

Firmar correos electrónicos usando Mozilla Thunderbird

Configuración de la herramienta e instructivo
PC - Ambiente Windows 7/8

Versión 1.0
Febrero 2015



Índice

[Índice](#)

[Alcance](#)

[Objetivo](#)

[Historial de versiones](#)

[Configuración inicial de Thunderbird](#)

[Descarga e instalación](#)

[Instalación de certificados de la AC-ONTI y la AC-Raíz](#)

[Carga del certificado digital a usar para firmar](#)

[Firmar digitalmente un correo electrónico](#)

[Validar la firma digital de un correo electrónico](#)

[Documentación externa de referencia](#)

[Anexos](#)

[Configuración de una cuenta de email UNC en Thunderbird](#)

Alcance

El presente documento contiene un resumen de instrucciones para configurar correctamente el cliente de correo electrónico "Mozilla Thunderbird v31.4.0" para enviar y validar correos electrónicos firmados digitalmente con certificados de AC ONTI bajo el protocolo PGP. El mismo se desarrolla para ambientes PC Windows 7 / 8 / 8.1 y no reemplaza la documentación oficial provista por Mozilla y por ONTI, referenciada al final del presente.

Objetivo

Los objetivos de este documentos son:

- Configurar Thunderbird para enviar correos electrónicos firmados digitalmente.
- Firmar digitalmente un correo.
- Validar la firma digital de correos recibidos.

Historial de versiones

Versión	Fecha	Responsable
v1.0	Feb-2015	José M. Sánchez <jsanchez@unc.edu.ar>
v1.1	Feb-2015	José M. Sánchez <jsanchez@unc.edu.ar>

Configuración inicial de Thunderbird

Descarga e instalación

La aplicación se distribuye de forma gratuita en internet bajo licencia *Mozilla Public License* y puede descargarse desde:

<https://www.mozilla.org/es-ES/thunderbird/>

Para la instalación se requieren permisos de administrador del sistema. Para ello, ejecutar el asistente y seguir las instrucciones en pantalla. Si la instalación es exitosa, se creará un acceso directo en el Escritorio.

Instalación de certificados de la AC-ONTI y la AC-Raíz

Para que el procedimiento de validación de correos firmados digitalmente sea correcto, es necesario agregar a la librería de Autoridades de Confianza de thunderbird los certificado de la *AC Raíz* y la *AC ONTI*. Para ello, primero se debe obtenerlos desde la web de la ONTI.

1. Abrir una ventana de Internet Explorer (exclusivamente, no otro navegador) y acceder a la URL:

<https://pki.jgm.gov.ar/app/>

2. En la barra de menús seleccionar “Certificados > Obtener el certificado Raíz y de la Autoridad Certificante”.
3. Una nueva página se abrirá. Clickear en el botón “Instalar certificado raíz”. En el cuadro de diálogo emergente elegir “Guardar como” y guardarlo en una ubicación de fácil acceso, por ejemplo en “Escritorio”.
4. Cerrar la ventana de Internet Explorer y abrir Thunderbird.
5. En la barra de menús seleccionar “Editar > Preferencias”. Luego, abrir la solapa “Avanzadas” y seleccionar la pestaña “Certificados”. Hacer clic en el botón “Ver certificados”.
6. Se abrirá la ventana del Administrador de Certificados. Seleccionar la pestaña “Autoridades” y luego dar clic en el botón “Importar...”.
7. En el explorador de archivos, seleccionar el certificado de la AC guardado en el punto 3 (si es necesario, cambiar el filtro de “Tipo de archivo” a *Todos los archivos* para visualizarlo).
8. Se abrirá una ventana de Descarga de certificado. Allí indicar que se confíe en “AC Raíz” para identificar a usuarios de correo electrónico y Aceptar.
9. Cerrar el Administrador de certificados y la ventana de Preferencias de Thunderbird.
10. Cerrar el programa.

Carga del certificado digital a usar para firmar

Para firmar digitalmente un correo electrónico, es necesario indicar el certificado digital a utilizar. Thunderbird, entre sus opciones de seguridad, permite asociar cada cuenta de correo configurada con un certificado digital. Para hacerlo se deben seguir los siguientes pasos:

1. Insertar el token con el certificado digital del firmante (importante hacerlo antes de realizar cualquier otro paso).
2. Abrir Thunderbird. En la barra de menús, acceder a “Editar > Configuración de cuentas”.
3. En la ventana emergente, ubicar en la columna de la izquierda la cuenta que desea asociar a un certificado. Desplegar sus propiedades y seleccionar “Seguridad”.
4. A la derecha de la ventana ubicar la sección de Firma digital. Dar clic en el botón “Seleccionar...” e indicar el certificado digital a utilizar. Si el mismo no aparece, verifique que tenga instalados los drivers del token y que el dispositivo se encuentre correctamente conectado. También puede verificar manualmente que Thunderbird tenga acceso a él a través del botón “Dispositivos de seguridad”, en la sección Certificados.
5. Una vez seleccionado el certificado a utilizar para la firma digital de correos de la cuenta, se habilitará la opción “Firmar los mensajes digitalmente (por defecto)”. Si marca esta opción, por defecto todos los mensajes que envíe se firmarán digitalmente (lo cual requerirá conectar su token para enviar los mismos). Si no la marca, entonces podrá elegir cuándo firmar digitalmente un correo, al momento de redactarlo (ver el instructivo siguiente).
6. Cerrar la ventana de configuración de la cuenta con el botón “Aceptar”. Cerrar Thunderbird.

Configuración inicial de Thunderbird

Firmar digitalmente un correo electrónico

Si en la *Carga del certificado digital a usar para firmar* no indicó firmar todos los mensajes por defecto, entonces podrá elegir cuándo firmar digitalmente un correo al momento de redactarlo. Para ello debe:

1. Conectar el token que contiene el certificado y la clave privada asociados a la cuenta.
2. Abrir Thunderbird y luego abrir la ventana de “Redactar correo”.
3. En la ventana de redacción del mensaje, hacer clic en el menú desplegable “Seguridad” y elegir la opción “Firmar digitalmente este mensaje”. Si existe un inconveniente con la configuración, una mensaje emergente se lo indicará y le guiará a la ventana de configuración correspondiente (para más información, ver el instructivo anterior).
4. Si no hay inconvenientes, la opción “Firmar digitalmente este mensaje” quedará marcada y podrá redactar y enviar el mensaje. Al enviarlo, la aplicación le solicitará el PIN del token para realizar la firma digital del mismo.

Validar la firma digital de un correo electrónico

La validación de un correo electrónico firmado digitalmente se realiza de manera automática:

Al abrir un correo firmado, podrá ver junto a la fecha y hora del mismo un ícono con forma de sobre. Haciendo clic sobre él podrá acceder al resultado de la validación del mismo, la cual verifica:

- la integridad del correo firmado (es decir, que no fue alterado),
- la validez de la firma, en base al certificado de la AC-Raíz instalado en la aplicación,
- la validez de la firma, en base al servicio OCSP de verificación en línea de revocación de certificados, y
- la correspondencia de la dirección de correo del remitente contra la dirección de correo declarada en el certificado digital del firmante.

Documentación externa de referencia

- ONTI: Tutorial para la configuración y firma de un correo electrónico:
http://pki.jgm.gov.ar/docs/Instructivo_para_configuracion_y_firma_de_correo_electronico.pdf
- Página de soporte de Mozilla Thunderbird:
<https://support.mozilla.org/es/products/thunderbird>

Anexos

Configuración de una cuenta de email UNC en Thunderbird

Las cuentas de correo electrónico de dominio unc.edu.ar se encuentran administradas por Google y tienen acceso a las aplicaciones web Google Apps, entre ellas Gmail para el correo electrónico. En ellas, el logueo se realiza en el sistema "Yuli" de Gestión de Personas y Usuarios de la UNC (esquema Single Sign On). Sin embargo, eso se dificulta al configurar clientes de correo electrónico como Thunderbird, ya que estos intentarán autenticarse ante el servidor de correo de Google y no ante Yuli. Para salvar este inconveniente, puede utilizarse el servicio de seguridad de "Verificación en dos pasos" de Google, que incluye la opción de crear contraseñas exclusivas para aplicaciones. A continuación, se resumen los pasos a seguir para configurar una cuenta de correo de dominio unc.edu.ar en Mozilla Thunderbird bajo este esquema:

1. Abrir un navegador de internet y loguearse en el webmail normalmente (autenticación a través de Yuli).
2. Abrir en otra pestaña la URL:

<https://myaccount.google.com/>

3. Habilitar la verificación de dos pasos (two-steps-verification). Con ello configuraremos nuestro teléfono celular como segundo factor de validación (sugerencia: configurar y utilizar la app Google Authenticator en su celular).
4. Luego, en la misma página, podremos crear una "Contraseña de Aplicación". Con ello generaremos una contraseña aleatoria exclusiva para una aplicación, en este caso Thunderbird.
5. De regreso en el webmail, ir a "Configuración > Reenvío de correo y POP/IMAP" y habilitar IMAP.
6. Abrir Thunderbird. Si el asistente de bienvenida no lo guía para configurar una nueva cuenta, puede hacerlo manualmente. Para ello debe seleccionar en la barra de menú "Editar > Configuración de cuentas".
7. En la ventana emergente, seleccionar "Acciones de cuenta > Agregar cuenta de correo". Completar lo siguiente:
 - a. **Su nombre:** Nombre para mostrar en los correos enviados.
 - b. **Correo electrónico:** Su cuenta de dominio unc.edu.ar.
 - c. **Contraseña:** Pegar aquí la contraseña generada en el punto 4.
 - d. **Recordar contraseña:** marcar la opción si desea que Thunderbird recuerde la contraseña ingresada (recomendado). De hacerlo, también es recomendable que luego establezca una contraseña maestra para Thunderbird, la cual protegerá todas las contraseñas almacenadas.
8. Dar clic en continuar para que Thunderbird detecte automáticamente la configuración del correo. Confirmar con el botón "Finalizar".
9. Cerrar la ventana de configuración de cuentas con el botón "Aceptar".
10. Cerrar Thunderbird.

Importante: La contraseña de aplicación generada en el punto 4 es de un solo uso y solamente podrá visualizarse al momento de generarla. Luego solo podrá ser revocada. Si no eligió la opción de Recordar Contraseña al configurar la cuenta, y por alguna razón Thunderbird vuelve a requerirla, deberá revocar la contraseña generada y crear una nueva.