

Manual de uso de correo seguro en Microsoft Outlook

| Fecha: 22/03/2006 | Versión: 1.4 |
|-------------------|-------------------|
| Estado: APROBADO | Nº de páginas: 10 |



Secretaria Autonòmica de Telecomunicacions i Societat de la Informació

Conselleria d'Infraestructures i Transport



Tabla de Contenido

| 1. | CO | ONFIGURACIÓN DE MICROSOFT OUTLOOK | 3 |
|----|------------|--|--------|
| | 1.1. | REQUISITOS PREVIOS | 3 |
| 2. | 1.2. EN | IVÍO DE MENSAJES FIRMADOS DIGITALMENTE CON MICROSOFT OUTLOOK | 3 8 |
| 3. | OB | TENCIÓN DE LA CLAVE PÚBLICA DE OTROS USUARIOS | 9 |
| 4. | EN | VÍO DE MENSAJES CIFRADOS DIGITALMENTE CON MICROSOFT OUTLOOK | 10 |

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 2 de 10 |



1. Configuración de Microsoft Outlook

1.1. Requisitos previos

Esta guía asume que el usuario dispone de:

- Una cuenta de correo configurada en Microsoft Outlook para el envío y recepción de correo electrónico desde un servidor de correo.
- Los certificados digitales registrados en el navegador Internet Explorer 5.5 o superior, tal y como se expone en el Manual de instalación de la tarjeta criptográfica y el lector USB y en el Manual de instalación de los certificados digitales en fichero.

1.2. Configuración de seguridad

Una vez iniciado Microsoft Outlook, en el menú **Herramientas**, seleccionar **Opciones**. Se abre el cuadro de diálogo que se muestra a continuación:

| Preferencia | as Entrega de correo 🛛 Forma | ito de correo Ortogra | afía Seguridad Otros |
|-------------------|--|---|---|
| Formato (| del mensaje | | |
| | Elija un formato para el correo saliente y cambie la configuración avanzada. | | |
| | Enviar en este formato: | Texto enriquecido d | e Microsoft Outlook 📃 💌 |
| | 🔲 Usar Microsoft Word para | modificar mensajes de | correo electrónico |
| | | Configuración | Opciones internacionales |
| Diseño de | e fondo y fuentes | | |
| A ³⁸ C | Utilice el diseño de fondo para cambiar la fuente y el estilo predeterminados, cambiar los colores y agregar fondos a los mensajes. | | |
| | Litilizar este diseño de fondo | | |
| | de forma predeterminada: | <ninguno></ninguno> | v |
| | de forma predeterminada: | <ninguno></ninguno> | Selector de diseño de fondo |
| Firma — | de forma predeterminada: | <ninguno></ninguno> | Selector de diseño de fondo |
| Firma — | de forma predeterminada: Incluya automáticamente su fi (vCard) a los mensajes salient | <pre>{Ninguno> Fuentes irma o adjunte una tar; es.</pre> | Selector de diseño de fondo |
| Firma — | Incluya automáticamente su fri (vCard) a los mensajes salient Utilizar esta firma de forma predeterminada: | <ninguno> Fuentes ima o adjunte una tar; es.</ninguno> | Selector de diseño de fondo jeta de presentación electrónica |
| Firma — | de forma predeterminada: Incluya automáticamente su fi (vCard) a los mensajes salain Utilizar esta firma de forma predeterminada: M. No utilizar al responder o r | <ninguno> Fuentes irma o adjunte una targes. (Ninguno> cenviar</ninguno> | Selector de diseño de fondo jeta de presentación electrónica Selector de firmas |

Sitúese en la pestaña Seguridad, pulsar el botón Cambiar configuración, campo Preferencias de configuración de seguridad y hacer clic en el botón Nueva.

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 3 de 10 |



| Cambiar la configuración | de seguridad 🛛 💽 🗙 |
|--|---|
| Preferencias de configuraci Nombre de configuración de seguridad: Formato de mensaje seguro: | in de seguridad UNITE |
| 🔲 Configuración predete | rminada para este Formato de mensaje seguro |
| 🔲 Configuración pre | determinada para todos los mensajes seguros |
| | Nueva Eliminar Contraseña |
| Certificados y algoritmos | |
| Certificado de firma: | Elegir |
| Algoritmo de tipo hash: | Y |
| Certificado de cifrado: | Elegir |
| Algoritmo de cifrado: | _ |
| 🔽 Enviar estos certificad | os con mensajes firmados |
| | Aceptar Cancelar |

- Introducir un nombre descriptivo en el campo Nombre de configuración de seguridad, por ejemplo CERTICADOS DIGITALES.
- En el campo Formato de mensaje seguro indicar S/MIME.
- Marcar las opciones Configuración predeterminada para este Formato de mensaje seguro y Configuración predeterminada para todos los mensajes seguros para asegurar que esta configuración se va a aplicar a todos los mensajes de correo.

En el campo **Certificados y Algoritmos**, indica el certificado que quiere asociar a la cuenta de correo para firmar y cifrar.

En el caso de **Certificado de firma**, pulse **Elegir** y aparece un cuadro de diálogo con los certificados disponibles en el repositorio. Éstos serán los certificados que se hayan registrado previamente, como indica el punto 2.1 Requisitos previos. En el caso de haber más de un certificado, debe elegir el **Certificado de firma**. Para comprobar que lo hacemos adecuadamente, una vez seleccionado, pulsar el botón **Ver certificado** para ver sus propiedades.

| 5 | eleccionar | certificado | | | <u>? x</u> |
|---|--------------|-------------------|----------------|-----------|-----------------|
| | Seleccione e | l certificado que | e quiere usar, | | |
| | | | | | |
| | Enviad | Emitido por | Propósitos | Nombre de | Fecha de c |
| | ESPE | CAGVA | Autenticaci | Ninguno | 15/06/2006 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | [| Aceptar | Cancelar | Ver certificado |

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 4 de 10 |



Compruebe que el certificado que elige es el de firma y el asociado a la cuenta de correo correcta. Verifique en la pestaña **Detalles**, campo **uso de claves**: firma digital y que en el campo **Nombre alternativo del sujeto** está indicada su cuenta de correo.

| General Detailes Ruta de certificación Confianza Mostrar: <todos> Campo Valor Bases del certificado [1]Directiva de certificado:Identi Bases del certificado [1]Directiva de certificado:Identi Identificador de la clave de a [1]Acceso a información de aut Identificador de clave de e Id. de clave=7 Identificador de clave de asu F480 D937 1558 FEEB D01F Valor Sha1 Algoritmo de identificación sha1 Huella digital 4F85 4A3D 4E69 3088 AA8F 0 Firma digital(80) </todos> | ertificado 🤗 🔀 | | | | | |
|--|--|------------------------------------|-------|--|--|--|
| Mostrar: <todos> Campo Valor Bases del certificado [1]Directiva de certificado:ldenti Acceso a la información de a [1]Acceso a información de aut Identificador de la clave de e Id. de clave=7 Identificador de clave de e Id. de clave=7 Identificador de clave de e F480 D937 1558 FEEB D01F Valor Frima digita(80) Algoritmo de identificación sha1 Huella digital 4F85 4A3D 4E69 3088 AA8F 0 Firma digita(80) Firma digita(80) </todos> | General Detalles Buta de certificación Confianza | | | | | |
| Mostrar: <todos> Campo Valor Bases del certificado (1)Directiva de certificado:Identi Acceso a la información de a (1)Acceso a información de aut (2)Acceso a información de aut (2)Acceso a información de aut (2)Acceso a información de aut (3)Acceso a información de aut (4)Acceso autoritación de aut (4)Boritación de identificación sha1 (2)Algoritación de identificación sha1 (3)Algoritación de identificación sha1 (4)Boritación de identificación sha1 (4)Boritación de identificación sha1 (3)Algoritación de identificación sha1 (4)Boritación de identificación sha1 (4)Boritación de identificación sha1 (4)Boritación de identif</todos> | | | | | | |
| Campo Valor Bases del certificado [1]Directiva de certificado:Identi Acceso a la información de a [1]Acceso a información de aut Identificador de la clave de e Id. de clave=7 Identificador de clave de e.a F480 D937 1558 FEEB D01F Uso de la clave Firma digita(80) Algoritmo de identificación sha1 Huella digital 4F85 4A9D 4E69 3088 AA8F 0 Firma digita(80) | Mostrar: <todos></todos> | - | | | | |
| Campo Valor S Bases del cettificado [1]Directiva de cettificado:Identi Acceso a la información de a [1]Acceso a información de aut Identificador de la clave de e Id. de clave=7 Identificador de clave de e.a F480 D937 1558 FEEB D01F Uso de la clave Firma digita(80) I Algoritmo de identificación sha1 Huella digital 4F85 4A3D 4E69 3088 AA8F 0 Image: Firma digita(80) Image: Firma digita(80) | | | | | | |
| Image: Bases del certificado [1]Directiva de certificado:Identi Image: Acceso a la información de a.u. [1]Acceso a información de aut Identificador de la clave de e Id. de clave=7 Identificador de la clave de asu F480 D937 1558 FEEB D01F Image: Algoritmo de identificación sha1 Image: Huella digital 4F85 4ASD 4E69 3088 AA8F 0 Image: Firma digital(80) Image: Firma digital(80) | Campo | Valor | | | | |
| Acceso a la información de a [1]Acceso a información de aut I Identificador de la clave de e Id. de clave=7 I Identificador de la clave de esu F480 D937 1558 FEEB D01F Firma digital(80) Sha1 Argoritmo de identificación sha1 Huella digital 4F85 4A9D 4E69 3088 AA8F 0 Firma digital(80) Imaginal digital Firma digital(80) Imaginal digital Firma digital(80) Imaginal digital Firma digital(80) Imaginal digital | 🔂 Bases del certificado | [1]Directiva de certificado:Identi | | | | |
| Identificador de la clave de e Id. de clave=7 Identificador de clave de esu F480 D937 1558 FEEB D01F Uso de la clave Firma digital(80) Kalgoritar de identificación sha1 Huella digital 4F85 4A9D 4E69 3088 AA8F 0 Firma digital(80) ✓ Firma digital(80) ✓ Madifica exercicidado ✓ | Acceso a la información de a | [1]Acceso a información de aut | | | | |
| Identificador de clave de asu Firma digital(80) Uso de la clave Firma digital(80) Algoritmo de identificación sha1 Huella digital 4F85 4A3D 4E69 3088 AA8F 0 Firma digital(80) v | Identificador de la clave de e | ld. de clave=7 | | | | |
| Uso de la clave Firma digita(80) Algoritmo de identificación sha1 Huella digital 4F85 4A3D 4E69 3088 AA8F 0 | Identificador de clave de asu | F4B0 D937 155B FEEB D01F | | | | |
| Algoritmo de identificación sha1 Huella digital 4F85 4A9D 4E69 3088 AA8F 0 Firma digital(80) | Uso de la clave | Firma digital(80) | | | | |
| Firma digital(80) | Algoritmo de identificación | shall | | | | |
| Firma digital(80) | Huella digital | 4F85 4A9D 4E69 3088 AA8F 0 | | | | |
| Firma digital(80) | 1 | | | | | |
| | Eirma digital(80) | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Madifica contratados de Contra os el contrios | | | | | | |
| Madifican environmentation Continue of analytica | | 1 | | | | |
| Mounical propiedades Copiar en el archivo | Modificar propi | iedades Copiar en el archivo | | | | |
| | | | | | | |
| Aceptar | | Ac | eptar | | | |

| ertificado | | ? |
|---|--|-------|
| General Detalles Ruta de certifica | ción Confianza | |
| Mostrar: <todos></todos> | × | |
| Campo | Valor |] |
| 🔁 Puntos de distribución CRL | [1]Punto de distribución CRL: N | |
| Nombre alternativo del sujeto | Nombre RFC822= | |
| Bases del certificado | [1]Directiva de certificado:Identi | |
| Acceso a la información de a | [1]Acceso a información de aut | 1 |
| Les identificador de clave de e | 10. 06 Clave=/ E480 D937 1558 EEE8 D01E | |
| I Iso de la clave | Firma digital(80) | J |
| Algoritmo de identificación | sha1 | i i |
| | | |
| Nombre RFC822= Dirección del directorio: | | |
| CN= 01D 0 9 2342 19200300 100 1 1 | =1 | |
| | | |
| | | |
| | | |
| 1 | | |
| Modificar propi | edades Copiar en el archivo | |
| | Ac | eptar |

Pulsar **Aceptar** para confirmar la elección del certificado. Elija SHA1 como **algoritmo de tipo hash** de Firma.

Repetiremos el proceso para el **Certificado de cifrado.** Algoritmo de cifrado 3DES. Marcar la opción **Enviar estos certificados con mensajes firmados** (para permitir que nos envíen mensajes cifrados).

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 5 de 10 |

Pulsar Aceptar para confirmar la elección y Cerrar a continuación.

Autoritat de Certificació

de la Comunitat Valenciana

Para poder firmar y cifrar todos los correos electrónicos sin necesidad de hacerlos cada vez que escribe uno de ellos puede hacerlo de la siguiente manera:

Sitúese en el menú Herramientas, Opciones, pestaña Seguridad. En el campo correo electrónico seguro. Marque la opción Cifrar contenido y datos adjuntos para mensajes salientes si quiere que los correos se envíen siempre cifrados; marque Agregar firma digital a los mensajes salientes si quiere firmar todos los correos que envíe.



No obstante, si quiere firmar o cifrar los mensajes individualmente añadirá los botones



correspondientes a la barra de herramientas.

Para ello, siga las siguientes instrucciones:

- Abra un nuevo correo.
- En el menú Herramientas, ir a Personalizar.
- Hacer clic en la pestaña Comando como aparece en la siguiente figura.

| ersonalizar | | ? |
|---|---|---------------------|
| <u>B</u> arras de herramientas | Comandos Opciones | |
| C <u>a</u> tegorías: | Coma <u>n</u> dos: | |
| Archivo Edición Ver Insertar Formato Herramientas Acciones ? Macros Barra de menús | Nuevo Mensaje Mensaje de f ⊂ Cita @ ² Convocatoria Convocatoria | fax a de reunión |
| Comando seleccionado: Descripi | ón Modificar selecc | ión ▼ |
| 2 | | Cerrar |

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 6 de 10 |



- Elegir la categoría Estándar y los comandos Cifrar el contenido del mensaje y de los datos adjuntos, pinche y arrastre el botón hasta la barra de herramientas.
- Repita la operación anterior con el comando agregar firma digital.
- Pulsar Cerrar para seguir con la configuración.

Una vez añadidos los botones podrá decidir si quiere firmar y cifrar de forma individual los mensajes salientes.

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 7 de 10 |



2. Envío de mensajes firmados digitalmente con Microsoft Outlook

Para crear un mensaje de correo en blanco pulsamos el botón **Nuevo** o en el menú **Archivo** seleccionamos **Nuevo**, **Mensaje**.

| 🔀 Sin título - Mensaj | je (Texto enriqueo | ido) | |
|-----------------------|--------------------|----------------------------|----------|
| Archivo Edición Ver | Insertar Eormato | Herramientas Acciones ? | |
| Enviar 📙 🎒 | X 🖻 🖬 🛃 | 🕕 😰 🕵 🚦 🖡 🔻 🚼 Opciones 🧖 🗸 | |
| Arial | • 10 • <u>A</u> | N K S 国 国 国 福 俸 福 🍇 🎦 🗸 | |
| Para coporte@p | ki gua ec | | |
| raja | IN. QVB. CS | | |
| | | | |
| Agunto: | | | |
| | | | <u>_</u> |
| Hola, | | | |
| · · | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | - |

Los pasos a seguir para enviar el mensaje firmado son:

- Escribir la dirección de correo del destinatario del mensaje en el campo **Para**. Pulsando sobre este botón se abre la **Libreta de Direcciones** y puede buscar y seleccionar el contacto.
- Completar los campos Asunto y el cuerpo del mensaje.
- En caso que haya añadido los botones anteriormente, pulse el botón firmar. De lo contrario, en la barra de Herramientas pulsar el botón Opciones. Aparecerá el siguiente cuadro de diálogo:

| Opciones de mensaje | | <u>?×</u> |
|--|-----------------------|---|
| Configuración de mensaje Importancia: Normal V Carácter: Normal V | Seguridad | nsaje y de los datos adjuntos nsaje saliente |
| Enviar las respuestas a: Guardar el mensaje enviado No entregar antes del: Caduca después del: Enviar el mensaje usando: | en: Sent Items | Seleccionar nombres |
| Opciones de seguimiento | ura para este mensaje | |
| Contactos Categorías | | Cerrar |

- Pulsar **Cerrar** para confirmar las Opciones de mensaje.
- Pulsar el botón Enviar para enviar el mensaje.

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 8 de 10 |



3. Obtención de la clave pública de otros usuarios

Para enviar correo cifrado a un usuario es necesario disponer de la clave pública del mismo. A continuación describimos las dos formas posibles de la clave pública de un usuario.

La primera opción consiste en obtener la clave pública del usuario a través de un correo firmado por él. Para ello:

- Solicitar al usuario que nos envíe un correo firmado digitalmente (los correos firmados adjuntan el identificador digital del usuario).
- Abrir el correo firmado y hacer clic con el botón derecho del ratón en el campo De y seleccionar Agregar a Contactos en el menú.
- Rellenar los datos del contacto y pulsar **Guardar y cerrar**. Si ya existe una entrada para esta persona en la lista de contactos, seleccione **Actualizar el contacto existente con la nueva información** en la ventana que aparece.

| Q | ontact | tos duplicados 🛛 🗙 |
|---|--------|--|
| 1 | R | El nombre o dirección de correo electrónico de este contacto ya existe en la siguiente carpeta: |
| | | Contactos |
| ł | | ¿Qué desea hacer? |
| | | C Agregar esta información como un nuevo contacto de todas formas |
| | | |
| | | Nota: se incluirá una copia de seguridad del contacto existente en la carpeta Elementos eliminados. |
| | | Abrir el contacto existente Aceptar Cancelar |

El ID. Digital se almacena ahora con la entrada de contacto correspondiente a este destinatario y ya puede enviar mensajes de correo electrónico cifrados a esta persona. Para ver los certificados de un contacto debe ir a **Herramientas, Libreta de** direcciones, hacer doble clic en el nombre de la persona y seleccionar la pestaña **Identificadores Digitales**.

En el caso particular de los certificados emitidos por la Autoridad de Certificación de la Generalitat Valenciana, otra alternativa para obtener la clave pública de otros usuarios es hacerlo a través de la página web <u>http://www.accv.es/otrosusu_c.htm</u>, donde obtendrá información de cómo hacerlo.

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|--------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 9 de 10 |



4. Envío de mensajes cifrados digitalmente con Microsoft Outlook

Para crear un mensaje de correo en blanco pulsamos el botón **Nuevo** o en el menú **Archivo** seleccionamos **Nuevo**, **Mensaje**.

| 🔀 Sin título - Mensaj | je (Texto enriqueo | ido) | |
|-----------------------|--------------------|----------------------------|----------|
| Archivo Edición Ver | Insertar Eormato | Herramientas Acciones ? | |
| Enviar 📙 🎒 | X 🖻 🖬 🛃 | 🕕 😰 🕵 🚦 🖡 🔻 🚼 Opciones 🧖 🗸 | |
| Arial | • 10 • <u>A</u> | N K S 国 国 国 福 俸 福 🍇 🎦 🗸 | |
| Para coporte@p | ki gua ec | | |
| raja | IN. QVB. CS | | |
| | | | |
| Agunto: | | | |
| | | | <u>_</u> |
| Hola, | | | |
| · · | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | - |

Los pasos a seguir para enviar el mensaje cifrado son:

- Escribir la dirección de correo del destinatario del mensaje en el campo **Para**. Pulsando sobre este botón se abre la **Libreta de Direcciones** y puede buscar y seleccionar el contacto.
- Completar los campos Asunto y el cuerpo del mensaje.
- En caso que haya añadido los botones anteriormente, pulse el botón cifrar. De lo contrario, en la barra de Herramientas pulsar el botón Opciones. Aparecerá el siguiente cuadro de diálogo:

| Opciones de mensaje | <u>? ×</u> |
|---|--|
| Configuración de mensaje Seguridad Importancia: Normal T Carácter: Normal T Carácter: Normal T | aje y de los datos adjuntos saje saliente |
| Opciones de entrega Enviar las respuestas a: Guardar el mensaje enviado en: Caduca después del: Enviar el mensaje usando: pop3.gva.es | Seleccionar nombres |
| Opciones de seguimiento Opciones de seguimiento Solicitar confirmación de lectura para este mensaje Contactos Categorías | Cerrar |

- Pulsar Cerrar para confirmar las Opciones de mensaje.
- Pulsar el botón Enviar para enviar el mensaje.

| Clf.: PUBLICO | Ref.: MicrosoftOutlook.doc | Versión: 1.4 |
|----------------|--------------------------------|---------------|
| Est.: APROBADO | OID: 1.3.6.1.4.1.8149.1.1.8.18 | Pág. 10 de 10 |