos del curso, el área de contenido o la barra de menú del curso.
- Numerosas funcionalidades de las que carecen otras metodologías como, entre otras, herramientas de blog o wiki. Posibilidad de hacer búsquedas y enlazar (incrustar) directamente en el área de contenido, recursos publicados en Powerpoint, Flickr, SlideShare o Youtube, permitiendo la asociación de metadatos.
- Las herramientas de evaluación se han actualizado mejorando la experiencia virtual de exámenes, encuestas, catálogo de preguntas, permitiendo establecer categorías, objetivos de aprendizaje y metadatos.

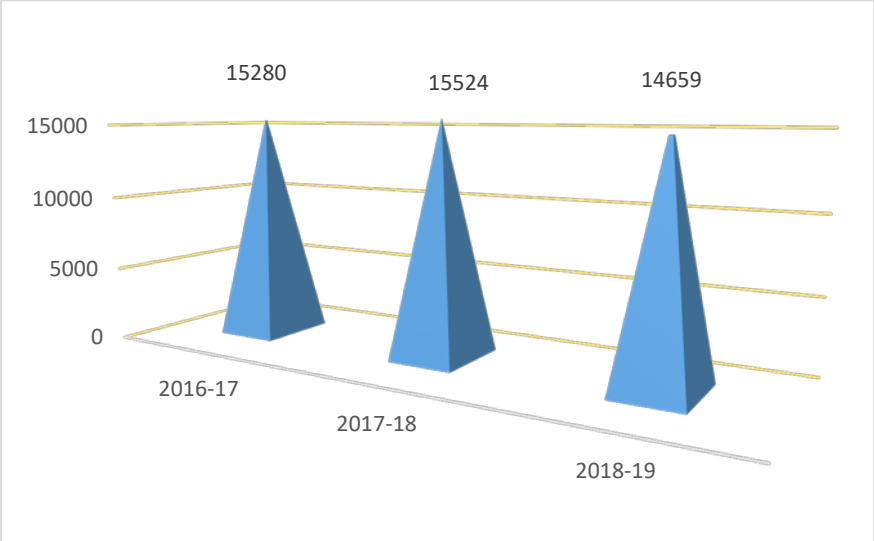
- La barra de herramientas del menú del curso sigue siendo totalmente personalizable, incluyendo la posibilidad de añadir cabeceras, líneas de división de herramientas, enlaces a carpetas y a cualquier otro elemento disponible dentro de las herramientas activas en el curso.
- Potente módulo para el seguimiento de las actividades, tareas del/a alumno/a en el curso, así como módulo SCORM con multitud de informes de seguimiento de la actividad del/la alumno/a en los contenidos del mismo.
- Roles de usuario/a (profesor/a, alumno/a, etc.) más personalizado y flexible, fácilmente gestionables.
- Acceso mediante SSL.

Durante el curso académico 2018-2019 las tareas realizadas han estado dirigidas a la mejora del rendimiento de la plataforma y a la satisfacción de los usuarios:

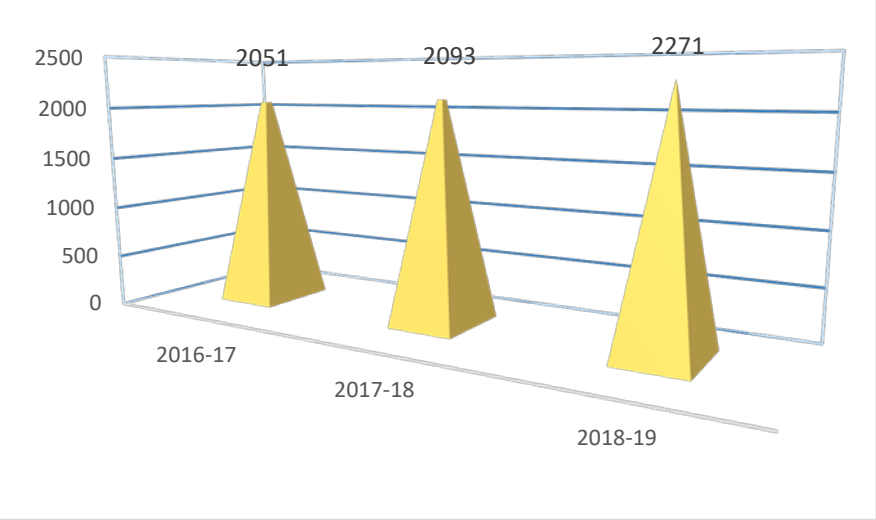
- Se ha modificado el documento de Gestión del Aula Virtual en el que se recogen los criterios y procedimientos de gestión relacionados con la programación de actividades de mantenimiento regular en el Aula Virtual, la creación y borrado de espacios virtuales, y las altas y bajas de estudiantes y docentes en los espacios virtuales, para adecuarse mejor a la operativa académica.
- Con el objetivo de mantener la plataforma de Aula Virtual lo mejor posible, mejorando así el tiempo de respuesta de la plataforma al usuario y reduciendo el tiempo de parada para mantenimiento, se ha realizado limpieza de espacios obsoletos del curso 2017-2018 de la plataforma Blackboard Learn 9.1 y se han eliminado de la plataforma los usuarios que no tienen ningún espacio virtual asignado en el curso 2018-2019.
- Se ha actualizado el módulo Blackboard Mobile Learn facilitando y mejorando la experiencia de los/as alumnos/as y profesores/as de la Universidad que deseen hacer uso de la plataforma desde dispositivos móviles. Con esta aplicación se puede acceder a los cursos/asignaturas en cualquier momento, desde el dispositivo móvil, consiguiendo una mayor interactividad y un seguimiento, a tiempo real, de todas las actividades que se realizan en el curso de manera inmediata e intuitiva.
- Se está trabajando en la actualización de la infraestructura que soporta la plataforma de Docencia Virtual, con el fin de poder llevar a cabo las actualizaciones de software que pudieran ser necesarias y que exigen una infraestructura más actual.

Datos estadísticos Aula Virtual

Total de estudiantes - espacios por curso académico



Total de docentes - espacio por curso académico



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 especial 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 a nuestros usuarios y que su uso sea lo más amigable posible.

En el curso 2017-18 comenzaron dos series de video tutoriales, 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, en la que se expone de forma clara y concisa el funcionamiento de las distintas herramientas del Aula Virtual. Durante este curso, se han seguido añadiendo videos a estas series, teniendo actualmente un total de 48 vídeos.

El Plan de Formación se ha centrado en conocer lo máximo posible las nuevas funcionalidades de la plataforma de docencia virtual (Blackboard Learn 9.1). La formación se ha dividido en distintos niveles:

- Nivel básico. Formación en el uso del Aula Virtual a nivel básico. Semipresencial. 2 horas de duración.
- Nivel medio. Formación en el uso del Aula Virtual a nivel medio. Presencial. 2 horas de duración.
- Nivel avanzado. Formación en el uso del Aula Virtual a nivel avanzado. Presencial. 2 horas de duración.
- Collaborate Ultra. Formación en el uso de Blackboard Collaborate Ultra. Presencial. 2 horas de duración.

Todos los seminarios se plantean como herramienta de formación para el profesorado y de aclaración de dudas surgidas en el manejo de la plataforma de docencia virtual. Los seminarios se han distribuido en dos sesiones por semana, en horario de mañana y tarde, en los meses octubre - noviembre de 2018, y febrero - marzo de 2019.

Datos sobre la participación del plan de formación

Sesión	Inscritos	Asistentes	N.º de sesiones	% Participación
Nivel básico	27	22	4	81,48
Nivel medio	43	37	4	86,04
Nivel avanzado	55	50	4	90,90
Collaborate Ultra	40	34	4	85
Total	165	143	16	85,85