## Normas y Consejos de Seguridad

## -Área Española del Registro de la Unión-

**De conformidad con lo establecido en la solicitud de apertura y mantenimiento de cuenta en el Área Española del Registro de la Unión, los usuarios de dicho Área deberán cumplir con las normas de seguridad recogidas en el presente documento.**

## El presente documento recoge una serie de normas y consejos de seguridad destinados a los usuarios que accedan y realicen cualquier clase de actuación en el Área Española del Registro de la Unión, con objeto de garantizar la máxima seguridad en el uso del referido Área evitando, por ejemplo, que se produzcan intentos de suplantación de la identidad de los usuarios. En este sentido, es necesario tener en cuenta que los correos electrónicos y las páginas web fraudulentas pueden llegar a ser muy elaborados y sofisticados.

## A continuación se expone una relación de las normas de seguridad que tienen que cumplir los usuarios del Área Española del Registro de la Unión:

* Conectarse al Área Española del Registro de la Unión desde el puesto de trabajo proporcionado por la empresa o bien, desde el propio dispositivo del usuario siempre que haya sido autorizado por la política de seguridad de la empresa.
* Tener instalado en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión, como mínimo, un programa antivirus, y asegurarse de que éste se encuentra permanentemente actualizado. No obstante, se recomienda tener instalados dos programas antivirus diferentes (procedentes de dos proveedores diferentes) ejecutados en paralelo.
* Asegurarse de que el dispositivo que se utilice para acceder al Área Española del Registro de la Unión, a través del programa antivirus que tenga instalado, realiza automáticamente y con una periodicidad mínima de dos semanas, procesos de detección de virus o *spyware*.
* Tener instalado en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión un cortafuegos o *firewall* y asegurarse de que éste se encuentra permanentemente actualizado[[1]](#footnote-1).
* Mantener permanentemente actualizado el sistema operativo y demás *software* instalado en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión con las últimas actualizaciones disponibles.
* Comprobar que el sistema operativo que instala en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión es la última versión del mismo, de tal forma que incluya las últimas novedades y actualizaciones en lo que a aplicaciones de seguridad se refiere.
* Elaborar una lista del *software* autorizado que está instalado en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión y asegurarse, llevando a cabo los procesos de verificación correspondientes en colaboración con el personal técnico competente encargado del mantenimiento y supervisión de los equipos informáticos, de que ningún otro *software* está instalado en dicho dispositivo, de manera que si se detecta la presencia de un *software* no autorizado se deberá eliminar.
* Asegurarse de que los accesos al dispositivo que se utilice para acceder al Área Española del Registro de la Unión son analizados por personal técnico competente encargado del mantenimiento y supervisión de los equipos informáticos, con el fin de que se pueda detectar la existencia de un acceso no autorizado. En caso de detectarse, deberá llevarse a cabo una investigación sobre dicho acceso no autorizado.
* Acceder al Área Española del Registro de la Unión sólo a través de una conexión segura de Internet. Dicha conexión deberá incluir una protección *firewall,* un sistema de detección de intrusos*,* un antivirus e, igualmente, deberá disponer de mecanismos para restringir el acceso a páginas de Internet no seguras.
* No compartir el dispositivo que se utilice para acceder al Área Española del Registro de la Unión con otras personas.
* No incorporar a correos electrónicos ni hacer caso de correos electrónicos que incorporen enlaces a la página web del Área Española del Registro de la Unión. En este sentido, IBERCLEAR nunca enviará correos electrónicos con enlaces a la página web del Área Española del Registro de la Unión.
* No atender nunca a mensajes que soliciten contraseñas y/o nombres de usuario y/o códigos SMS. En los últimos tiempos se ha registrado un importante incremento de los casos de *phishing*[[2]](#footnote-2). Desde IBERCLEAR nunca se solicitará por ningún tipo de medio los datos de contraseña y/o nombre de usuario y/o código SMS para el acceso al Área Española del Registro de la Unión, ni tampoco ningún detalle del software instalado. Por otro lado, los correos electrónicos enviados por IBERCLEAR serán siempre mandados desde la direcciones: correo.titulares.renade@grupobme.es; auditoria.renade@grupobme.es; DesarrolloNR.renade@grupobme.es
* No abrir documentos que estén adjuntos a correos electrónicos que no provengan del Registro de la Unión (CLIMA-EU-ETS-REGISTRY-PROD@ec.europa.eu) sin antes haber verificado minuciosamente la fuente de la que proviene el correo electrónico.
* No abrir documentos que estén adjuntos a correos electrónicos y que tengan como extensión del archivo “.com, .bat, .vbs, .wsh, o .exe”.
* Contactar inmediatamente con IBERCLEAR y no realizar ninguna otra actuación en el registro, si se tiene alguna sospecha sobre el origen, contenido, etc., de algún correo electrónico recibido (los errores ortográficos en el contenido de los mismos pueden ser indicadores de un origen fraudulento), o se tiene cualquier otro tipo de sospecha no necesariamente relacionada con un correo electrónico. En este sentido, los usuarios del Área Española del Registro de la Unión siempre serán informados de hechos relevantes en relación con el Registro de la Unióna través de anuncios en la página web del Área Española del Registro de la Unión.
* Usar un salvapantallas que después de 15 minutos de inactividad desconecte al usuario de cualquier sesión que tuviera iniciada, cerrando la sesión abierta. Además, deberá existir una política de empresa de no dejar desatendido el ordenador sin activar el salvapantallas, asegurándose de que se activa cuando el usuario deja el puesto de trabajo.
* No configurar en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión la opción de “*auto log-in*” para el acceso al mencionado Área. Cada vez que se acceda al Área Española del Registro de la Unión se deberá escribir la contraseña y el usuario. En este sentido, el navegador de Internet deberá estar configurado de manera que se impida que se guarde la contraseña, el nombre de usuario y cualquier otra información (historial, cookies) cuando se cierre.
* Evitar (utilizando la configuración BIOS de su dispositivo) arrancar el dispositivo desde CD’s/DVD’s y/o dispositivos USB conectados al mismo. Los usuarios no deben poder acceder a la configuración BIOS del dispositivo que se utilice para acceder al Área Española del Registro de la Unión, la cual, debe estar protegida con una clave segura y diferente a la clave de acceso al Área Española del Registro de la Unión.
* Asegurarse de que el dispositivo que se usa para conectarse al Área Española del Registro de la Unión está configurado de manera que impida que se comparta con entidades externas a la propia empresa en la que trabaja el usuario, para evitar que servidores de ejecución (ej. http(s), ftp) o programas de intercambio de archivos (ej. BitTorrent) se ejecuten en dicho dispositivo.
* Se recomienda no conectar ningún dispositivo USB que no sea de confianza al dispositivo que se utilice para acceder al Área Española del Registro de la Unión. En todo caso, el dispositivo que se utilice para acceder al Área Española del Registro de la Unión deberá disponer de un sistema que detecte y registre la conexión de un dispositivo USB.
* Tomar precauciones para prevenir el uso no autorizado del teléfono móvil que se utilice para conectarse al Área Española del Registro de la Unión.
* No usar el teléfono móvil con el que accede al Registro de la Unión para conectarse al Área Española del Registro de la Unión, para realizar transacciones en Internet al mismo tiempo.
* Abstenerse de transmitir a terceros (incluidos otros titulares de cuentas), el nombre de usuario, y/o contraseña, y conservar los mismos en secreto y debidamente custodiados, ya que los mencionados datos son estrictamente personales, de manera que cualquier actuación realizada en el Área Española del Registro de la Unión bajo un nombre de usuario y/o contraseña y/o código SMS se considerará realizada bajo la responsabilidad del titular de dicho nombre de usuario y/o contraseña. Por lo tanto, los usuarios son responsables de todas las acciones que realicen con su nombre de usuario y/o contraseña, por lo que deberán comunicar inmediatamente a IBERCLEAR el acceso a la cuenta abierta en el Área Española del Registro de la Unión por parte de un tercero no autorizado, haciéndose responsable de todos los perjuicios que se pudieran derivar de la falta de dicha comunicación. Igualmente, en caso de que se produjera el extravío o sustracción del nombre de usuario, y/o contraseña, se deberá notificar a IBERCLEAR de inmediato, haciéndose responsable de todos los perjuicios que se pudieran derivar de la falta de dicha notificación.
* Elegir una contraseña que contenga caracteres especiales, numéricos y alfabéticos; en este último caso, combinando mayúsculas y minúsculas, y modificar la contraseña de forma regular.
* Desconectarse del Área Española del Registro de la Unión cerrando siempre la sesión que se tuviera abierta, con el fin de que personas que no estén autorizadas tengan acceso a la/s cuenta/s abierta/s en la misma.
* Informar a IBERCLEAR de cualquier cambio que se produzca en la dirección de correo electrónico asociada a la cuenta abierta en el Área Española del Registro de la Unión. IBERCLEAR procederá siempre a verificar, para cualquier comunicación recibida, que la dirección de correo electrónico de origen coincide con la que le consta previamente registrada.
* En el caso de que no se acceda a la página web del Área Española del Registro de la Unión escribiendo directamente la dirección de la misma en el cuadro correspondiente del buscador de Internet, será necesario verificar siempre que se están introduciendo los datos en una página segura. Para ello será necesario:
* Comprobar que la dirección (URL) del servidor comienza por “https:” (servidor seguro), en lugar de por “http:”.
* Comprobar los certificados de seguridad de la página a la que se ha accedido. Para ello:
* Si el navegador es ***“Microsoft Edge”***,

Una vez se accede a la página web del registro pulsar en el icono del candado (deberá estar cerrado) que aparece al acceder a una zona segura. El candado aparece en la parte derecha de la barra de navegación:

Pulsar en dicho candado 🡪 “Ver certificados”



Pulse en la pestaña “La conexión es segura” dónde puede verificar la procedencia y dirección web asociada al certificado, así como la fecha de validez del mismo.





* Si el navegador es ***“Chrome”***,

Una vez se accede a la página web del registro, haga clic en el candado al lado del URL.



Pulse en “Conexión segura”, y después en “el certificado es válido”.



Una vez hecho clic en “el certificado es válido” le aparecerá la siguiente información:



**IBERCLEAR nunca solicitará datos de contraseña y/o nombre de usuario y/o código SMS a través de ningún tipo de medio de comunicación (teléfono, correo electrónico, fax, etc.).** **En caso de recibir un mensaje en este sentido o, dudar sobre la autenticidad del mismo por simular cualquier correo electrónico o sitio de Internet que diga estar remitido o ser propiedad de IBERCLEAR, por favor, no facilite dato alguno y contacte inmediatamente con IBERCLEAR en el teléfono 91 709 51 55.**

Finalmente, se expone una relación de consejos deseguridad que deberían ser observados por los usuarios del Área Española del Registro de la Unión:

* Se aconseja tener instalados en el dispositivo que se utilice para acceder al Área Española del Registro de la Unión dos programas de antivirus de diferentes proveedores y tenerlos permanentemente actualizados.
* Se aconseja acceder a la página web del Área Española del Registro de la Unión escribiendo directamente la dirección de la misma en el cuadro correspondiente del buscador de Internet.
* Se aconseja desconfiar de los correos electrónicos repetidos. Si se reciben dos o más correos con remitentes diferentes y un mismo asunto, puede tratarse de un virus que disimula su origen.
* Se aconseja no conectarse a la página web del Área Española del Registro de la Unión desde dispositivos de uso público sobre los que no se pueda tener control del *software* que hay instalado (ciber-cafés, bibliotecas, universidades, etc.).

En nombre y representación del Titular de Cuenta[[3]](#footnote-3) Haga clic aquí para escribir texto., (en adelante, el “Titular de Cuenta”) por medio de la firma del presente documento, declaro que he leído y comprendido las normas de seguridad y consejos recogidos en el mismo, y **me obligo a cumplir dichas normas de seguridad, y a comunicarlas y a hacerlas cumplir por parte de todos los usuarios que accedan y realicen cualquier clase de actuación en el Área Española del Registro de la Unión en relación con la cuenta abierta en el mencionado Área por el Titular de Cuenta**. Igualmente, me comprometo a comunicar los consejos de seguridad a todos los usuarios que accedan y realicen cualquier clase de actuación en el Área Española del Registro de la Unión en relación con la cuenta abierta en el mencionado Área por el Titular de Cuenta.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Nombre completo del Representante Legal]

Representante Legal

En [Lugar], a [Seleccione fecha]

1. Un cortafuegos es un software destinado a garantizar la seguridad en sus comunicaciones vía Internet. El cortafuegos bloquea las entradas sin autorización al dispositivo y restringe la salida de información. [↑](#footnote-ref-1)
2. ¿Qué es el *phishing*?

 El *phishing* es una estafa informática consistente en suplantar la identidad de una empresa para conseguir información confidencial de los clientes, así como sus claves de acceso.

 ¿Cómo actúa el *phisher*?

 Los ataques se producen mediante correos electrónicos engañosos en los que se suplanta la identidad de la empresa afectada. Estos correos redirigen a una web fraudulenta que imita el aspecto de la página original. El *phisher* se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, generalmente mediante un [correo electrónico](http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico) o algún sistema de [mensajería instantánea](http://es.wikipedia.org/wiki/Mensajer%C3%ADa_instant%C3%A1nea), o incluso utilizando también llamadas telefónicas. Los daños causados por el *phishing* oscilan entre la pérdida del acceso al correo electrónico y pérdidas económicas sustanciales. [↑](#footnote-ref-2)
3. Nombre del Titular de Cuenta abierta en el Área Española del Registro de la Unión [↑](#footnote-ref-3)