

Guía para configurar Outlook 365 para envío de correos firmados y cifrados con certificado de la FNMT.

<u>Objeto</u>

El objeto de la guía es facilitar la configuración del cliente de correo Microsoft Outlook 365, para enviar y recibir correos firmados y cifrados con un certificado digital emitido por la FNMT, en particular el certificado de empleado público, aunque puede hacerse extensivo a otro de similares características.

Consideraciones previas

Antes de nada, se debe estar en posesión de un certificado digital emitido por la FNMT. En la siguiente dirección se explica cómo poder conseguirlo.

https://www.ucm.es/faq/proceso-de-solicitud-y-descarga/

Este certificado debe tener registrada la cuenta de correo electrónico que se quiere utilizar para firmar y cifrar.

Es necesario **no utilizar la aplicación Google Suite Sync** puesto que no se firmarían correctamente los correos.

Instrucciones

Por seguridad, se recomienda que el cliente esté actualizado a la última versión (32 y 64 bits indistintamente). En el momento de realizar este manual, la versión utilizada de Microsoft Outlook 365:

1908 (compilación 11929.20648)



1.- Instalar certificados.

Para instalar el certificado en Outlook 365 procederemos de la siguiente manera:

1. Abriremos la ventana **Opciones de Outlook**, pinchando en Archivo que se encuentra en la parte superior de la ventana de Outlook y seleccionando Opciones en el menú lateral de la ventana que nos muestra:

| Opciones de Outlook | ? > |
|---|--|
| General Correo | Ayude a mantener los documentos seguros y el equipo protegido. |
| Calendario | Seguridad y más información |
| Personas | Para obtener más información sobre la protección de privacidad y seguridad, visite Office.com |
| Centro de confianza | ? |
| Editores de confianza Opciones de privacidad Segunidad del correo electrónico Tratarmiento de datos adjuntos Descarga automática Configuración de macros Acceso mediante programación | Correo electrónico cifrado Correo electrónico cifrado Correo electrónico cifrado Corfigr contenido y datos adjuntos para mensajes salientes Corfigra confirma gigital a los mensajes salientes Corfiguración predictorninada: Corfiguración configuración con |
| 1 | .eer como texto sin formato |
| | Leer todo el correo estándar en texto sin formato Leer todo el correo firmado digitalmente en texto sin formato |
| 8 | Scripts en las carpetas |

- Accederemos a la ventana Centro de Confianza seleccionando, en el menú de la izquierda de la ventana anterior, Centro de Confianza y pincharemos en el botón Configuración de centro de Confianza.
- 3. Procederemos a importar el fichero con el certificado pinchando en importar. Pinchando en examinar, seleccionaremos el fichero que contiene el certificado y rellenamos el campo Contraseña. *El fichero ha de estar en formato p12 o pfx.*

| | | . ~ |
|--|--|--|
| escrita al exportar el ce | el archivo a su PC. Debe utilizar la ertificado a este archivo. | contrasena |
| Importar archivo: | H:\empleado_Publico.p12 | Examinar |
| Contraseña: | ••••• | |
| Nombre del Id. digital: | | |
| | | |
| | | |
|) Exportar el Id. digita | l a un archivo | |
| Exportar el Id. digita Exporte la informaciór una contraseña para a | l a un archivo I del identificador digital a un arcl yudar a proteger esta información | hivo. Escriba n. |
| Exportar el Id. digita Exporte la informaciór una contraseña para a Id. digital: | l a un archivo del identificador digital a un arcl yudar a proteger esta información | hivo. Escriba n. Seleccionar |
| Exportar el Id. digita Exporte la informaciór una contraseña para a Id. digital: Nombre de archivo: | l a un archivo del identificador digital a un arci yudar a proteger esta información | hivo. Escriba n. Seleccionar Examinar |
| Exportar el Id. digita Exporte la informaciór una contraseña para a Id. digital: Nombre de archivo: Contraseña: | l a un archivo del identificador digital a un arcl yudar a proteger esta información | hivo. Escriba n. Seleccionar Examinar |
| D Exportar el Id. digita Exporte la información una contraseña para a Id. digital: Nombre de archivo: Contraseña: Confirmar: | l a un archivo del identificador digital a un arcl yudar a proteger esta información | hivo. Escriba n. Seleccionar Examinar |
| Exportar el Id. digita Exporta el Id. digita Exporte la informaciór una contraseña para a Id. digital: Nombre de archivo: Contraseña: Confirmar: Compatible con Mi | l a un archivo del identificador digital a un arcl yudar a proteger esta información | hivo. Escriba Seleccionar Examinar bajo de seguridad) |



4. Nos aparecerá la ventana **Importación de una nueva clave privada de intercambio** en la que podremos seleccionar el nivel de seguridad para la clave. *Es conveniente seleccionar un nivel alto, sobre todo en caso de equipos compartidos, para que nos solicite la contraseña cuando Outlook utilice el certificado.*

| Importación de una nueva clave privada de intercambio 🛛 🗙 🗙 | Elegir un nivel de seguridad | × |
|--|--|---|
| Una aplicación está creando un elemento protegido. Clave privada de CryptoAF Nivel de seguridad: medio | Elija un nivel de seguridad apropiado para este elemento Alto Solicitar mi permiso con una contraseña cuando la información vaya a utilizarse. Medio Solicitar mi permiso cuando la información vaya a utilizarse. | |
| Aceptar Cancelar Detalles | Atrás Siguiente > Cancelar | |

5. En caso de haber seleccionado nivel de seguridad Alto nos solicitará una contraseña que nos pedirá cada vez que usemos el certificado.

| Crear una contraseña | | × |
|----------------------|---|---|
| | Crear una contraseña para proteger este elemento. | |
| | Crear una contraseña para este elemento. Contraseña para: Clave privada de CryptoA | |
| | Contraseña: Confirmar: | |
| | < Atrás Finalizar Cancelar | |

6. Pinchamos en Finalizar y tendríamos instalado el certificado.



2.- Configurar el firmado y/o Cifrado de correos electrónicos.

Una vez instalado el certificado hay que configurar como lo utilizará Outlook a la hora de firmar o cifrar correos, lo suyo es que firme todos los correos salientes para certificar que somos nosotros los que los enviamos y cifrarlos solo en el caso de enviar información confidencial. Para el caso del cifrado necesitaremos la clave pública del destinatario, pero eso lo veremos más adelante.

1. Accedemos a Seguridad del correo electrónico en la pantalla de Centro de confianza.

| Editores de confianza Opciones de privacidad Opciones de privacidad Correo electrónico Cifrar contenido y datos adjuntos para mensajes salientes Agregar firma digital a los mensajes salientes Enviar mensaje firmado de texto no cifrado al enviar mensajes firmados Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados Configuración predeterminada: Configuración Id. digitales (Certificados) Id. o certificados digitales son documentos que permiten demostrar la identidad del usuario en las transacciones electrónicas Importar o exportar Leer como texto sin formato Leer todo el correo firmado digitalmente en tegto sin formato Scripts en las carpetas | Centro de confianza | ? | × |
|---|---|---|----------|
| Opciones de privacidad Cifrgr contenido y datos adjuntos para mensajes salientes Larviar mensaje salientes Lerviar mensaje firmado de texto no cifrado al enviar mensajes firmados Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados Configuración de macros Acceso mediante programación Id. digitales (Certificados) Los Id. o certificados digitales son documentos que permiten demostrar la identidad del usuario en las transacciones electrónicas. Importar o exportar Leer como texto sin formato Leer todo el correo estándar en texto sin formato Leer todo el correo firmado digitalmente en tegto sin formato Scripts en las carpetas | Editores de confianza | Correo electrónico cifrado | ^ |
| Acceso mediante programación Id. digitales (Certificados) Importar o exportar Los Id. o certificados digitales son documentos que permiten demostrar la identidad del usuario en las transacciones electrónicas. Importar o exportar Importar o exportar Leer como texto sin formato Leer todo el correo estándar en texto sin formato Leer todo el correo firmado digitalmente en texto sin formato Scripts en las carpetas | Opciones de privacidad Seguridad del correo electrónico Tratamiento de datos adjuntos Descarga automática Configuración de macros | Configuración Configuración Configuración Configuración | |
| Leer como texto sin formato Leer todo el correo estándar en texto sin formato Leer todo el correo firmado digitalmente en texto sin formato Scripts en las carpetas | Acceso mediante programacion | Id. digitales (Certificados) Image: solution of the standard sta | |
| Scripts en las carpetas | | Leer como texto sin formato Leer todo el correo estándar en texto sin formato Leer todo el correo firmado digitalmente en tegto sin formato | |
| | | Scripts en las carpetas | - |

2. Pinchamos en el botón Configuración... y rellenamos el campo Nombre de configuración de seguridad. Marcamos las casillas de Configuración Predeterminada para este formato de mensaje cifrado y Configuración predeterminada para todos los mensajes cifrados. Elegimos el certificado de firma y el certificado de cifrado pinchando en botón Elegir... correspondiente y pinchamos en Aceptar. En algoritmo tipo hash se selecciona SHA256. Ha de quedar todo como en la imagen siguiente.

| Cambiar la configuración d | le seguridad | \times |
|---|--|----------|
| Preferencias de configuració Nombre de configuraciór | n de seguridad n de seguridad: | |
| Mi configuración S/MIM | E () | ~ |
| Formato de cifrado: | S/MIME | |
| 🗹 Configuración predet | erminada para este formato de mensaje cifrado erminada para todos los mensajes cifrados | |
| Etiquetas de segurida | ad Nueva Eliminar | |
| Certificados y algoritmos Certificado de firma: | Elegir. | |
| Algoritmo de tipo hash: | SHA256 ~ | |
| Certificado de cifrado: | Elegir. | |
| Algoritmo de cifrado: | AES (256-bit) \checkmark | |
| 🗹 Enviar estos certificado | os con mensajes firmados | |
| | Aceptar Cancela | ar |



3. En seguridad de correo electrónico marcamos las casillas Agregar firma digital a los mensajes salientes y Enviar mensajes de texto no cifrados al enviar mensajes firmados.

| Centro de confianza | ? | \times |
|---|--|----------|
| Editores de confianza Opciones de privacidad | Correo electrónico cifrado | 1 |
| Seguridad del correo electrónico | Cifrge contenido y datos adjuntos para mensajes salientes Acreose firma dicital a los mensaies salientes | |
| Tratamiento de datos adjuntos | Enviar mensaje firmado de testo no cifrado al enviar mensajes firmados | |
| Descarga automática | Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados | |
| Configuración de macros | Configuración predeterminada: Certificado de Empleado Público 🔹 Configuración | |
| Acceso mediante programación | Id. digitales (Certificados) | |
| | Los Id. o certificados digitales son documentos que permiten demostrar la identidad del usuario en las transacciones electrónicas. [Importar o exportar] | |
| | Leer como texto sin formato | |
| | Lger todo el correo estándar en testo sin formato | |
| | | |

En caso de querer que nos confirme que el correo enviado no ha sido modificado cuando lo reciban marcaríamos la opción Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados en este caso recibiríamos un correo por cada correo enviado indicándonos si el correo enviado ha sufrido modificaciones durante el envío.



3.- Obtención de la clave pública del destinatario.

Como hemos dicho anteriormente se debe de tener la clave pública del destinatario del correo para poder tener una comunicación cifrada con él. La manera más fácil de obtener dicha clave es remitirnos a algún correo que nos haya mandado firmado y recuperar, desde el, la clave pública.



Abrimos el mensaje firmado y en la parte de la derecha tenemos un icono que muestra una medalla, eso indica que el correo está firmado.

En caso de que no tengamos el remitente entre nuestros contactos al añadirlo recuperará todos los datos del correo, incluso la clave pública. Pare ello, con el correo abierto, al posicionarnos sobre el remitente del correo nos desplegara una ventana flotante, pinchamos en los 3 puntos de esta ventana y nos da la opción de agregar el correo a nuestros contactos.



En la ventana que nos abre con los datos del contacto tenemos que pinchar en Certificados para asegurarnos que va a incluir el certificado y pinchamos en Guardar y cerrar.

| 🖽 9 Ö A 4 8 • • | - Contacto | | ■ - □ × |
|--|---|--|-----------------------------------|
| Archivo Contacto Insertar Formato de texto Revisar Guardar Eliminar Guardar y Reenviar OneNote nuevo Acciones Outlook utilizará uno de estos certificados para mandar correo dirádo a este cont dudo de terre un certificado correo fimado digitalmente de este cont | yuda Q ¿Qué desea hacer? Correo Reunión Más comunicar Nombres to to to to to to to to to to | Tarjeta de Imagen resentación Opdones Etiquetas Zo | Por Iniciar entradas de lipitz |
| Certificados (identificadores digitales) - DNII (Predeterminada) | | | Propiedades |
| | | | Importar |
| | | | Exportar |
| | | | Quitar |
| | | | |



En caso de querer añadir el certificado a un contacto que ya tenemos habría que exportar la clave pública a un fichero para después importarla al contacto.

En este caso accederíamos al correo y pinchamos en la medalla que indica que el correo está firmado.



Esto nos abrirá una ventana donde podremos comprobar que la firma es válida.



En esta ventana pincharemos en Detalles para abrir la ventana de las propiedades de seguridad del mensaje.

| Propiedades de seguridad del mensaje | Х |
|---|-------|
| Asunto: Prueba certificados | |
| Los mensajes pueden contener niveles de firma digital y cifrado. Cada nivel de firma dis puede contener varias firmas. | gital |
| Niveles de seguridad | |
| Seleccione uno de los niveles siguientes para ver su descripción. | |
| Asunto: Prueba certificados | |
| ✓ Nivel de firmas digitales | |
| Firmante: @UCM.ES | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Descripción: | |
| Correcto: Firmado por OUCM.ES utilizando RSA/SHA1 a la 11:11:22 19/03/20 | 20. |
| | |
| | |
| Haga dic en gualquiera de los siguientes botones nara ver más información acerca del | nivel |
| seleccionado o realizar cambios en éste: | IIVEI |
| Modificar confianza Ver detalles Confiar en entidad emisora de certifica | dos |
| | |

Dentro de los niveles de seguridad que nos muestra pincharemos en Firmante y luego en ver detalles donde accederemos a los detalles de la firma.



| Información de l | a firma |
|----------------------------|---------------------------|
| Formato del mensaje: | S/MIME |
| Firmado por: | @UCM.ES |
| Estado de la firma: | Correcto |
| Fecha de firma: | 11:11:22 19/03/2020 |
| Algoritmo de codificación: | SHA1 |
| Algoritmo de firma: | RSA (2048-bits) |
| Información del | certificado |
| Emitido por: | AC Administración Pública |
| Estado del certificado: | Correcto |

A continuación, pincharemos en Ver certificado que nos llevará a los detalles del certificado.

| 💼 Ver c | ertificado | | > |
|---------|--|---|----|
| General | Detalles Ruta d | e certificación Trust | |
| | Información | del certificado | |
| Est | e certif. está de • Protege los men | stinado a los siguientes propósitos: sajes de correo electrónico | |
| * Pa | ra ver detalles, cor Emitido para: | suíte la declaración de la entidad de cer | |
| | Emitido por: | AC Administración Pública | |
| | Válido desde | 30/01/2020 hasta 30/01/2022 | |
| | | Declaración del emisor | |
| | | | |
| | | Acept | ar |

Iremos a la pestaña Detalles y en ella le daremos a Copiar en archivo.



| | tificación Trust | |
|--------------------------|-------------------------------------|---|
| Mostrar: <todos></todos> | ~ | |
| Campo | Valor ^ |] |
| Versión | V3 | |
| Número de serie | | |
| Algoritmo de firma | sha256RSA | |
| Algoritmo hash de firma | sha256 | |
| Emisor | AU Administración Pública, Q28 | |
| Váldo basta | dominan 30 de enero de 2020 1 | |
| Suieto | V | |
| | | |
| E | ditar propiedades Copiar en archivo |] |

Nos lanzará un asistente en el que tendremos que indicarle el formato en el que queremos el certificado, debería ser DER binario codificado x.509 (.CER), y el nombre de archivo.

| ÷ , | 🚰 Asistente para exportar certificados | × | ÷ | 🚰 Asistente para exportar certificados | × | ÷ | 🐺 Asistente para exportar cettificados | × |
|-----|---|-----|---|--|---|---|--|------|
| | Este es el Asistente para exportar certificados | | | Formato de archino de exportación Los certificados pueden ser exportados en diversos formatos de archino. | | | Archèro que se sa a exportar Específique el nombre del archivo que desea exportar | |
| | Eine auchreite is unde a sociar confilicados, latas de entificados de confineta y latas de renocación de confilicados un abasión de confilicados a su diors. Un conflicado, par lamenta una entidad de militación e a un diorse al derestrator y contener ariomando que ou sa para porteger datas o para estabalero guarden los confilicados. Un almando en que su para porteger datas o para estabalero guarden los confilicados. | | | Selectione el formato que deces usar: BOR banario codificado 15.009 (-CRN) Or.5.007 codificado tene 64 (-CRI) Or Eschador de atrastas de derándo de mensajes: certificados PICS #7 (-P7D) Deda todas los certificados en la ruta de certificados (si se poste) Ortenados de aformados de presenta PICS #12 (-P7D) | | | Rober de aches: C(parr) Countrijerthadoljuronano.ce | |
| | | | | hdue todos los centificados en la nuta de centificación (is es posible) Eliminar la dave prinda si la exportación es correcta oportar todos las progradades entendáss Haladar privacidad de centificado Alsacén de centificados en serie de Microsoft (.531) | | | | |
| | Siguiente Cancela | r - | | Siguiente Cancela | 1 | | Siguiente Can | elar |

Una vez tenemos el fichero con la clave pública accedemos al contacto, pincharemos en certificados y luego en importar. Nos solicitará el fichero que hemos generado y añadirá la clave pública al contacto. No se os olvide darle a guardar y cerrar.

| 8 9 0 ↑ ↓ 8 • • | - Contacto | | ■ – □ × |
|--|---|--|--------------------------------|
| Archivo Contacto Insertar Formato de texto Revisar Ayu | da 🛛 🖞 ¿Qué desea hacer? | | |
| Guardar Eliminar Guardar y Reenviar OneNote y cerrar nuevo | Correo Reunión Más electrónico | eta de Imagen intación Continuer | Iniciar entradas de lápiz |
| Outlook utilizará uno de estos certificados para mandar correo cifrado a este contacto | Comunicar i Nombres i | opciones i ecquecas i 200m | r i Eritrada de lapiz i 🕆 |
| Puede obtener un certificado recibiendo correo firmado digitalmente de este contacto | o importando un archivo de certificado para el mismo. | | |
| Certificados (identificadores digitales) | | | |
| - DNI (Predeterminada) | | | Propiedades |
| | | | Establecer como predeterminado |
| | | | Importar |
| | | | Exportar |
| | | | Quitar |
| | | | |
| | | | |
| 1 | | 1 | 1 |

En caso de no tener ningún correo firmado del destinatario tenemos dos opciones. Les solicitamos un fichero con su clave pública o les solicitamos un correo firmado para poder extraer la clave pública para poder seguir los pasos anteriores.



4.- Firmado y/o cifrado de correos.

Una vez que tenemos configurado nuestro certificado y tenemos las claves públicas de los destinatarios en nuestros contactos ya podemos cifrar nuestras comunicaciones de manera que nadie mas que el destinatario pueda ver nuestros correos.

Para ello cuando estemos redactando un correo solo tenemos que pinchar en Opciones y luego en Firmar y/o en Cifrar.

| | ୨୯↑ | 0.8 | * ÷ | | Sin título - | Mensaje (H | TML) | | | | | æ | - | | × |
|------------------|---------------------------------------|----------------------|----------------|------------------|-----------------------------|------------|--|-------------------------|-------------------|---------------------|---------------------|-------------------|---------------------|-------------------------|---|
| Archivo | Mensaje | Inserta | r Opciones | Formato de texto | Revisar | Ayuda | Adobe PDF | Q | ¿Qué de | sea hacer | ? | | | | |
| Aa Temas | Colores + A Fuentes + Efectos + | Color de página * | CCO De | Permise & Firmar | Utilizar boton de voto * | Solici | tar una confirmac tar una confirmac | ción de e ción de le | entrega ectura | Guardar e enviad | elemento lo en * | Retrass entreg | / ir D a resp | k irigir uestas a | |
| | Temas | | Mostrar campos | Permiso | | Segu | uimiento | | 5 | | Más o | pciones | | Fa | ^ |
| \triangleright | f | Para | Ľ | | | | | | | | | | | | |
| Envia | r | сс | | | | | | | | | | | | | |
| | A | sunto | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |



5.- Comprobación de la firma y cifrado de los correos recibidos.

Si el correo está firmado, en la bandeja de entrada nos muestra una medalla y la palabra Firmado debajo del destinatario del correo. En la vista previa nos aparece una línea debajo del destinatario en la que nos indica quien lo ha firmado y una medalla en la parte derecha de dicha línea. En caso de que la firma no sea válida o no pueda comprobarla aparecerá un símbolo de alerta 1.

| Archivo Indo Enviar y recibir Carpeta Vista Ayuda Adobe POF V (Qué desea hacer? Nuevo correro Nuevos electrónicos elementos - Nuevo correro Nuevos electrónicos elementos - Nuevos electrónicos - Parate de corres firmado - Correro firmado - Pueba de correo firmado - Correro firmado - Pueba de correo firmado - Correro firmado - Pueba de correo firmado - - - - - - - - - - - - - | 0 % % · · | | | cados - Oucn | | | | |
|--|---|---------------------|--|---|---|--|---|---------|
| ✓Favoritos Bandeja de entrada Enviados Papelera Surdeja de entrada Enviados Todo No leidos Por Fecha ∨ 1 > Varon Correo firmado Surdeja de entrada > [Gravita] Avicos Surdeja de salida Bandeja de salida Surdeja de salida Surdeja de salida | Archivo Inicio Envia Nuevo correo Nuevos electrónico elementos * | r y recibir Carpeta | Vista Ayuda ← Responder ← Responder a todo: → Reenviar Responder | Adobe PDF Adobe PDF Pasos rápidos - Pasos r. fis | 2Qué desea hacer? | Enviar y recibir todas las carpetas Enviar o recibir | Guardar archive adjuntos Google Drive | |
| | Favoritos Bandaja de entrada Envisãos Papelera Guanti de entrada Simali Autos Bandaja de salida Borrador Consentemente Consentemente Q ^Q Consentemente | Correco Prueba | Certificados P No leidos Por Eucres Irmado E correo firmado E correo firmado E correo firmado E correo firmado | Carpeta actual • Fecha v ↑ 18:55 | Correo firmado ©Curnes Pan Destinatario Cifrad Firmido por ØUCMES Prueba de correo firmado | (5) | ≪5 → 10: [| 55 9 |

En el caso de los correos cifrados y firmados los podemos ver en la vendeja de entrada por que aparecen marcados con un candado y en la vista previa aparece un candado y una medalla.

| 0 9 8 · · | Certificados - Øucm.es - Outlook | | - 0 | × |
|--|--|--|--|-------------------|
| Archivo Inicio Emviar y recibir Nuevo correo Nuevos electrónico elementos + Nuevo Ellir | Carpeta Vista Ayuda Adobe PDF Q (Qué desea hacer? T - Carpeta Vista Ayuda Adobe PDF Q (Qué desea hacer? S Responder Etodos mar Archivo Paros Responder Stodos Paros Responder Stodos Paros Responder Por Paros r. 15 Comparison Por | Enviar y recibir todas las carpetas Enviar o recibir | Guardar archi adjuntos Google Driv | vc+ |
| Cavoritos 1 Envisidos 1 Envisidos 1 Papelera | Burckr en Certificados Curpets actual Todo No leidos Per fecha < 1 | ptado 🤤 |) ≪) → fi | ••• 10:50 9 |
| Filtro aplicado | Conettado | | | 100 % |

Si se ha cifrado aparece un candado en la bandeja de entrada.





En caso de recibir un correo cifrado de un destinatario del que no tengamos la clave pública o esté cifrado con una clave privada que no se corresponda con la clave pública que tenemos para ese remitente no seriamos capaces de ver el contenido del correo.