DIRECCIÓN GENERAL DE LA POLICÍA | SUBDIRECCIÓN GENERAL DE LOGÍSTICA | UNIDAD DE INFORMÁTICA Y COMUNICACIONES

SERVICIO de SEGURIDAD TIC

INS-6.5.17.1-N3-DGP-Notificación de correos maliciosos

Propiedades del documento

Tipo de documento

Clasificación del documento:	**DIFUSIÓN LIMITADA**
Número de páginas:	9
Referencia del documento:	INS-6.5.17.1-N3-DGP-Notificacion de correos maliciosos
Resumen del documento:	Manual para la notificación de correos maliciosos.

Historial de versiones

Versión	Fecha	Elaborado por	Descripción del cambio
V1.0	23/05/16	Servicio de Seguridad TIC	Versión aprobada

Aprobación del documento

Responsable de la Seguridad - Jefe del Servicio de Seguridad TIC

Índice

Relación de ilustraciones

1 Introducción

Cuando recibamos un correo electrónico sospechoso de spam o phishing, debemos reenviarlo como adjunto a la dirección de correo seguridadtic@policia.es del Servicio de Seguridad TIC.

Es muy importante reenviar el correo **como adjunto**. Si no lo reenviamos como adjunto se perderían metadatos del correo electrónico original. Estos metadatos son muy importantes, ya que pueden incluir información esencial para investigar el origen como:

- Numero de serie del equipo que lo envió
- Dirección IP del equipo que lo envió.
- Buzón de correo usado para el envío.
- Dirección IP del servidor que envió el correo.

A continuación se muestra paso a paso como hacer los envíos a través de **Microsoft Outlook** y de **Thunderbird**.

2 Notificación de correos maliciosos

2.1 Microsoft Outlook 2007

Lo primero es seleccionar el correo supuestamente malicioso tal y como se muestra en la siguiente Ilustración.

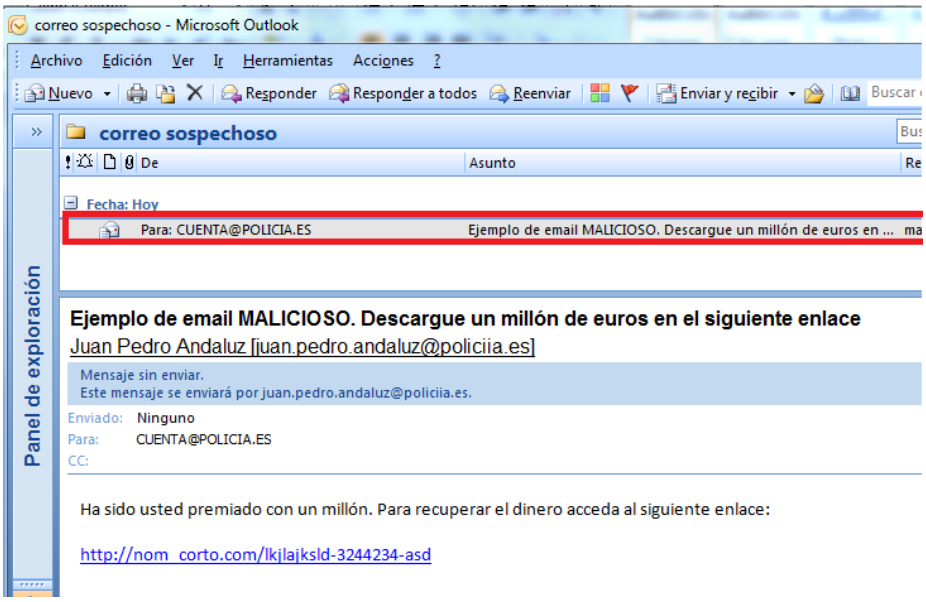

Ilustración 1: Seleccionamos el correo malicioso (Outlook 2007)

Una vez seleccionado el correo, hacemos clic en el menú “Acciones” y a continuación hacemos clic en “Reenviar como datos adjuntos” (tal y como se muestra en la siguiente Ilustración).

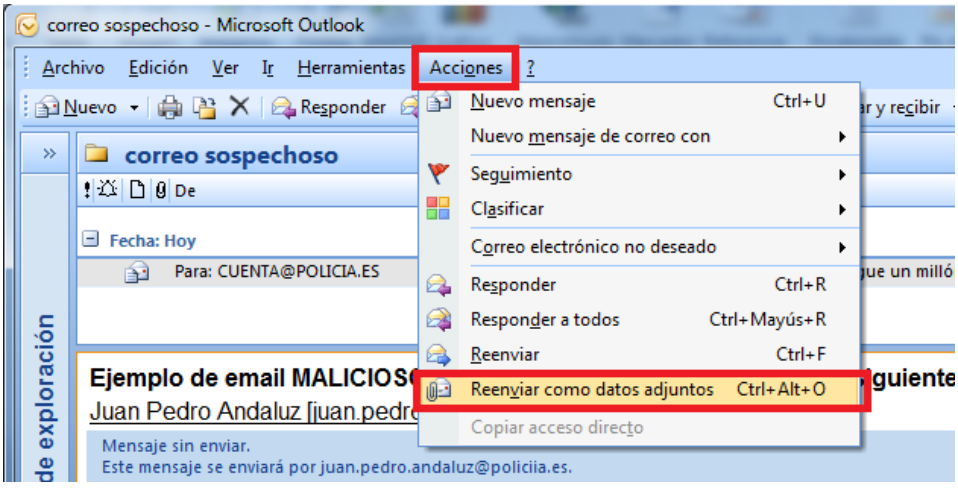

Ilustración 2: Reenviar como datos adjuntos (Outlook 2007)

A continuación nos aparece la redacción de un correo electrónico, que antes de enviar tenemos que revisar los siguientes puntos que aparecen marcado en rojo en la ilustración:

- Como destinatario (“Para”) del correo electrónico ponemos la dirección de correo del Servicio de Seguridad TIC: seguridadtic@policia.es.

- Como fichero adjunto debe aparecer un fichero cuyo nombre es el asunto del e-mail malicioso.
- En el cuerpo del correo electrónico escribimos detalles del incidente de los que nos hayamos percatado como, lentitud en el equipo, reiniciado, no funciona el antivirus, o cualquier otra información que pueda ser de interés para solventar la incidencia por parte del Servicio de Seguridad TIC.

Para finalizar hacemos clic en el botón

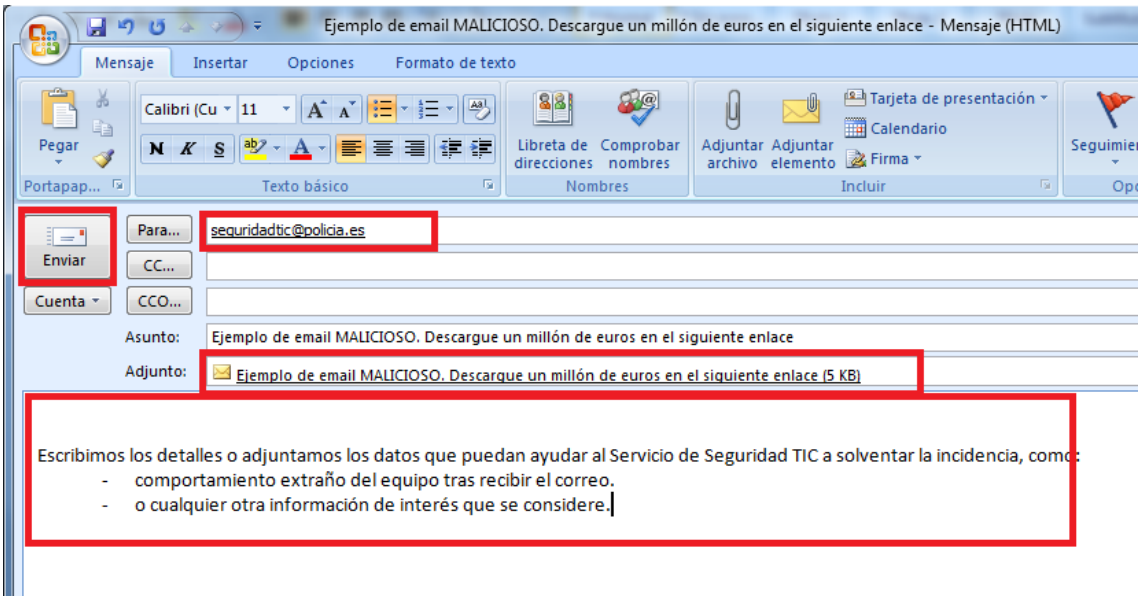

Ilustración 3: Reenviar como datos adjuntos al Servicio de Seguridad TIC (Outlook 2007)

2.2 Para otras versiones de Microsoft Outlook

En el caso de que no nos aparezca la opción de “reenviar como datos adjunto”, seguimos los pasos siguientes:

- creamos un nuevo correo y lo ponemos en paralelo con la bandeja de entrada.

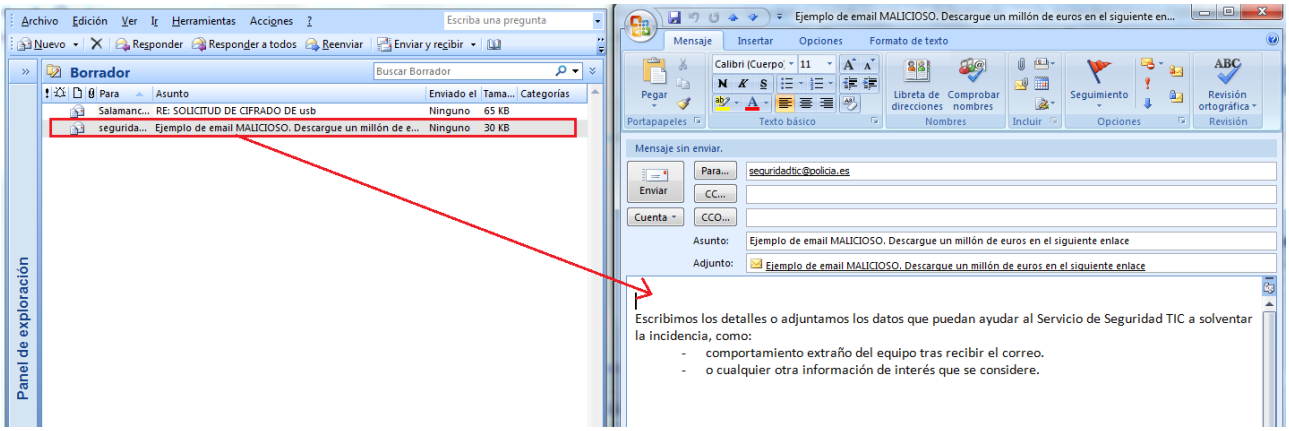

Ilustración 4 Otras versiones de Microsoft Outlook

- A continuación arrastramos el correo malicioso al correo nuevo y al soltarlo nos aparecerá como adjunto.
- Una vez adjuntado el correo, se redacta el correo tal y como se muestra en la “Ilustración 3”.
- A continuación enviamos el correo.

2.3 Thunderbird

Lo primero es seleccionar el correo supuestamente malicioso tal y como se muestra en la siguiente Ilustración.

Ilustración 5: Seleccionamos el correo malicioso (Thunderbird)

Una vez seleccionado el correo, hacemos clic en el menú “Mensaje” y a continuación hacemos clic en “Reenviar como” y para finalizar hacemos clic en “Adjunto” (tal y como se muestra en la siguiente Ilustración).

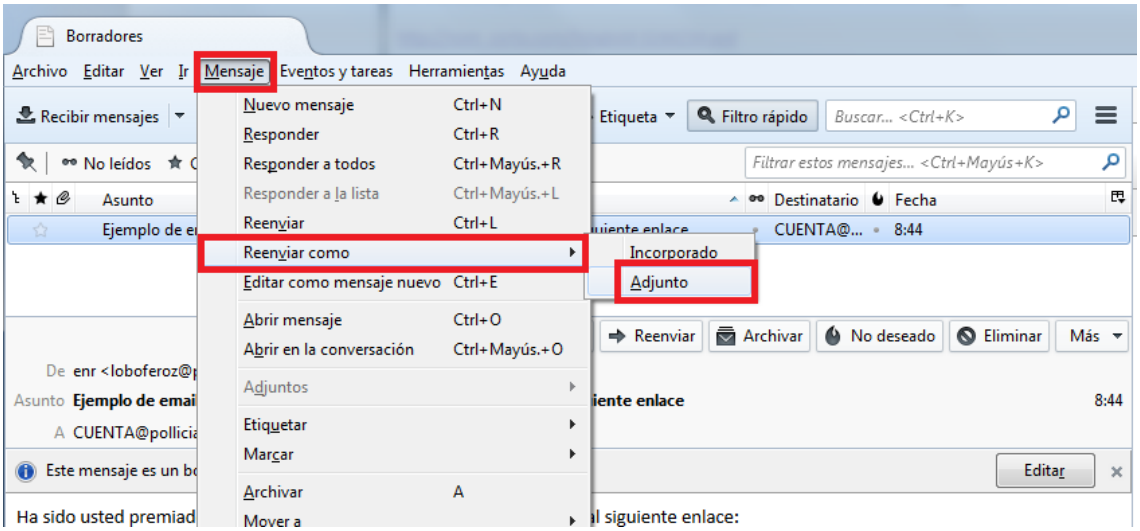

Ilustración 6: Reenviar como datos adjuntos (Thunderbird)

A continuación nos aparece la redacción de un correo electrónico, que antes de enviar tenemos que revisar los siguientes puntos que aparecen marcado en rojo en la ilustración:

- Como destinatario (“Para”) del correo electrónico ponemos la dirección de correo del Servicio de Seguridad TIC: seguridadtic@policia.es.

- Como fichero adjunto debe aparecer un fichero cuyo nombre es el asunto del e-mail malicioso.
- En el cuerpo del correo electrónico escribimos detalles del incidente de los que nos hayamos percatado como, lentitud en el equipo, reiniciado, no funciona el antivirus, o cualquier otra información que pueda ser de interés para solventar la incidencia por parte del Servicio de Seguridad TIC.
- Para finalizar hacemos clic en el botón Enviar.

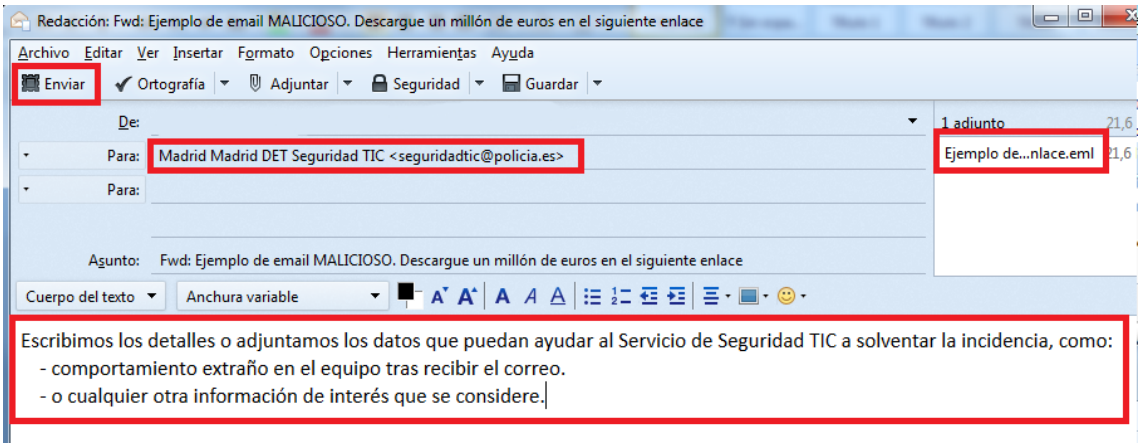

Ilustración 7: Reenviar como datos adjuntos al Servicio de Seguridad TIC (Thunderbird)