ESTAMOS A TU LADO

Servicio de Atención al Cliente

956 34 61 61

GABINETE DE MEDIADORES
Correduría de Seguros CS-J129

CIBER SEGURIDAD

GABINETE DE MEDIADORES
Correduría de Seguros CS-J129

www.gabinetedemediadores.com

Estimado Cliente,

Te agradecemos que hayas depositado tu confianza en nuestro seguro **CIBER SEGURIDAD**.

A partir de este momento dispones de las siguientes coberturas tecnológicas:

- **Análisis de Vulnerabilidades**: realizaremos un análisis automático y remoto de tu sistema informático.

- **Servicio de Asistencia Tecnológica:** una vez realizado el chequeo de seguridad, recibirás un informe del estado de tu sistema desde el que podrás acceder al servicio de asistencia tecnológica para resolver a distancia los problemas de seguridad que se hayan detectado.

- **Adaptación a la Ley de Protección de Datos**: nuestros especialistas te ayudarán a adecuar tu empresa al cumplimiento de las obligaciones específicas del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

Te recomendamos que empieces a utilizar nuestros servicios en este mismo momento, para ello debes ponerte en contacto con nosotros.

Si lo deseas puedes llamarnos al 956 34 61 61 o enviarnos un correo a **produccion@gabinetedemediadores.com**

GABINETE DE MEDIADORES
Correduría de Seguros CS-J129

CIBER SEGURIDAD: GARANTÍAS INCLUIDAS

Con el objetivo de incrementar aún más tu protección frente a un ciber ataque, y ofertar una óptima solución aseguradora, este producto se completa con las siguientes garantías:

- **Asistencia técnica y gastos de investigación del siniestro:** realizaremos una asistencia técnica "in situ", así como la investigación y peritaje para conocer el origen de los daños.

- **Gastos de reparación y recuperación de datos borrados y equipos dañados de los soportes electrónicos del asegurado** (discos duros, dispositivos móviles y servidores del asegurado).

- **Responsabilidad Civil frente a terceros**, consecuencia de:

  - Reclamaciones por difusión de datos de terceros de carácter personal.
  - Defensa jurídica.

GABINETE DE MEDIADORES
Correduría de Seguros CS-J129

Nuestro equipo de especialistas te asesorará y gestionará tu incidencia con la Agencia Española de Protección de Datos, así como llevará a cabo la defensa ante un posible procedimiento o denuncia de un tercero, haciendo frente al pago de indemnizaciones en caso de condena al asegurado.

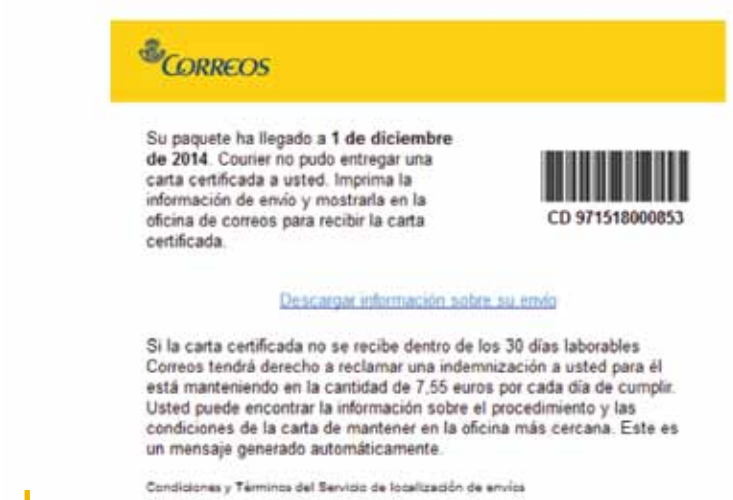
Se muestra un detalle exhaustivo de dichas coberturas tecnológicas y garantías en el contenido plasmado en póliza, la cual se encuentra incluida dentro de este paquete de bienvenida.

RECOMENDACIONES ANTE UN INCIDENTE DE SEGURIDAD

A continuación encontrarás las recomendaciones necesarias en caso de que se produzca un incidente de seguridad, en equipos con sistema operativo Windows:

1. SECUESTRO DE INFORMACIÓN O RANSOMWARE

El primer paso es poder identificar un secuestro de información. Normalmente suele aparecer en la pantalla del equipo una ventana pidiendo un rescate por la información que acaba de ser cifrada.


De: support@correos24.net [mailto:support@correos24.net]
Enviado el: miércoles, 03 de diciembre de 2014 14:41
Para:
Asunto: usted tiene una Carta certificada

CORREOS

Su paquete ha llegado a **1 de diciembre de 2014**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

CD 971518000853

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 30 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de 7,55 euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Condiciones y Términos del Servicio de localización de envíos

Otro caso muy famoso ha sido el mensaje de correo electrónico recibido supuestamente por Correos indicando que hay un paquete por entregar al usuario. Dicho mensaje adjunta un enlace para descargar un fichero malicioso.

Otra manera de verificar si se está infectado con este tipo virus es verificar si sus ficheros han sido cambiados de nombre, añadiendo al final del fichero .CRYPTED , .OMG, .ECC, .ENCRYPTED u otra extensión:

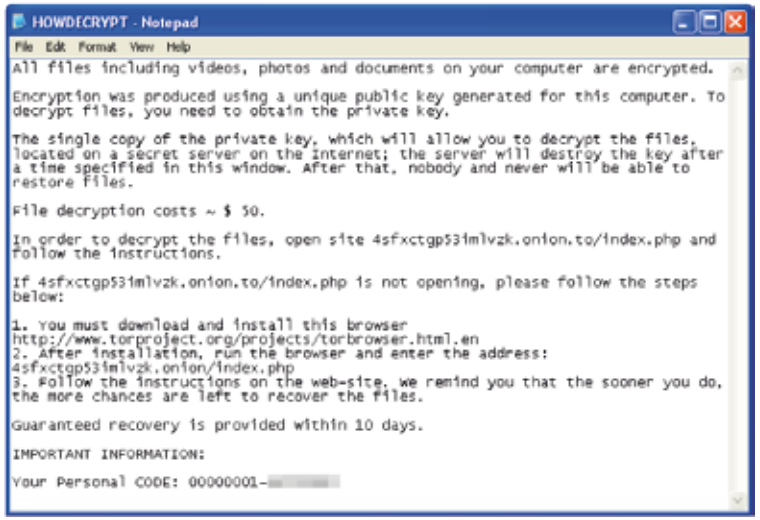
- **Documento_Word.doc.ENCRYPTED**
- **Documento_Adobe.pdf.OMG**
- **Documento_Excel.xlsx.CRYPTED**
- **IMAGEN.jpg.ECC**

Cuando se completa el proceso de cifrado de tus ficheros suele aparecer un fichero de reivindicaciones en el ESCRITORIO del usuario, de cómo proceder al pago del rescate para poder recuperar tus ficheros, nunca pague, no le asegura que pueda recuperarlos.

EJEMPLOS DE FICHERO DE REVINDICACIONES:

Fichero HTML

Fichero de Texto



GABINETE DE MEDIADORES
Correduría de Seguros CS-J129

Una vez identificado que nos encontramos ante un secuestro de información, inmediatamente desconectar el equipo de Internet, de cualquiera de las siguientes maneras.

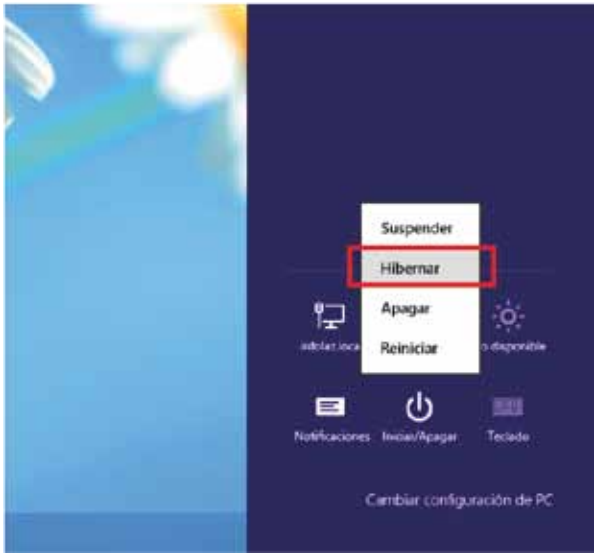
- **Apagar el Wifi**
- **Apagar el Router**
- **Desenchufar el cable de red**

Ten en cuenta que para aumentar el porcentaje de éxito en la reversión de los archivos que han sido cifrados por el virus:

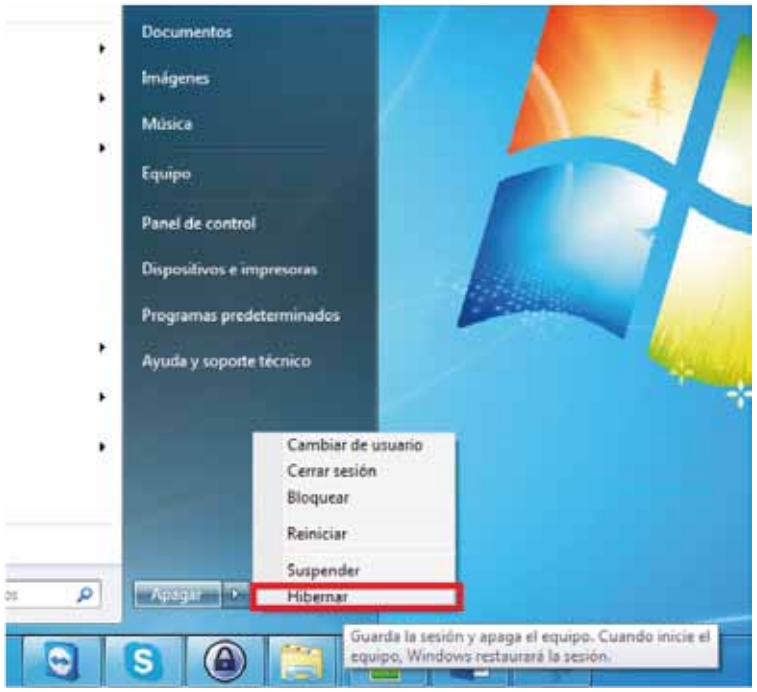
- **No utilizar el equipo infectado a menos que quiera recuperar toda su información cifrada.**
- **No instalar ningún antivirus ni ningún otro software.**
- **No manipularlo.**

Lo siguiente que se debe hacer es hibernar el sistema:

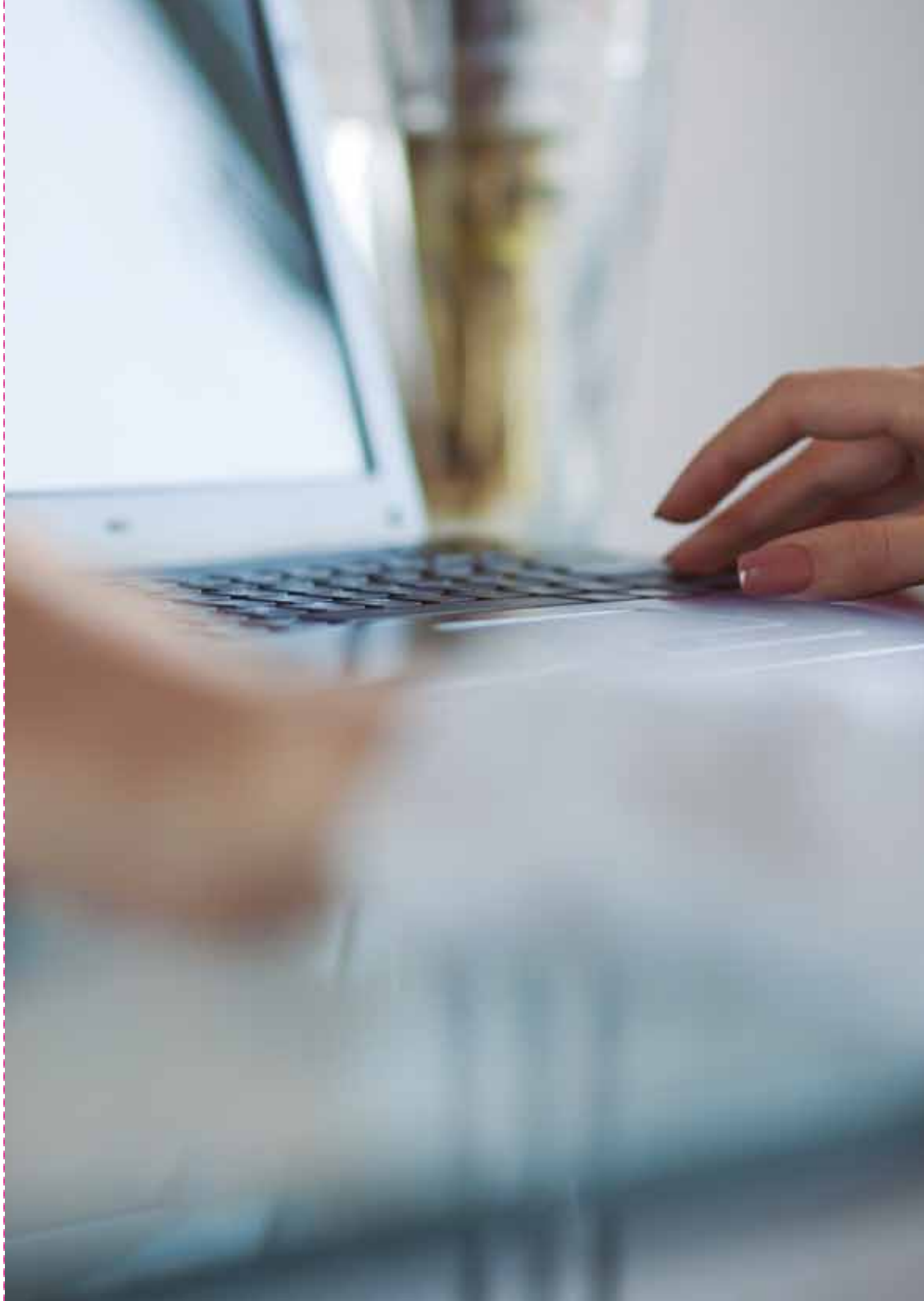
WINDOWS 8



WINDOWS 7



De esta manera todo el contenido de la memoria RAM pasará a ser volcado al fichero al hiberfil.sys.



2. VULNERABILIDADES

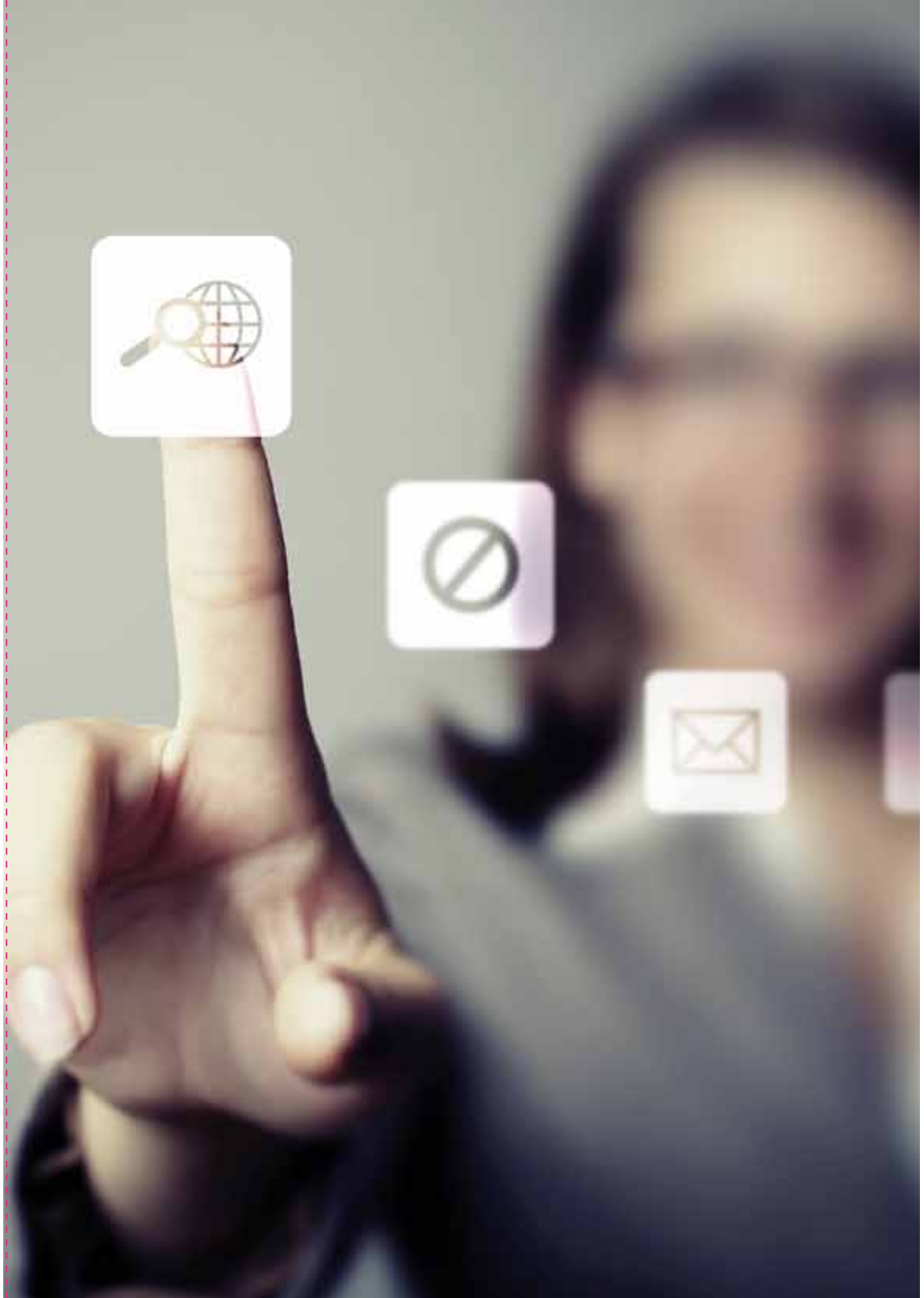
Las vulnerabilidades se pueden identificar de varias maneras:

- Mala configuración del sistema.
- Software anticuado y vulnerable.
- Puertos abiertos y publicados en Internet.

Estas vulnerabilidades pueden ser explotadas por virus informáticos:

- **Troyanos:** control remoto del equipo del usuario permitiendo monitorización en tiempo real.
- **Malware**: mal funcionamiento del sistema.
- **Botnet:** control remoto del equipo utilizado para realizar ataques informáticos a terceros.

Una mala configuración del sistema puede permitir que un atacante que se encuentre dentro de la organización pueda extraer información:

- Contraseñas inseguras tanto del equipo como de la red WiFi si tuviese.
- Equipos sin protección de contraseña.

En caso de que se identifique uno de los supuestos anteriores se recomienda desconectar el equipo de internet e hibernarlo. En caso de no poder hibernar el equipo, no apagar bajo ninguna circunstancia el equipo, hasta la peritación del mismo.