

El correo electrónico

El correo electrónico

El Correo Electrónico (Email) es un servicio de red que permite a los usuarios enviar y recibir mensajes a través de sistemas de comunicación electrónica. Es la herramienta de comunicación formal y legalmente reconocida en la mayoría de las organizaciones. Se utiliza para la coordinación, la documentación de decisiones, el envío de informes y la comunicación con partes externas (clientes, proveedores, otras instituciones).

Estructura y componentes esenciales del correo electrónico

Un mensaje de correo electrónico se compone de dos partes principales que facilitan su envío y comprensión:

- **Cabecera (Header):** Contiene la información técnica necesaria para el enrutamiento y la identificación, como la dirección del remitente, las direcciones de los destinatarios, la fecha y la hora del envío, y el asunto. Es la parte que organiza y dirige el mensaje.
- **Cuerpo (Body):** Contiene el mensaje real y el contenido que el remitente desea comunicar. Puede ser texto plano, HTML (que permite formatos, colores, imágenes) o una combinación.

Los componentes esenciales de un correo son los siguiente, y los dos primeros son necesarios:

- **Remitente:** La dirección de correo electrónico de la persona o entidad que envía el mensaje. Confirma la identidad del emisor.
- **Destinatario:** La dirección de correo electrónico principal o principal a la que va dirigido el mensaje. Indica la persona (o personas) que debe actuar o responder principalmente.
- **Asunto:** Una línea de texto que resume brevemente el tema del mensaje. Permite al destinatario priorizar la lectura y organizar su bandeja de entrada.
- **Cuerpo del Mensaje:** El contenido principal (texto, imágenes) que se desea comunicar. Contiene la información o la solicitud de acción.
- **Archivos adjuntos:** Documentos, imágenes u otros archivos que se envían junto con el mensaje. Proporcionan la documentación o soporte necesario para el contenido del correo.

Protocolos de Acceso

Los protocolos estándares que un programa de correo electrónico usa para descargar o visualizar los mensajes desde el servidor central de correo son el POP, IMAP y Exchange. Su principal diferencia radica en dónde se guarda la copia principal del mensaje.

- El protocolo POP (Post Office Protocol) descarga completamente al dispositivo local (ordenador) y elimina nuestro correo del servidor. Por su escasa practicidad ha caído en desuso. Solo se usaría si solo accedes al correo desde un único dispositivo y necesitas liberar espacio en el servidor.
- El protocolo IMAP (Internet Message Access Protocol) se basa en la sincronización. El correo principal permanece en el servidor, mientras el dispositivo local (desde el que estamos consultando nuestro

buzón) solo muestra una copia sincronizada. Es el estándar actual, y permite ver la misma bandeja de entrada, carpetas, correos leídos/no leídos y enviados en todos tus dispositivos (ordenador, móvil, web).

- El protocolo Exchange (Microsoft Exchange ActiveSync / MAPI): Sincronización Total e Integrada. El correo, los contactos, el calendario y las tareas permanecen en el servidor y se sincronizan completamente en tiempo real. Es la base del trabajo en Microsoft 365. Garantiza que tu calendario, tus tareas, tus contactos y tu correo estén siempre idénticos y se actualicen al instante en tu móvil, Outlook de escritorio y el correo web. Además, permite funcionalidades avanzadas como la delegación de calendario y los buzones compartidos.

Listas de Distribución y Grupos:

La UPV ofrece a Servicios, Centros, Departamentos, Grupos de Investigación, etc. la posibilidad de creación de listas de distribución autogestionables.

Para solicitar la creación de listas de distribución es necesario leer la normativa y rellenar el impreso de Solicitud de Lista de distribución

¿Qué son las listas de distribución?

Las listas de distribución son mecanismos de difusión de información basadas en el correo electrónico.

El objetivo de una lista de distribución es hacer llegar **mensajes a varios usuarios de una vez**, en lugar de enviar un mensaje individual a cada uno de ellos. Las listas de distribución son útiles para compartir información en un Servicio u Organización o para organizar grupos de trabajo cuyos componentes deban estar permanentemente informados del desarrollo de una tarea.

Cualquier lista de distribución **debe tener un administrador de la lista**, que se encarga de gestionarla, y **usuarios** que son los que **envían mensaje** a la lista para ser distribuidos **o reciben** los mensajes de la lista. Además de estos administradores y usuarios de las listas se puede destacar la presencia del **administrador del servicio de listas de distribución que es la persona encargada de crear y configurar las listas**. El administrador del servicio de listas de distribución es personal del Área de Sistemas de Información y Comunicaciones, mientras que el administrador de una lista puede ser cualquier persona con dirección de correo electrónico (e-mail) que se haga cargo de ella y aprenda a administrarla. Para administrar una lista de distribución NO hace falta tener grandes conocimientos de ningún tipo: sólo es necesario saber navegar por web o saberse manejar con el correo electrónico y conocer unas pocas instrucciones.

Para implantar el servicio de listas de distribución en la UPV se ha utilizado un programa que permite crear, gestionar y utilizar las listas denominado Mailman. La comunicación con este programa Mailman se puede realizar de dos formas:

- A través de un interfaz web: <https://listas.upv.es>
- Mediante el envío de mensajes de correo electrónico a la dirección < lista >-request@upv.es Para obtener un resumen de ordenes disponibles, mandar un mensaje que contenga en el cuerpo (o en el subject), la palabra HELP. Mailman nos responderá con un mensaje con ayuda sobre los comandos que podemos utilizar.

Mailman mantiene bajo su control las listas que se van creando en la UPV. El usuario interactúa con Mailman de dos formas: enviando un mensaje a una de sus listas para que Mailman lo distribuya entre sus miembros

o solicitando que Mailman efectúe alguna operación sobre una de sus listas (suscribirlo, desuscribirlo, solicitar información, etc.).

Tipos de listas disponibles en la UPV

Cuando se crea una lista de distribución, se le asignan una serie de atributos que la dotan de unas características particulares en cuanto a la manera de suscribirse, la gestión de los mensajes enviados a la misma, la privacidad de los contenidos, etc.

Antes de solicitar una lista de distribución al ASIC es necesario tener claros los siguientes términos, que son los que se piden en el formulario de solicitud:

- **Política de suscripción:** Abierta o Cerrada (Se refiere a cómo se gestionarán las solicitudes de suscripción de nuevos usuarios). 'Cerrada' exigirá autorización por parte del administrador de la lista y confirmación por parte del solicitante. 'Abierta' pedirá confirmación al solicitante.
- **Moderación de los mensajes de los suscriptores:** No moderar, Aprobar, Rechazar o Eliminar. Si se van a moderar las contribuciones de mensajes, esto es, si los suscriptores van poder enviar libremente mensajes a la lista o van a ser moderados, en cuyo caso indicamos qué hacer con los mensajes recibidos.
- **Moderación de los mensajes de los no-suscriptores:** Aceptar, Aprobar, Rechazar o Eliminar.

En los casos de moderación las opciones son:

- 'No moderar' acepta todos los mensajes de los suscriptores.
 - 'Aprobar' retiene el mensaje hasta que el administrador lo apruebe.
 - 'Rechazar' lo devuelve al remitente con mensaje de devolución.
 - 'Eliminar' lo elimina sin notificación alguna.
- **Privacidad del archivo de contribuciones a la lista:** público o privado. Con esto indicamos quién puede ver el historial de contribuciones a la lista. 'Público' permite el acceso a la recopilación de mensajes a cualquier usuario. 'Privado' hace que sólo los suscriptores (con su usuario y contraseña) puedan consultar los contenidos de dicha lista.

Normativa

Puede solicitar la creación de lista de distribución cualquier Servicio de la UPV, Centros, Departamentos, Grupos de Investigación, etc. En general, todos los organismos vinculados a la UPV. Todas las listas pertenecerán al dominio "@upv.es".

La petición se realizará mediante el formulario colgado a tal efecto en la web del ASIC debidamente cumplimentado y enviado por correo electrónico.

Características de la lista de distribución: Las listas que se pueden crear en la UPV podrán tener las características del punto anterior.

Todas las listas de distribución deben tener un administrador de la lista, este administrador de la lista podrá ser el propio solicitante u otra persona en quien éste delegue.

Administración de la Lista

La contraseña del administrador de la lista es personal e intransferible.

Es responsabilidad del administrador de la lista el correcto uso de la Lista de Distribución.

Otras listas de distribución Microsoft 365 y Google Groups

Más allá de las listas de la UPV, otras plataformas de colaboración modernas han integrado las funciones de lista de distribución dentro de estructuras más amplias, denominadas Grupos, que ofrecen recursos adicionales:

- Grupos de Microsoft 365: Al crear un Grupo de Microsoft 365 (el contenedor que subyace a un Equipo de Teams), se genera automáticamente una dirección de correo electrónico grupal. Esta dirección de correo actúa como una lista de distribución para el envío de información, pero también está asociada a un buzón de correo compartido, un calendario y un sitio de almacenamiento (SharePoint), consolidando recursos para la colaboración.
- Google Groups: Google Groups permite la creación de una lista de distribución que funciona simultáneamente como un foro de discusión web. Es una herramienta muy utilizada para la colaboración con usuarios externos a la organización, ya que mantiene un archivo histórico de todas las comunicaciones en línea, accesible y consultable por los miembros.

Ambas soluciones garantizan que la comunicación a un grupo se realice con una única dirección, pero lo hacen integrando dicha comunicación dentro de entornos más ricos y funcionales que las simples listas de reenvío.

Normativa de uso del correo electrónico de la UPV¹

1.- Objetivo y ámbito de aplicación

La Universitat Politècnica de València (UPV) ofrece a la comunidad universitaria el servicio de Correo Electrónico. El objetivo de esta Normativa de Uso es garantizar la calidad del mismo y un uso de acuerdo con los fines últimos de la Universidad.

Otros objetivos que persigue esta normativa son los siguientes:

- a) Preservar la privacidad y seguridad de las comunicaciones de la UPV.
- b) Evitar situaciones que puedan causar algún tipo de responsabilidad civil o penal.
- c) Garantizar la seguridad y rendimiento de los sistemas informáticos de la UPV.

Toda persona que utilice estos servicios adquiere la condición de usuario del servicio y por ello está obligado al cumplimiento de la normativa redactada en el presente documento.

Esta normativa se aplica además a:

- a) Todos los equipos de la UPV implicados habitualmente en el encaminamiento del correo electrónico.
- b) Todos los componentes de mensajes (texto, cabeceras, anexos, registros de actividad, ...) residentes en ordenadores gestionados por la universidad.

¹ Aunque no aparece específicamente en el temario, consideramos necesario conocer la normativa propia de la UPV, ya que es un texto sobre el que se puede preguntar sin miedo a la impugnación.

- c) Todos los propietarios de buzones de correo de la universidad.
- d) Todos los servicios internos que hacen uso del correo electrónico, tales como las listas de distribución, noticias, etc.

Una copia de esta normativa estará siempre a disposición del usuario y publicada en la web de la universidad.

2.- Acceso a los servicios

2.1.- Usuarios de los servicios

Pueden disfrutar del servicio de correo electrónico de la UPV los miembros de la comunidad universitaria, tanto los alumnos matriculados en cualquier ciclo, como el personal de administración y servicios y el personal docente e investigador, además de las entidades o personas autorizadas en virtud del convenio o autorización debidamente emitida por el órgano competente de la Universitat Politècnica de València.

El servicio se vincula a la existencia del vínculo con la UPV.

2.2.- Asignación de recursos

El tamaño de los mensajes en tránsito está limitado. De igual forma la capacidad de almacenamiento de los servidores es finita y como tal, se asignará a los usuarios un tamaño de buzón, dentro de unos límites aceptables.

El correo electrónico ha sido diseñado con el propósito de enviar mensajes cortos, no para la difusión de ficheros de grandes tamaños, para los cuales están disponibles otros medios. El Área de Sistemas de Información y Comunicaciones (ASIC) establecerá el espacio de memoria en disco atribuido a las cuentas de correo.

El usuario puede revisar la versión más reciente de la Política de cuentas de correo en la dirección <http://www.asic.upv.es/normativa>.

3.- Responsabilidades del usuario

3.1.- Aceptación de las condiciones y normas de uso

La utilización del servicio de Correo Electrónico proporcionado por la Universitat Politècnica de València implica el conocimiento y plena aceptación de las normas de uso y condiciones que se especifican en el presente documento y en todos los documentos complementarios de normativa de utilización de servicios y recursos informáticos proporcionados por la Universitat Politècnica de València.

3.2.- Confidencialidad del correo electrónico

Se asignará una cuenta y una contraseña a cada usuario del servicio. El usuario es responsable de mantener la confidencialidad de su cuenta y contraseña, y de todas las actividades que se efectúen bajo su cuenta.

La UPV recomienda que los mensajes confidenciales vayan siempre encriptados.

3.3.- Uso exclusivo del correo electrónico para comunicaciones interpersonales

El correo electrónico es una herramienta para el intercambio de información entre personas, no un medio de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos.

3.4.- Uso para fines profesionales o académicos

Las cuentas de correo de la Universitat Politècnica de València no deben ser, en principio, utilizadas para fines privados, ya que constituyen una herramienta de trabajo. Sin embargo, dado que en ocasiones un usuario puede verse obligado a gestionar asuntos personales durante su horario de trabajo, se autoriza el uso de este servicio siempre y cuando la frecuencia y duración sea limitada y ello no afecte a su uso profesional o académico. Este uso personal además no puede constituir una actividad política, comercial o con ánimo de lucro y no puede ser inapropiado u ofensivo.

3.5.- Prohibición de abuso en el correo electrónico (ACE)

El abuso en el correo electrónico es definido por la Red Académica y de Investigación Nacional (Rediris) como “las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios”. Estas actividades se pueden catalogar, a título no exhaustivo, en los siguientes grupos:

- Abusivas por el contenido: queda prohibido enviar, almacenar o distribuir mensajes cuyo contenido atente contra los derechos reconocidos en las Leyes españolas y Tratados Internacionales suscritos por España o promueva actuaciones contrarias a la ley.
- Abusivas por el medio: queda prohibido el envío de correo utilizando un servidor de correo ajeno sin el consentimiento del titular del mismo.
- Abusivas por no solicitadas: queda prohibido el envío de comunicaciones electrónicas con finalidad comercial a una pluralidad de receptores que no las hayan solicitado (“spam”) a excepción del expresamente autorizado por la UPV.
- Abusivas por su finalidad: queda prohibido el envío de mensajes de correo electrónico cuyo único propósito sea el de sobrecargar, paralizar o, de cualquier otro modo, perjudicar el normal uso de este servicio o los equipos informáticos de otros usuarios de Internet.

Está prohibido cualquier uso del correo electrónico que pueda ser catalogado como ACE en cualquiera de las modalidades anteriormente descritas.

El envío de correo masivo o difusión masiva de mensajes y el envío continuo de un número elevado de mensajes queda asimismo limitado. Desde el momento en que la Universitat Politècnica de València detecte que dichas actividades perjudican el correcto funcionamiento de los servicios y/o provoquen retrasos en las entregas de correo de los demás usuarios de los sistemas, adoptará las medidas que considere necesarias, ya sea bloqueando direcciones IP, dominios, usuarios u otras medidas, pudiendo incluso procederse a la suspensión inmediata y sin previo aviso del servicio.

Asimismo, el usuario del correo electrónico de la UPV por el mero hecho de hacer uso del servicio se entiende que acepta los principios enunciados en la Política antispam de la Universitat Politècnica de València, que se conforma como la principal herramienta de la UPV para la lucha contra esta práctica tan perniciosa para el uso responsable de los recursos de Internet.

4.- Usos incorrectos de los servicios

Se considera incumplimiento de las condiciones y normas de uso del correo electrónico UPV, los supuestos siguientes:

- Difusión de contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
- Difusión de mensajes correo electrónico sin identificar plenamente a su remitente. En el caso de que la cuenta sea utilizada por grupos de usuarios, deberá identificarse el autor.
- Difusión de contenidos contrarios a los principios enunciados en los Estatutos de la Universidad.
- Difusión de mensajes comerciales o propagandísticos sin autorización expresa.
- Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
- Ataques con objeto degradar el servicio.
- Envío masivo de mensajes o información que consuma injustificadamente recursos de la UPV.
- No está permitido manipular las cabeceras de los mensajes para intentar ocultar o falsear la identidad del usuario remitente del mensaje.
- No está permitido instalar ni usar servidores o encaminadores de correo que no cuenten con la autorización de la UPV.
- Hacer un uso del correo electrónico contrario a las condiciones y normas de uso del presente documento y de todos los documentos complementarios de normativa de utilización de los servicios y recursos informáticos proporcionados por la Universitat Politècnica de València.

Uso Adecuado de los Campos de Dirección:

En la siguiente tabla damos una visión general de los tres campos de dirección disponibles en un correo electrónico:

<i>Campo</i>	<i>Función (Rol del Destinatario)</i>	<i>Uso Correcto</i>
Para (To)	Acción y Responsabilidad Primaria.	Se incluye a los destinatarios de los que se espera una respuesta directa , una acción específica o que son los principales responsables del tema.
CC (Copia de Carbón)	Información y Conocimiento.	Se incluye a los destinatarios que necesitan estar informados del contenido, pero de los que no se espera una respuesta o acción directa . Actúan como observadores.
CCO (Copia de Carbón Oculta)	Privacidad y Cumplimiento.	Se incluye a destinatarios que deben recibir el mensaje, pero cuya presencia no debe ser visible para el resto de los destinatarios (los campos "Para" y "CC").

Campo "Para" (Acción):

Es el campo destinado al destinatario directo del que se espera una respuesta o una acción. Para un uso adecuado, se ha de intentar limitarlo a las personas absolutamente necesarias para que el mensaje no se pierda. Si hay varios destinatarios, es recomendable nombrar en el cuerpo del correo a quién corresponde cada tarea.

Campo "CC" (Información):

Es un campo destinado a destinatarios indirectos de los que no se requiere respuesta o acción. La persona destinataria entiende, cuando recibe un correo en copia, que es solo para que se considere informado del contenido. Por tanto, debe ser usado con moderación, para evitar la saturación de su bandeja de entrada y que se ignoren los mensajes importantes.

Es común usar "CC" para mantener informado a un superior o a un coordinador de proyecto sin requerir su intervención; a quien ha encomendado una tarea que se completa o tramita con ese correo; e incluso al superior jerárquico de la persona destinataria (PARA), para hacer constar que su subordinado ha recibido ese correo.

Campo "CCO " (Discreción):

Es el campo más importante cuando se envían correos a listas grandes de personas que no se conocen entre sí (ej. una comunicación a todos los estudiantes o proveedores). Su uso protege la privacidad de sus direcciones de correo electrónico.

Su uso es imperativo legal cuando la comunicación puede afectar a datos personales sensibles, como por ejemplo al hacer una comunicación al personal que ha secundado una huelga.

También se puede usar para informar a un tercero sin que el destinatario principal lo sepa. Pero este campo no debe usarse para espiar o socavar la confianza. Su uso debe estar justificado por la privacidad o el protocolo.

Uso Seguro del Correo (Riesgos):

El correo electrónico, a pesar de su utilidad, es la principal puerta de entrada para amenazas de seguridad como el phishing y el malware. El uso seguro se basa en la identificación de riesgos y la aplicación de buenas prácticas.

Phishing: Intentos de suplantación de identidad. El atacante se hace pasar por una entidad de confianza (un banco, un servicio informático o un directivo) para robar credenciales de acceso o información confidencial.

"Urgencia extrema, faltas de ortografía, solicitud de verificación de contraseña a través de un enlace."

Malware: Archivos adjuntos maliciosos que se activan al ser descargados o abiertos, infectando el sistema del usuario o de la red.

"Adjuntos inesperados o sin relación con el contexto, archivos con extensiones sospechosas (.exe, .zip inesperado)."

Spam / Correo No Deseado: Mensajes masivos e irrelevantes que saturan la bandeja de entrada y consumen recursos del servidor.

Para identificar estos correos hemos de estar atentos a las siguientes señales: “Contenido promocional o irrelevante que no ha sido solicitado por el usuario”.

Mejores Prácticas de Prevención

La responsabilidad de la seguridad recae tanto en la tecnología (filtros) como en el comportamiento del usuario:

- **Verificar al Remitente:** No confiar únicamente en el nombre que aparece. Compruebe la dirección de correo completa y asegurarse de que corresponde al dominio oficial de la organización que dice ser (ej. que termine en @upv.es o el dominio correcto del banco).

Si un directivo o superior pide algo urgente e inusual por correo, se ha de verificar la petición por otro medio (llamada telefónica o chat de Teams).

- **Manejo de Enlaces y Archivos Adjuntos:** Comprueba la dirección real a la que apunta (aparece en la esquina inferior del navegador) cualquier enlace pasando el cursor sobre él antes de hacer clic. Si el enlace es sospechoso, no hagas clic.

Nunca abras archivos adjuntos inesperados de remitentes desconocidos, incluso si parecen ser documentos legítimos (facturas, informes). Si tienes dudas, póngase en contacto con el remitente por separado.

- **Cuidado con la Información Sensible:** Nunca envíes contraseñas, números de cuenta o información altamente confidencial a través de un correo electrónico sin encriptar.
- **Utiliza el campo CCO** cuando envíe correos a listas de personas no relacionadas para proteger la privacidad de sus direcciones.

El eslabón más importante de la seguridad es el usuario. La conciencia y la precaución son las mejores defensas contra los ataques basados en correo.

Firma y Encriptación de Mensajes:

Estos dos conceptos son fundamentales para garantizar la autenticidad y la confidencialidad de la comunicación por correo electrónico, especialmente en el ámbito institucional donde se maneja información sensible.

Firma Digital de Mensajes (Autenticidad)

La Firma Digital no es la firma gráfica que se inserta en el pie del correo, sino un mecanismo criptográfico que asegura que el mensaje proviene realmente del remitente que dice ser y que no ha sido alterado durante el tránsito.

- **Objetivo:** Confirmar la identidad del remitente (autenticidad) y garantizar la integridad del contenido. Otorga validez legal y probatoria al mensaje, evitando la suplantación de identidad (spoofing).
- **Funcionamiento:** El remitente utiliza un certificado digital (o clave privada) único para generar un código que se adjunta al mensaje. El software de correo del destinatario verifica este código usando la clave pública del remitente. El destinatario ve un icono o mensaje que confirma que el correo es "Firmado Digitalmente" y es auténtico.

- Requisito: El usuario debe poseer un Certificado Digital válido (como el DNI electrónico o un certificado de una Autoridad de Certificación reconocida, ej. FNMT, ANF).

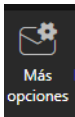
Encriptación de Mensajes (Confidencialidad)

La Encriptación (o Cifrado) es el proceso de codificar el contenido de un mensaje para que solo pueda ser leído por el destinatario legítimo.

- Objetivo: Asegurar la confidencialidad del mensaje. Impide que terceros (incluso si interceptan el mensaje) puedan leer el contenido. Protección de datos sensibles, personales o confidenciales (como actas, informes internos o datos sanitarios).
- Funcionamiento: El mensaje se transforma en un texto ilegible mediante un algoritmo. Solo el destinatario, que posee la clave privada asociada a su certificado, puede descifrar y leer el contenido. Garantiza que la información se transmite de forma segura a través de la red pública.
- Requisito: Tanto el remitente como el destinatario deben tener certificados digitales y, en la mayoría de los casos, el remitente debe conocer la clave pública del destinatario para cifrar el mensaje.

El proceso de encriptación (o cifrado) desde la perspectiva del usuario es sorprendentemente sencillo en los sistemas de correo modernos (pondré el ejemplo en Outlook en Microsoft 365 por ser el utilizado mayoritariamente en la UPV), ya que la plataforma se encarga de la complejidad técnica.

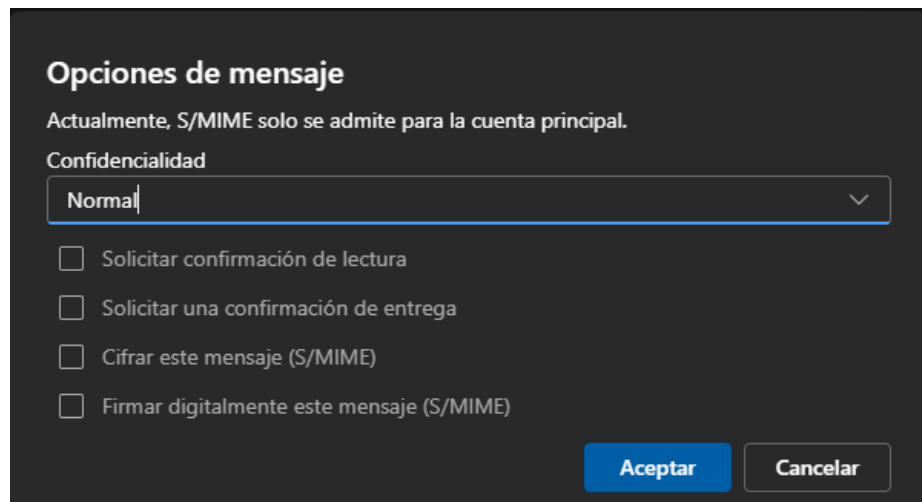
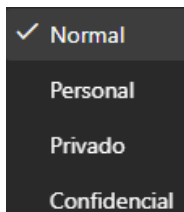
El objetivo es que solo el destinatario deseado pueda leer el mensaje. Para ello, el usuario tiene que realizar dos acciones clave: activar el cifrado y, en algunos casos, verificar la identidad del destinatario.



El usuario redacta el correo, añade los destinatarios y los archivos adjuntos. Después, en la pestaña de **Más opciones** en la barra de opciones del correo (no del programa) abrimos la siguiente ventana.

Además de las opciones de solicitar las confirmaciones de lectura y entrega, Outlook nos permite Cifrar y Firmar.

Además, desde el desplegable podemos elegir 4 opciones de confidencialidad del correo.



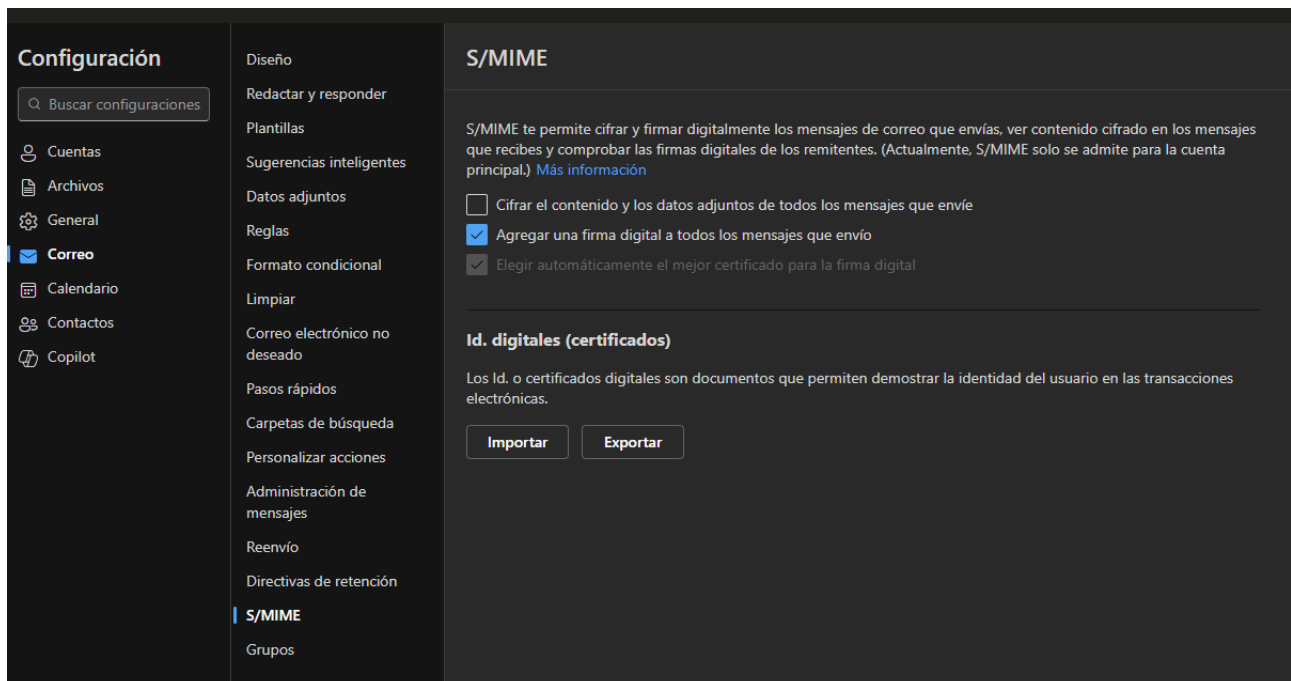
Seleccionada la opción de Cifrar este mensaje (S/MIME), es el servidor de Microsoft 365 el que toma el mensaje, lo cifra (lo vuelve ilegible) y aplica la política de acceso que el usuario seleccionó.

El remitente no tiene que gestionar claves o certificados para cada persona. En su lugar, el acceso se gestiona mediante la identidad digital del destinatario, que, actualmente en la UPV, se restringe únicamente a las cuentas de correo principal de cada usuario.

Cuando el destinatario lo abre, su cliente de correo (Outlook) verifica automáticamente su identidad (está logueado con su cuenta usuario@upv.es). Si su identidad coincide con los permisos definidos en el mensaje, el cliente descifra y muestra el contenido al instante, sin que el usuario tenga que hacer nada.

Si el mensaje se envía a un correo externo, el destinatario recibe un aviso de que tiene un mensaje protegido. Para leerlo, el destinatario debe verificar su identidad ante el servidor de la UPV. Esto se hace, por lo general, a través de Iniciar sesión con una cuenta de Microsoft o Google, o solicitar un código de un solo uso que se envía a su correo. Una vez verificada su identidad, el servidor descifra el contenido y se lo muestra en una ventana segura del navegador.

En las opciones de Configuración de **Outlook**, en el apartado **S/MIME** podemos configurar las opciones por defecto de nuestra firma y cifrado.



Cientes de Escritorio y Web:

Los clientes de correo son el software o la interfaz que los usuarios utilizan para acceder y gestionar sus mensajes. Se dividen en dos categorías principales según su modo de acceso y gestión de datos.

Cliente de Correo Web (Webmail)

El cliente Web, o Webmail, permite el acceso a la bandeja de entrada directamente a través de un navegador web (Chrome, Firefox, Edge, etc.).

Es una interfaz alojada en el servidor de correo. Y ofrece las siguientes ventajas:

- Ubicuidad: Acceso desde cualquier dispositivo con conexión a Internet, sin necesidad de instalar software.
- Sincronización Total: El trabajo se guarda siempre en el servidor, garantizando que el estado de los mensajes sea idéntico en todos los lugares.

- **Mantenimiento Cero:** No requiere que el usuario instale actualizaciones o gestione copias de seguridad.

Pero también presenta las siguientes desventajas:

- **Dependencia de la Conexión:** No se puede acceder o trabajar sin una conexión activa a internet.
- **Menos Funcionalidad:** Generalmente, ofrece menos opciones avanzadas de gestión y automatización que un cliente de escritorio.

Los principales webmail son Gmail o Yahoo Mail.

Cliente de Correo de Escritorio

El cliente de escritorio es un programa instalado localmente en el ordenador (PC o Mac) que se conecta al servidor para descargar y sincronizar los mensajes. Es una aplicación que se ejecuta en el sistema operativo local.

Sus **ventajas** son:

- **Trabajo sin Conexión:** Permite acceder a mensajes y redactar respuestas (que se enviarán después) sin conexión a internet.
- **Funcionalidad Avanzada:** Ofrece integraciones más profundas con el sistema operativo y herramientas avanzadas (reglas, plugins, cifrado avanzado).
- **Rendimiento:** Generalmente es más rápido y eficiente para gestionar grandes volúmenes de correo y búsquedas.

Y sus **desventajas**:

- **Configuración:** Requiere una configuración inicial (protocolos IMAP/POP).
- **Dependencia del Dispositivo:** La información descargada puede no estar totalmente sincronizada si se accede desde otro dispositivo.

Los principales ejemplos son: Mozilla Thunderbird (cliente de escritorio libre y gratuito, muy configurable) o Apple Mail (Cliente nativo para sistemas macOS e iOS).

Cientes de correo de Microsoft Outlook

Microsoft Outlook no es solo un programa para gestionar el correo electrónico; es una suite completa de gestión de información personal (PIM) que integra múltiples herramientas de productividad. Es el cliente por excelencia en entornos que utilizan **Microsoft Exchange** (como **Microsoft 365**).

Ventajas Clave en el Entorno Microsoft 365

Outlook destaca por su integración nativa y profunda con los servicios de Microsoft de Correo, Calendario, Tareas y Contactos. Outlook combina estos cuatro elementos en una única interfaz. La capacidad de convertir un correo en una tarea o una cita de calendario con un solo clic es una función esencial para la productividad.

Además, se integra con **Exchange** y **Teams**. Facilita la gestión de permisos para poder gestionar el calendario o el buzón de otro usuario de forma segura; al crear una reunión, consulta automáticamente la disponibilidad

de los compañeros a través del calendario de Exchange (ver Tema 30). Permite crear reuniones de **Microsoft Teams** directamente desde la interfaz del calendario de Outlook (ver Tema 30).

Al usar el protocolo nativo de Exchange, la sincronización de mensajes, estados (leído/no leído) y carpetas es prácticamente instantánea y más fiable que con protocolos genéricos como IMAP.

Outlook en sus Versiones

Outlook está disponible en diferentes formatos, todos ellos sincronizados:

- Outlook de Escritorio: La aplicación instalada en el PC o Mac que es la más potente.
- Outlook en la Web (OWA): Acceso a través del navegador (ej. email.upv.es).
- Outlook Móvil: La aplicación en smartphones y tabletas, utilizada, principalmente, para la revisión en movimiento y gestión de la agenda y citas de calendario.

Funcionalidades más relevantes de Outlook



Reglas: Permite crear reglas complejas para mover automáticamente correos a carpetas específicas, reenviarlos o aplicar categorías, lo que facilita la organización.

La gestión de las reglas se basa en definirle a Outlook una o varias condiciones que ha de cumplir el correo recibido (la variedad de condiciones que ofrece es realmente amplia) y agregarle una acción a realizar con esos correos (las opciones más comunes son las de **Organizar**, moviendo o copiando a carpetas específicas o eliminado el correo, **Marcar mensaje**, con alguna categoría o importancia o Distribución del mismo reenviándolo o redirigiéndolo). También podemos agregar excepciones.

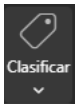
Otra forma de automatización son los **Pasos rápidos**. Los **Pasos rápidos** son atajos personalizables dentro del cliente de escritorio de **Outlook** que permiten a los usuarios aplicar una serie de acciones con un solo clic, automatizando tareas repetitivas de gestión de correo.

Los **Pasos rápidos** combinan múltiples comandos (mover a carpeta, marcar como leído, reenviar, añadir categoría, etc.) en un solo botón en la cinta de opciones de **Outlook**.

Su objetivo es **reducir** la fricción y el tiempo invertido en procesar correos electrónicos que requieren la misma secuencia de pasos de forma recurrente.

Buzones compartidos: Muestra los buzones de grupo o departamento a los que el usuario tiene acceso directamente en la lista de carpetas, como si fueran una cuenta más, facilitando la gestión de correos entrantes de servicios compartidos. También permite agregar las carpetas a las carpetas favoritas que aparecen al principio del panel de Carpetas (a la derecha del programa).

Archivado: Facilita el archivado automático de correos antiguos para mantener el buzón principal más limpio y rápido.



Clasificar: Es un método de organización transversal que permite marcar elementos según su tema, prioridad, o el proyecto al que pertenecen, independientemente de la carpeta donde se encuentren. Así, proporciona una forma visual e instantánea de identificar el contexto o la prioridad de un elemento.

Los correos se clasifican en **Categorías**, cuyas características son:

- Etiquetas de Color: Cada categoría tiene un nombre y está asociada a un color. Outlook permite personalizar tanto el nombre como el color.
- Sincronización: Las categorías están vinculadas a tu cuenta de Exchange/M365, por lo que las categorías que creas en tu PC aparecen también en tu Outlook Web y móvil.
- Asignación Múltiple: Se puede asignar más de una categoría a un mismo elemento. Por ejemplo, un correo puede ser "Proyecto A" y también "Urgente".
- Filtrado y Búsqueda: Puedes ordenar y filtrar tu bandeja de entrada o tu calendario por categoría, lo que te permite ver, por ejemplo, todas las citas y correos relacionados con el "Comité de Dirección".



Marcar: permite establecer un recordatorio o una fecha de vencimiento directamente en un correo electrónico, convirtiendo ese mensaje en un elemento de tarea que requiere una acción futura.

La función "Marcar" es un ciclo de gestión de tareas:

1. Marcar el Correo: Un correo importante llega a la bandeja. El usuario hace clic derecho en el correo o en el icono de la bandera para marcarlo con una fecha.
2. Aparece en Tareas: El correo se mueve automáticamente a la lista de **Tareas de Outlook** (y **Microsoft To Do**).
3. Recordatorio: Si se configuró, **Outlook** mostrará una ventana de recordatorio en la fecha y hora indicadas.

4. Completar la Tarea: Una vez que se ha realizado la acción requerida (por ejemplo, se ha enviado el documento solicitado), el usuario hace clic derecho en la marca (la bandera) y selecciona "**Marcar como completado**".
5. Desaparición: Al marcarlo como completado, la bandera se convierte en una marca de verificación y el elemento desaparece de la lista de tareas pendientes, indicando que el seguimiento ha terminado.



Chincheta: permite fijar elementos importantes a la parte superior de una lista, asegurando que permanezcan visibles y accesibles en todo momento, sin importar la fecha de recepción o el orden de clasificación.



Posponer: permite "ocultar" temporalmente un correo electrónico de la bandeja de entrada y hacer que reaparezca automáticamente como un mensaje "nuevo" en una fecha y hora posteriores que el usuario defina.



Directiva de retención: Define por cuánto tiempo debe conservarse (o eliminarse) la información. Existe una directiva que se aplica por defecto a la carpeta principal que se establece desde la Configuración de Outlook.

Configuración		Directivas de retención
Q Buscar configuraciones - Cuentas - Archivos - General Correo - Calendario - Contactos - Copilot - Diseño - Redactar y responder - Plantillas - Sugerencias inteligentes - Datos adjuntos - Reglas - Formato condicional - Limpiar - Correo electrónico no deseado - Pasos rápidos - Carpets de búsqueda - Personalizar acciones - Administración de mensajes - Reenvío Directivas de retención - S/MIME - Grupos	Las directivas de retención permiten controlar durante cuánto tiempo se guardarán los elementos en el buzón. La siguiente lista muestra las directivas de retención y archivado que tiene disponibles actualmente. Para utilizar directivas adicionales, haga clic en Agregar nueva directiva. + Agregar nueva directiva Borrar en 5 Años Eliminar (recuperar temporalmente) 5 años después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar. Borrar en 1 Año Eliminar (recuperar temporalmente) 1 año después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar. Borrar en 6 Meses Eliminar (recuperar temporalmente) 6 meses después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar. Borrar en 1 Mes Eliminar (recuperar temporalmente) 30 días después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar. Borrar en 1 Semana Eliminar (recuperar temporalmente) 7 días después de recibir el mensaje. Su administrador estableció esta directiva y no se puede quitar.	

Actualitzat a data de 28 de novembre.

Recorda revisar-lo de nou: Sis mesos abans de la primera prova. O, si la prova es convoca amb menys de sis mesos, quan acabe el termini de sol·licituds. Així t'asseguraràs que el temari està al dia.

Bona sort... A PER TOTES!

www.stepv.upv.es/axtotes