
PROTECTOR
SUITE QL
versión 5.6
TouchChip

Aviso de copyright e información acerca del propietario

UPEK®, Inc

http://www.upek.com

Este producto incluye software desarrollado por OpenSSL Project para su uso en OpenSSL Toolkit (http://www.openssl.org/).

Este producto incluye software criptográfico escrito por Eric Young (eay@cryptsoft.com).

Marcas comerciales

Índice

Capítulo 1
Instalación de Protector Suite QL

Instalación de Protector Suite QL

Protector Suite QLSe puede instalar en cualquier equipo con Windows 2000, XP Home o Professional edition, Windows Vista y un puerto USB libre. Se necesitan derechos de administrador para instalar o desinstalar Protector Suite QL. Si ya lo tiene Protector Suite QL preinstalado en el equipo, puede ignorar este capítulo.

Para instalar Protector Suite QL:

1. *Si tiene un CD insértelo en la unidad de CD-ROM, de lo contrario ejecute Setup.exe e ignore el paso 2.*
2. *Aparecerá la pantalla Protector Suite QL. Haga clic en el icono Instalación de. Si no aparece esta pantalla, ejecute Setup.exe manualmente.*
3. *Aparecerá la pantalla de bienvenida.*
4. *Haga clic en **Siguiente** para continuar.*
5. *Aparecerá la pantalla Información de usuario.*
6. *Introduzca su información de usuario y haga clic en **Siguiente** para continuar.*

7 *Confirme o seleccione un directorio de instalación.*

8 *Haga clic en **Siguiente** para comenzar la instalación.*

9 *Una vez finalizada la instalación, reinicie el equipo si se le solicita.*

La instalación ha finalizado ahora. Cuando reinicie el equipo, aparecerá la pantalla de inicio de sesión.

Nota: Durante la instalación, se instalarán todos los controladores del dispositivo necesarios. Si desea utilizar un sensor externo de huellas digitales, recomendamos que conecte el hardware de huellas digitales tras finalizar el proceso de instalación y reiniciar el equipo.

Desinstalación de Protector Suite QL

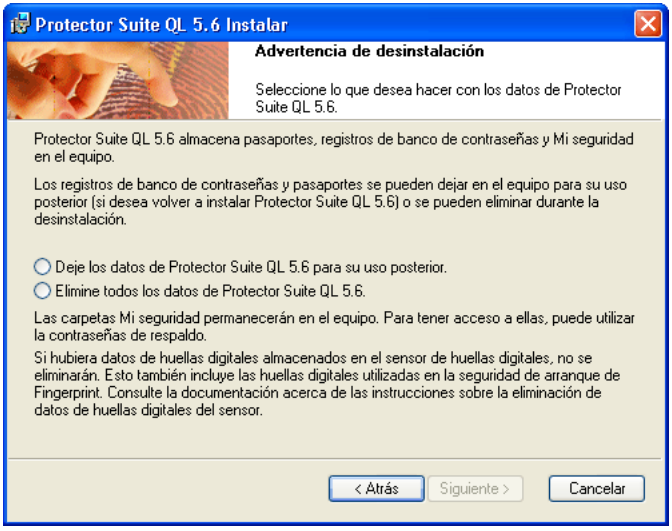
Para desinstalar Protector Suite QL:

1 *Haga clic en **Inicio > Panel de control***

2 *Haga doble clic en el icono **Agregar o quitar programas** (**Programas y funciones** en Windows Vista).*

3 *Seleccione Protector Suite QLy haga clic en el botón **Cambiar**.*

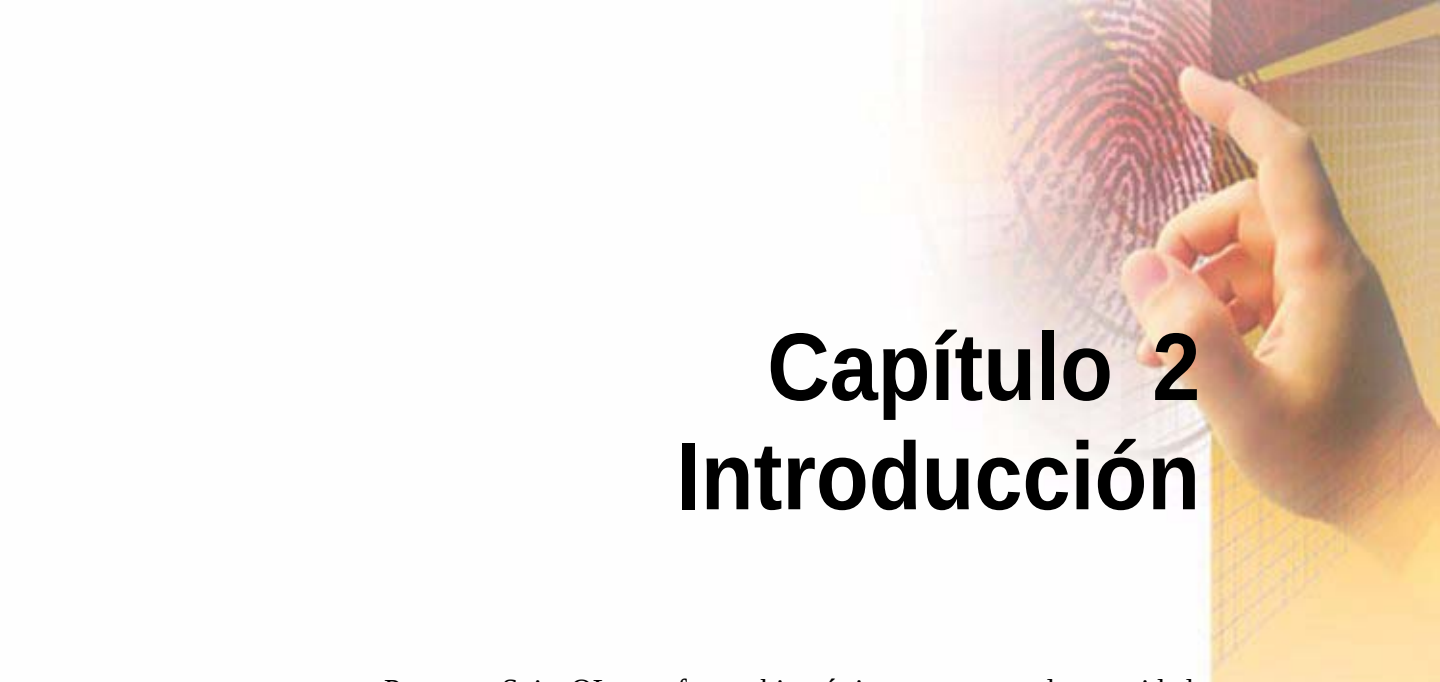
4 *Haga clic en el botón **Quitar**.*



5 *Se le preguntará qué desea hacer con los datos de Protector Suite QL almacenados en su equipo. Existen dos posibilidades:*

*• **Deje los datos de Protector Suite QL para su uso posterior** en el equipo. Esto significa que si reinstala Protector Suite QL posteriormente, puede continuar utilizando las huellas digitales incluidas para acceder a los datos de los archivos de seguridad de archivos cifrados, para iniciar sesión en su equipo y para acceder a los registros del Banco de contraseñas.*

*• Puede **eliminar todos los Protector Suite QL datos de** de su equipo. Las huellas digitales y los registros del Banco de contraseñas incluidos se eliminarán definitivamente.*



Capítulo 2
Introducción

Protector Suite QL es software biométrico que protege la seguridad de sus datos mediante el uso de la verificación de huellas digitales. La verificación de huellas digitales se realiza pasando el dedo por el sensor de huellas digitales.

Una vez instalado el software y reiniciado el equipo, tendrá que incluir sus huellas digitales para crear una asociación entre su nombre y contraseña de usuario y sus huellas digitales junto con claves de seguridad generadas automáticamente. Todos los datos se guardan en un *pasaporte* de usuario. Este procedimiento se llama **Inclusión de huellas digitales.**

Una vez incluidos sus dedos podrá:

- *utilizar el sensor de huellas digitales para administrar con seguridad los inicios de sesión "a nivel de prearranque" y a nivel de sistema operativo Windows“Inicio de sesión mediante huellas digitales” en la página 24)*
- *registrar páginas Web y aplicaciones de Windows para reemplazo de contraseñas (consulte “Banco de contraseñas” en la página 29)*
- *iniciar su aplicación favorita con sólo pasar el dedo por el sensor (consulte“Iniciador de aplicaciones” en la página 36)*

- *guardar información confidencial cifrada en una carpeta protegida (consulte“Seguridad de archivos” en la página 39)*

Este capítulo le ofrece una visión general de las principales características del software con el fin de que pueda dar sus primeros pasos rápidamente. Para obtener una descripción detallada de todas las funciones, consulte el Capítulo 3 “Utilización de Protector Suite QL” en la página 13 y para obtener una descripción de cómo controlar y administrar Protector Suite QL, consulte el Capítulo 4 “Gestión de Protector Suite QL” en la página 51).

Nota: Cada usuario de Windows debe tener un Protector Suite QLpasaporte único.

Inclusión de huellas digitales

Cada identidad de usuario en Protector Suite QL está representada por un "pasaporte", que contiene datos biométricos de huellas digitales para verificar la identidad del usuario.

Antes de utilizar el software por primera vez, deben crearse muestras de huellas digitales para su pasaporte.

Para iniciar el Asistente para la inclusión:

- *Seleccione **Inicio > Programas > Protector Suite QL > Inclusión del usuario***

Siga las instrucciones que aparecerán en pantalla. Para obtener más información,consulte el Capítulo 3 “Inclusión de huellas digitales” en la página 14.

Acceso a principales funciones

Biomenú

Biomenú le da un acceso rápido a las funciones de Protector Suite QL, como por ejemplo bloqueo del equipo, inicio de sitios registrados y registrar sitios web y diálogos, bloqueo de archivos de archivos o mostrar el menú **Ayuda.**

Para ver Biomenú:

- *Una vez incluido un dedo como mínimo, páselo por el sensor y aparecerá **Biomenú**.*

Consulte el Capítulo 4, “Biomenú” en la página 78 para saber más sobre los elementos de Biomenú.

Centro de control

Puede acceder a las funciones de administración general de **Configuraciones** de Protector Suite QL y **Huellas digitales** (por ejemplo edición y eliminación de pasaportes) en el cuadro de diálogo **Centro de control**.

Para ver Centro de control:

- *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***
- *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
- *o haga clic con el botón derecho en el icono de bandeja y seleccione **Iniciar centro de control...***

Aparece la pantalla principal del Centro de control. En esta pantalla aparecen las principales funciones del software. Haga clic en el nombre de la función para ver una pantalla que muestre las acciones válidas disponibles. Entre éstas se incluyen **Huellas digitales**, **Configuraciones** y **Ayuda**.

Para obtener más información sobre el Centro de control y sus funciones, consulte el Capítulo 4, “Centro de control” en la página 51.

Icono de la bandeja del sistema

El icono de Protector Suite QL en la bandeja del sistema indica que el programa está en ejecución y proporciona acceso a las funciones que no requieren la autenticación de las huellas digitales.

Haga clic con el botón derecho en el icono para ver el menú:

Para obtener más información sobre los elementos del menú Icono de la bandeja del sistema, consulte el Capítulo 4, “Icono de la bandeja del sistema” en la página 80.

Cómo utilizar el menú Ayuda

Protector Suite QL contiene un sistema de ayuda basado en código HTML.

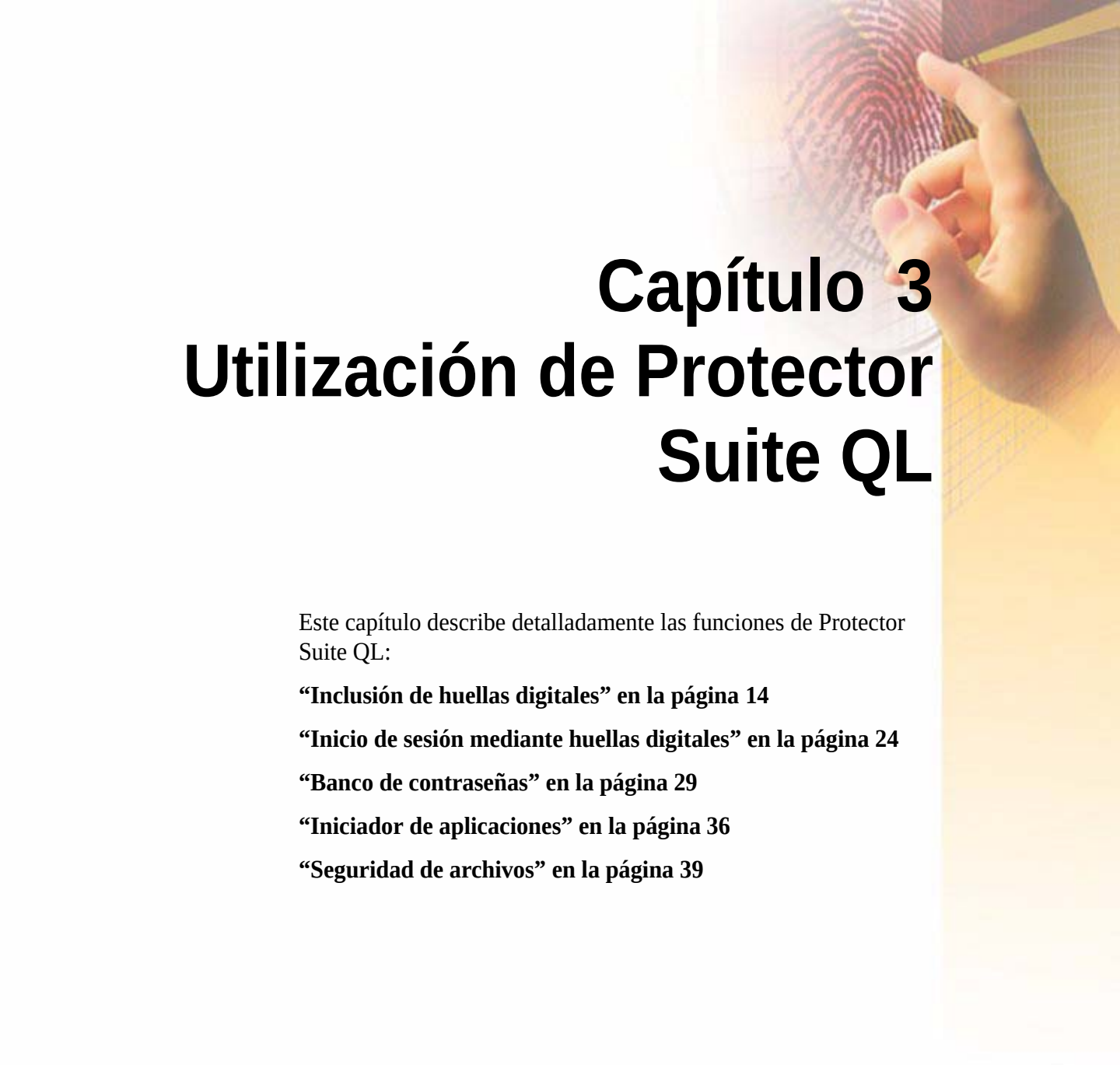
Para ver la ayuda HTML:

- *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Ayuda***
- *o seleccione **Ayuda** en **Biomenú**,*
- *o haga clic con el botón derecho en el icono de la bandeja y seleccione **Ayuda***
- *o haga clic en el icono Ayuda en el cuadro de diálogo Centro de control*

También se encuentra disponible una ayuda contextual en la mayoría de los cuadros de diálogo.

Para visualizarla:

- *Pulse F1 para ver la ayuda HTML del cuadro de diálogo para el que necesita ayuda.*



Capítulo 3
Utilización de Protector Suite QL

Este capítulo describe detalladamente las funciones de Protector Suite QL:

Inclusión de huellas digitales

Antes de comenzar a utilizar Protector Suite QL, debe *incluir*su dedo o dedos. La inclusión es el proceso de creación de una correspondencia entre su nombre y contraseña de usuario y sus huellas digitales (computerizadas, de manera que resulte imposible reconstruir la imagen original), junto con claves de seguridad generadas automáticamente. Todos los datos se almacenan en su *pasaporte*.

Primer uso

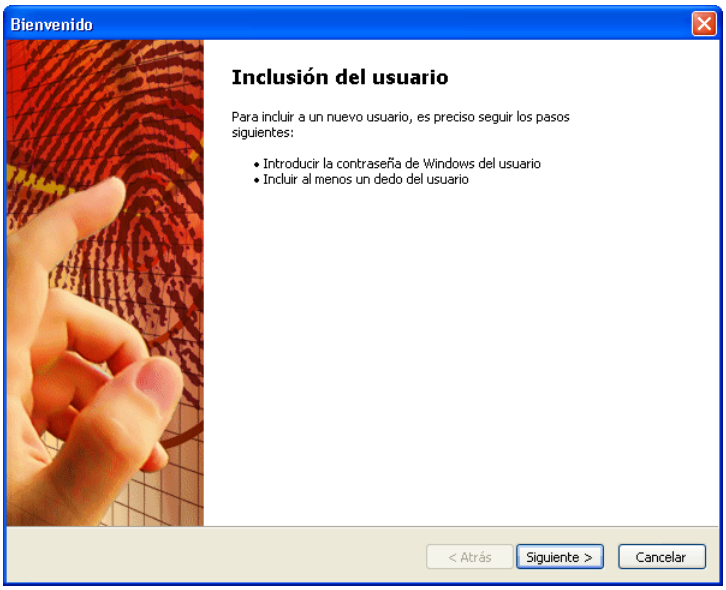
Para crear una nueva contraseña (incluir huellas digitales):

1. *Si desea utilizar un sensor externo de huellas digitales, conecte el dispositivo. Todos los controladores necesarios se instalan con Protector Suite QL. Aparecerá en la esquina inferior derecha de la pantalla un mensaje informativo de que el sensor está conectado y listo para usarse.*
2. *Aparecerá el Contrato de Licencia. Lea detenidamente el Contrato de Licencia.*
3. *Acepte el Contrato de Licencia seleccionando el botón de opción adecuado. Debe aceptar el Contrato de Licencia para instalar este producto. Haga clic en* ***Cancelar*** *para cerrar la aplicación si no acepta el Contrato de Licencia.*
4. *Para iniciar el asistente para la inclusión, vaya a*

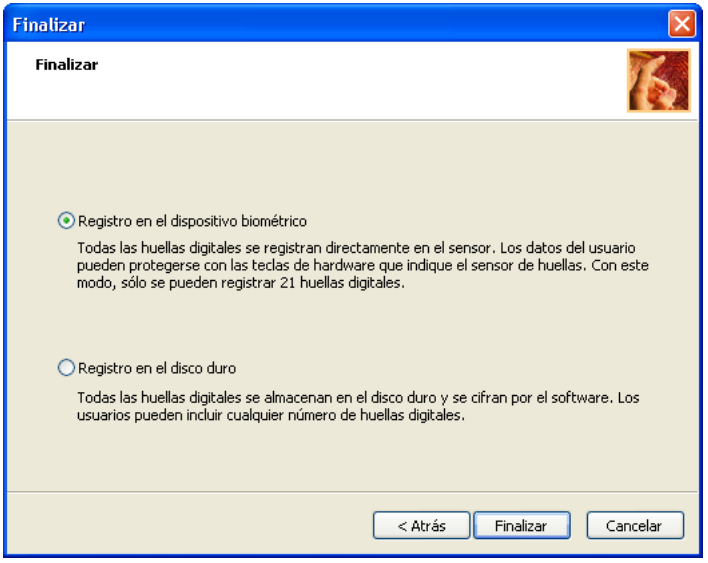
   Inicio > Todos los programas > Protector Suite QL > Inclusión del usuario

   o seleccione ***Huellas digitales > Incluir o editar huellas digitales*** *en* ***Centro de control***

   o haga clic en el icono de la bandeja y seleccione ***Editar huellas digitales...****.*



5 *Se le pedirá que escoja el tipo de inclusión. Si su dispositivo admite la inclusión en la memoria del dispositivo, puede seleccionar si desea almacenar los datos de autenticación en la memoria del dispositivo o en el disco duro.*



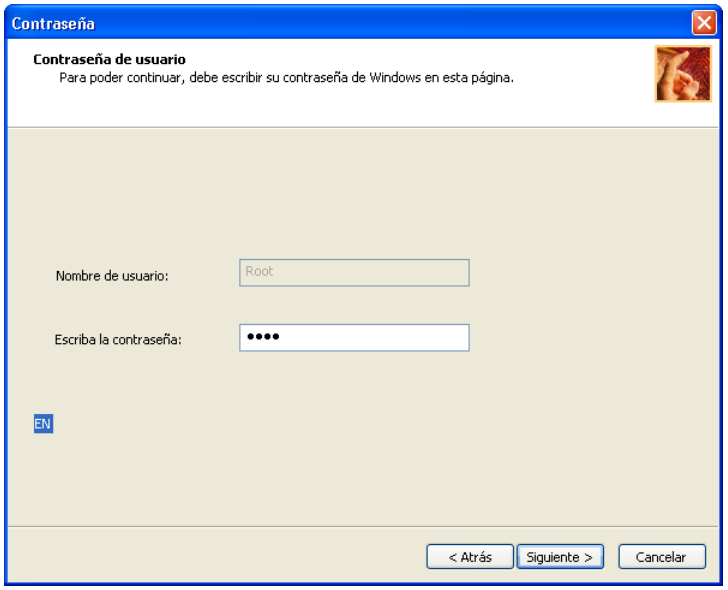
• Si escoge la inclusión en la memoria del dispositivo, no se podrá acceder a los datos sin el dispositivo de huella digital correspondiente. La información de autenticación estará protegida por una clave de cifrado de software, creada por el software de huella digital, además de la clave de hardware que se obtiene directamente del dispositivo.

• El único límite es la memoria del dispositivo. Si piensa incluir un número mayor de huellas digitales para varios usuarios (la memoria de dispositivo normal suele abarcar 21 huellas), es necesario realizar la inclusión en el disco duro. Si selecciona la inclusión en el disco duro, los datos se cifrarán usando una clave de software. La verificación biométrica se puede realizar usando cualquier lector de huellas digitales.

Importante: Una vez escogido el tipo de inclusión, no se puede cambiar más adelante. La única manera de cambiarlo es desinstalar Protector Suite QL y reinstalarlo de nuevo.

---

6 *Introduzca su nombre de usuario, contraseña y dominio (si procede) y haga clic en **Siguiente**.*



7 *Haga clic en **Siguiente** para proseguir con el tutorial de huellas digitales. O desactive la casilla de verificación **Ejecute el tutorial interactivo** y haga clic en **Siguiente** para ignorar el tutorial (consulte “Tutorial de huellas digitales” en la página 20 para obtener instrucciones sobre el tutorial).*

8 *Haga clic en la casilla de encima del dedo que desea incluir. Cree tres*

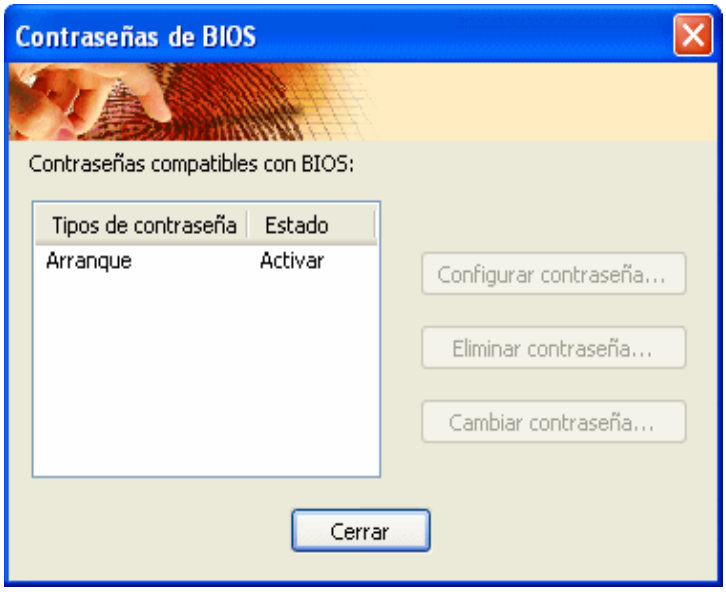
muestras de su dedo según las instrucciones del tutorial (consulte la página "Tutorial de huellas digitales" en la página 20). Estas muestras se combinarán en un único pasaporte de huellas digitales. Si las tres muestras creadas no coinciden, aparece una advertencia.

9 *(Opcional) Si se seleccionó la inclusión en el dispositivo y la configuración del sistema admite encendido seguro, también se utilizarán todas las huellas digitales incluidas para el encendido seguro.*

10 *(Opcional) Si se seleccionó la inclusión en el disco duro y la configuración del sistema admite encendido seguro, también se utilizarán todas las huellas digitales incluidas para el encendido seguro.*

Como la memoria del dispositivo es limitada, el número máximo de huellas digitales que se pueden almacenar es 21. Si algunas de las huellas digitales incluidas en los pasaportes no se asignan al encendido seguro del dispositivo (por ejemplo otro dispositivo está conectado), aparece el botón ***Encendido*** *encima de cada dedo. El botón Encendido aparece "minimizado" por defecto. Se utilizará el dedo correspondiente para el encendido seguro. Si no desea utilizar un dedo para el encendido seguro, sino sólo para el inicio de sesión, haga clic en el botón Encendido para eliminarlo de la memoria del dispositivo.*

11 *(Opcional) Si la BIOS del ordenador admite contraseñas seguras de BIOS, se mostrará una pantalla de* ***Encendido seguro****. Seleccione las contraseñas que se sustituirán por huellas digitales. (Se le pedirá que introduzca la contraseña después de seleccionarla).*
Los administradores locales también pueden administrar contraseñas de BIOS desde aquí. Al hacer clic en el botón ***Administrar pasaporte****, se abre el cuadro de diálogo* ***Contraseñas de BIOS****, en el que se pueden establecer o modificar dichas contraseñas.*



12 *Seleccione otro dedo que desee incluir. Puede incluir un máximo de 10 huellas digitales.* ***Es muy recomendable que incluya más de un dedo en caso de que se produzca una herida.*** *Haga clic en* ***Siguiente*** *cuando haya terminado.*

13 *Algunas configuraciones de hardware proporcionan seguridad de datos adicional mediante cifrado. En estas configuraciones, aparece un cuadro de diálogo adicional con un tipo de seguridad avanzado.*

- *Seleccione* ***Activar Seguridad avanzada para el usuario actual*** *para permitir el cifrado adicional, por ejemplo TPM.*
- *Defina el tipo* ***Seguridad avanzada****. Consulte “Seguridad avanzada” en la página 23 para obtener más información).*
- *Cree una contraseña de respaldo. Ésta puede utilizarse en caso de fallo de hardware del sensor para omitir la autenticación de huellas digitales.*

14 *En el caso de los dedos agregados para el encendido seguro, debe realizar las operaciones descritas en la página de finalización:*

- *Apague el equipo.*
- *Encienda el equipo.*

15 *Pase el dedo cuando se le indique. Cuando haya terminado, haga clic en* ***Finalizar.***

16 *Después de finalizar el asistente de inclusión, aparece una pantalla de* ***Introducción*** *que muestra los modos posibles de usar huellas digitales en Protector Suite QL*

Una vez que haya incluido las huella digitales, podrá usar su dedo:

- *para tener acceso a la cuenta del equipo,*
- *para ver el Biomenú con todas sus funciones, (bloqueo de equipo, registro de páginas, cuadros de diálogo, etc.) Puede navegar por el Biomenú moviendo el dedo por el sensorr,*
- *para rellenar los formularios Web o cuadros de diálogo registrados,*
- *para iniciar sus aplicaciones favoritas.*

Nota: Cada usuario de Windows sólo puede tener un pasaporte. Para crear una cuenta de usuario, seleccione **Inicio** > **Panel de control** y haga clic en **Cuentas de usuario**. Siga las instrucciones que aparecerán en pantalla.

Tutorial de huellas digitales

Es muy recomendable que siga el Tutorial de huellas digitales. El tutorial incluye un breve vídeo que muestra ejemplos de escaneado de huellas digitales correcto e incorrecto. A continuación, pruebe crear sus primeras muestras de huella digital.

Para ejecutar el tutorial:

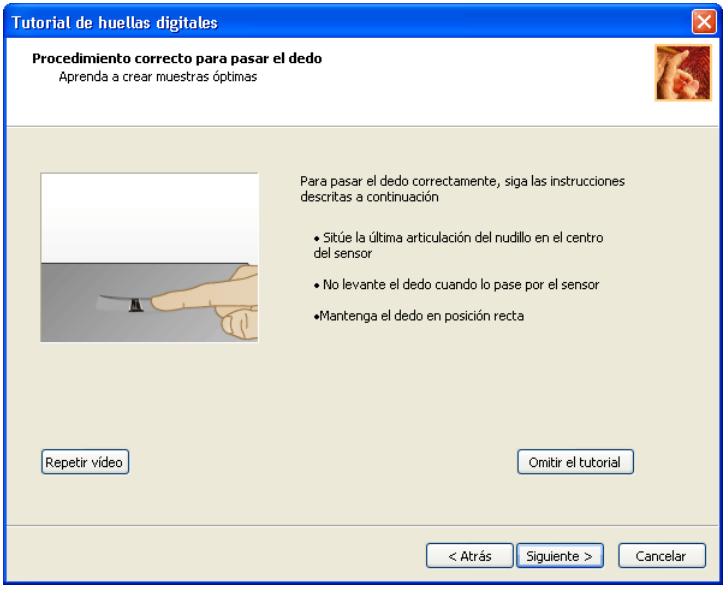
1 *Para iniciar el tutorial vaya a* **Inicio > Todos los programas >** ***Protector Suite QL*** **> Tutorial de huellas digitales.**

o ejecútelo desde el asistente para inclusión de huellas digitales

o seleccione ***Ayuda > Tutorial*** *en el cuadro de diálogo* ***Centro de control****.*

2 *La primera página explica el objetivo de este tutorial.*

3 *La siguiente página explica el procedimiento correcto de escaneado y muestra un breve vídeo de demostración.*



- *Sitúe la última articulación sobre el sensor.*
- *Mantenga el dedo en contacto con el sensor mientras lo desliza hacia usted en línea recta.*
- *Mantenga el dedo en horizontal.*

4 *En la página siguiente, pruebe a crear cuatro muestras de su huella digital. Si las muestras no coinciden, recomendamos que haga clic en el botón* ***Intentar de nuevo*** *para repetir el escaneado. Use el botón* ***Repetir***

vídeo *para repetir la demostración en vídeo. Una vez que haya creado las muestras correctamente, haga clic en* ***Finalizar*** *para cerrar el tutorial y volver al asistente de inclusión.*

Nota: Se agota el tiempo de espera de las operaciones biométricas (inclusión, verificación, tutorial) transcurridos 2 minutos de inactividad para ahorrar energía. En caso de que se agote el tiempo, simplemente reinicie el proceso

Seguridad avanzada

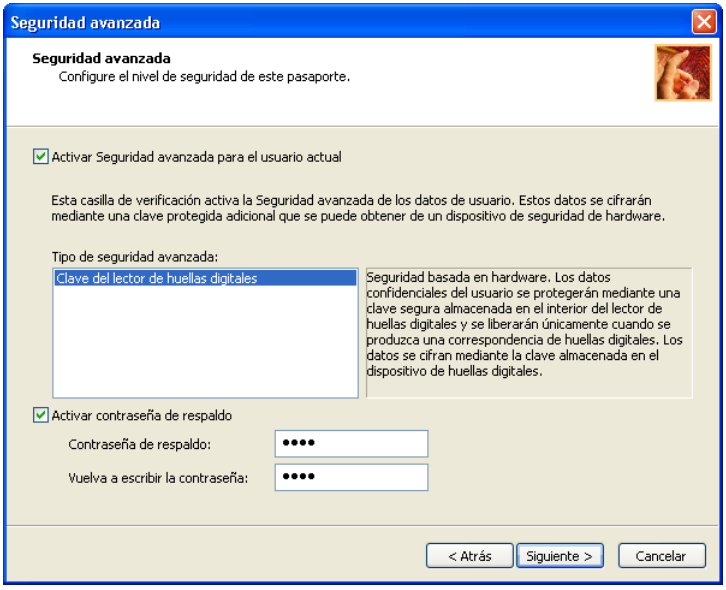
Para mejorar la seguridad de Protector Suite QL, utilice el cifrado adicional. Los posibles tipos de cifrado disponibles dependerán del hardware empleado. La seguridad avanzada la puede habilitar (o deshabilitar más adelante) cada usuario al final del asistente para la edición e inclusión de huellas digitales. El tipo de cifrado se puede cambiar utilizando este cuadro de diálogo para ajustar el nivel necesario de seguridad y comodidad para el usuario.

Para activar la seguridad avanzada (opcional):

1. *Vaya a **Inicio > Todos los programas > Protector Suite QL > Inclusión del usuario***

   Para iniciar el Asistente para la inclusión:
2. *En el cuadro de diálogo **Seguridad avanzada** después de la inclusión, seleccione **Activar Seguridad avanzada** para activarla para el usuario actual.*
3. *Defina el **tipo de seguridad avanzada.***

.



- ***Clave de lector de huellas digitales con TPM -*** *proporciona seguridad basada en hardware mejorada. El canal de cifrado entre el chip de seguridad TPM y el lector de huellas digitales mejora aún más la seguridad de los datos confidenciales del usuario. Recomendado para una mayor seguridad.*
- ***Clave de lector de huellas digitales -*** *proporciona seguridad basada en hardware. Los datos confidenciales del usuario se protegerán mediante una clave segura almacenada en el interior del lector de huellas digitales y que se liberará únicamente cuando se produzca una correspondencia digital. Los datos se cifran mediante la clave almacenada en el dispositivo de huellas digitales.*
- ***Clave de TPM con PIN -*** *los datos cifrados del usuario estarán protegidos con el chip de seguridad TPM con PIN. Requiere que el usuario introduzca un PIN en cada verificación de identidad. Recomendado para una mayor seguridad.*
- ***Clave de TPM con PIN -*** *los datos confidenciales del usuario se protegerán mediante el chip de seguridad TPM. Recomendado para mayor comodidad.*

4 *Defina la contraseña de respaldo. Esta contraseña de respaldo se puede usar en caso de un fallo de hardware para omitir la autenticación de huellas. Le recomendamos que utilice una contraseña compleja. Si no define la contraseña de respaldo, puede perder datos en caso de que se produzca un error en el hardware de autenticación.*

Inicio de sesión mediante huellas digitales

Para activarlo, debe incluir sus huellas digitales (consulte “Inclusión de huellas digitales” en la página 14). Durante la inclusión del usuario, se escanean muestras de huellas digitales y se crea una conexión entre la cuenta de usuario de Windows y estas muestras. Tras reiniciar el equipo, si desea iniciar sesión de nuevo, el cuadro de diálogo de inicio de sesión le solicitará que pase el dedo por el sensor o pulse **Ctrl + Alt + Supr** para iniciar sesión utilizando la contraseña de Windows. Una vez que ha pasado el dedo, la huella digital incluida es reconocida y ya puede iniciar sesión.

El inicio de sesión biométrico también protege el salvapantallas y el modo de reactivación de las funciones de ahorro de energía (deben establecerse en el equipo la salida del salvapantallas protegido por contraseña y el modo en espera. Vaya a **Inicio > Panel de control**, haga clic en **Mostrar** y seleccione la pestaña **Salvapantallas** para establecer el salvapantallas.)

Para deshabilitar el inicio de sesión mediante huellas digitales:

- *Seleccione* ***Inicio*** > ***Todos los programas*** > ***Protector Suite QL*** > ***Centro de control***

  o pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***
- *Seleccione****Configuración del sistema > Inicio de sesión***
- *Seleccione el botón de opción Estándar de Windows. Se deshabilitará el inicio de sesión mediante huellas digitales e iniciará sesión en el sistema utilizando el inicio de sesión estándar de Windows.*

Para habilitar Inicio de sesión de huellas digitales:

- *Seleccione* ***Inicio*** > ***Todos los programas*** > ***Protector Suite QL*** > ***Centro de control***

  o pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***
- *Seleccione* ***Configuración > Configuración del sistema > Inicio de sesión***
- *Seleccione el botón de opción Inicio de sesión mediante huellas digitales y ahora estará habilitado el inicio de sesión del sistema mediante huellas digitales en lugar de la contraseña de Windows.*

Para obtener más información sobre las configuraciones del inicio de sesión, consulte el Capítulo 4, Centro de control, “Inicio de sesión” en la página 58.

Nota: Debe crear una contraseña de Windows para proteger su equipo. Si no se crea una contraseña de Windows, Protector Suite QL no puede acceder de forma segura al ordenador.

Protector Suite QL también coopera con el inicio de sesión de la red Novell. Para que Protector Suite QLinicie una sesión automáticamente en una red Novell, su nombre de usuario y contraseña de Windows deben coincidir con su nombre de usuario y contraseña de Novell. Los siguientes clientes de Novell no funcionan con Protector Suite QL: 4.83, 4.90.

Cambio rápido de usuario

La función Cambio rápido de usuario de Windows también es compatible. Si el usuario A inicia sesión y el usuario B (ya incluido) pone un dedo en el sensor, reconoce las huellas digitales e intercambia los usuarios.Protector Suite QL

Para activar el Cambio rápido de usuario:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***
2. *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
3. *Seleccione **Configuración** > **Configuración del sistema***
4. *Seleccione la pestaña **Inicio de sesión**.*
5. *Seleccione la opción **Compatibilidad con activar cambio rápido de usuario (CRU)** Si está opcion no está visible, el sistema no es compatible con CRU (por ejemplo, su equipo es miembro de un dominio. Para activar Cambio rápido de usuario, tendrá que quitar al equipo del dominio.).*

Para quitar a un equipo de un dominio:

1. *Haga clic con el botón derecho en **Mi PC**(**PC** en Windows Vista) en el escritorio o en el menú **Iniciar** y seleccione **Propiedades***
2. *En Windows Vista haga clic en el enlace **Cambiar configuración** y autorícese como administrador.*
3. *Seleccione la pestaña **Nombre del equipo***
4. *Haga clic en **Cambiar** (o **Renombrar**) y seleccione **Grupo de trabajo** en el panel **Miembro de**.*

Nota: Sólo el administrador puede quitar a un equipo del dominio.

Cambiar contraseña de Windows (Restablecer)

La contraseña de inicio de sesión de Windows puede ser cambiada tanto por un usuario (mediante el Panel de control o Ctrl+Alt+Supr) como por un administrador (mediante el restablecimiento de contraseña). No hay diferencias entre ambos tipos de cambio de contraseña con respecto a Protector Suite QL. Las situaciones varían según el tipo de cuenta de usuario que se utiliza y el modo en que el usuario inicia sesión en el equipo.

Esto es aplicable a Windows 2000 y XP (en Windows Vista la funcionalidad es similar pero la Interfaz gráfica de usuario se muestra diferente).

Cuando se utiliza una cuenta de usuario local en un equipo de un grupo de trabajo o en un dominio, existen dos posibles situaciones:

1 *Un usuario inicia sesión utilizando el nombre de usuario y la contraseña de Windows y, posteriormente, la contraseña es cambiada.*

• el usuario bloquea el equipo o cierra sesión.

• el usuario pasa una huella digital incluida.

• aparece una advertencia diciendo que se ha utilizado una contraseña o un nombre de usuario incorrecto.

• el usuario debe escribir la nueva contraseña. esta contraseña se guarda en el pasaporte de las huellas digitales, el pasaporte se actualiza y el usuario inicia sesión en el equipo. el proceso de inicio de sesión mediante huellas digitales será como de costumbre la próxima vez.

2 *Un usuario inicia sesión utilizando una huella digital incluida y, posteriormente, la contraseña es cambiada.*

• la contraseña se guarda en el pasaporte de las huellas digitales. No es necesario volver a escribir la nueva contraseña posteriormente.

• el usuario bloquea o cierra sesión

• el usuario pasa la huella digital incluida

• el equipo se desbloquea o el usuario inicia sesión

Cuando se utiliza una cuenta de usuario de dominio en un domininio:

El usuario inicia sesión utilizando la contraseña y el nombre de usuario de Windows o una huella digital incluida. A continuación se cambia la contraseña.

• El usuario bloquea el equipo o cierra sesión.

• el usuario pasa una huella digital incluida.

• aparece una advertencia diciendo que se ha utilizado una contraseña o un nombre de usuario incorrecto.

• el usuario debe escribir la nueva contraseña. esta contraseña se guarda en el pasaporte de las huellas digitales, el pasaporte se actualiza y el usuario inicia sesión en el equipo. el proceso de inicio de sesión mediante huellas digitales será como de costumbre la próxima vez.

Casos especiales:

Se establece "El usuario debe cambiar la contraseña en el próximo inicio de sesión" o se define la caducidad de la contraseña en el dominio.

- *En un equipo cliente un usuario inicia sesión utilizando la huella digital incluida.*
- *Aparecerá un cuadro de diálogo solicitando al usuario que cambie la contraseña. Esta contraseña se guarda en el pasaporte de las huellas digitales, el pasaporte se actualiza y el usuario inicia sesión en el equipo. el proceso de inicio de sesión mediante huellas digitales será como de costumbre la próxima vez.*

Banco de contraseñas

El Banco de contraseñas es una función opcional de Protector Suite QL. Una vez instalado, éste guarda registros (nombres y contraseñas de usuario y otras configuraciones) de los sitios Web y cuadros de diálogo de aplicaciones para que pueda acceder a los sitios Web y aplicaciones que visita con más frecuencia (webmail, cuentas bancarias, ecommerce, etc.) con seguridad, sin la molestia de tener que volver a introducir nombres de usuario, contraseñas y datos de formulario. Se introduce la información necesaria sólo una vez, durante el registro del cuadro de diálogo o página Web. Cuando la ventana aparece de nuevo, puede introducir todos los datos mediante el sensor. También se puede acceder a los sitios web directamente desde el Biomenú.

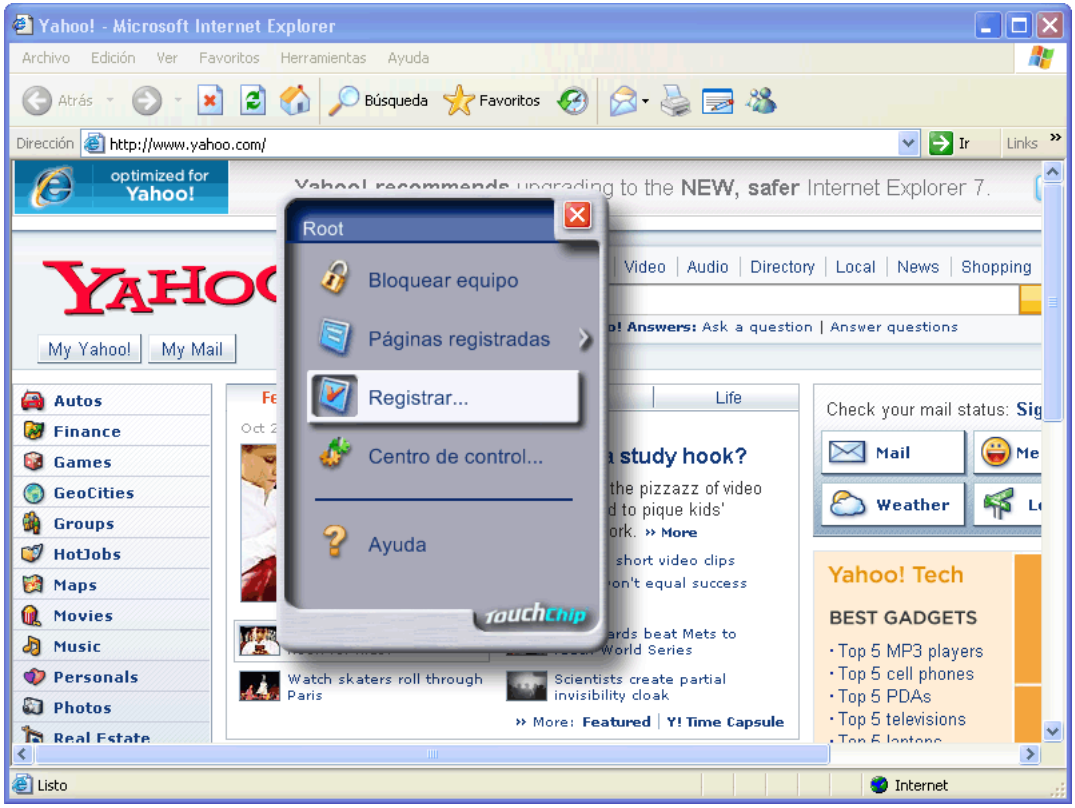
El Banco de contraseñas es compatible con los siguientes exploradores: Internet Explorer 5.0 y superior, Firefox 1.0 - 1.5. La compatibilidad para Internet Explorer se instala automáticamente. Cuando Protector Suite detecta Firefox, le pregunta al usuario si desea activar la compatibilidad. También se puede activar la compatibilidad de Firefox desde **Centro de control** > **Configuración** > **Configuración de usuario** > **Banco de contraseñas**. Si desea activar la asistencia del Banco de contraseñas para un explorador, marque la casilla de verificación correspondiente. (Sólo los administradores locales pueden ver esta opción y habilitar más navegadores.)

Registro de páginas Web y cuadros de diálogo

Debe registrar un sitio Web o cuadro de diálogo para guardar registros (nombres y contraseñas de usuario y otras configuraciones) de los sitios Web y cuadros de diálogo de contraseñas para poder repetirlos más tarde, es decir, completar la información después de pasar el dedo por el sensor.

Para crear un nuevo registro:

1. *Active una página Web o el cuadro de diálogo que desea registrar.*
2. *Complete los campos de nombre de usuario, contraseña y otros que sean necesarios.*
3. *Pase el dedo incluido para mostrar el **Biomenú**.*
4. *Seleccione **Registrar...***



Se almacenarán todos sus datos. Una vez creado un registro, aparece una indicación en la esquina del explorador confirmándole que el registro se ha creado. (Consulte “Activar o desactivar indicaciones en el Banco de contraseñas” en la página 35 cómo activar o desactivar indicaciones). Haga clic en **Editar** para editar los detalles del registro directamente en este cuadro de diálogo de indicación.

Repetición de registros

Al repetir un registro se inicia el sitio Web registrado y se inicia sesión automáticamente usando las credenciales registradas.

Para repetir un registro:

1. *Muestre el cuadro de diálogo o sitio Web registrado.*
2. *Pase el dedo sobre el sensor.*
3. *(opcional) Si aparece la indicación de repetición de cuadros de diálogo, confirme que desea repetir el registro.*
4. *Se repite el registro.*

Para iniciar un sitio Web registrado, también puede usar el Biomenú.

- *Pase el dedo incluido para mostrar el **Biomenú.***
- *Seleccione **Sitios registrados.** Aparece una lista de sitios registrados.*
- *Haga clic en el sitio que desea iniciar en el explorador y el registro se repetirá, o haga clic en **Atrás** para volver al **Biomenú**..*

Registro de sitios Web y cuadros de diálogo con varios formularios

Registro de sitios Web con varios formularios

El Banco de contraseñas registra formularios individuales. Si un sitio contiene diversos formularios, cada uno debe registrarse por separado. Esto significa que sólo se registra un formulario que está activo.

Para registrar un formulario en una página en la que ya exista un registro (una página con varios formularios), mantenga pulsada la tecla **Mayús** y pase el dedo para ver el **Biomenú**. (Si la página ya está registrada y pasa el dedo sin mantener pulsada la tecla **Mayús**, el registro existente se repetirá.)

- *Un formulario activo está registrado.*
- *Si ningún formulario está activo y utiliza Internet Explorer 5.5 o superior, se solicitará al usuario que seleccione un formulario para el registro.*
- *Si nada de lo anterior ocurre, no se producirá ninguna acción.*

Situaciones de ejemplo:

Supongamos que no existe ningún registro para esta página. La página contiene el formulario A y el formulario B.

A. Acaba de cumplimentar el formulario A y dicho formulario todavía está activo. Pase el dedo por el sensor. El formulario A está registrado.

B. Acaba de cumplimentar el formulario A y pasa al formulario B, de manera que el formulario B está activo. Pase el dedo por el sensor. El formulario B está registrado (aunque todavía está vacío).

C. Acaba de cumplimentar el formulario A y hace clic fuera del formulario de forma que ningún formulario está activo. Está utilizando Internet Explorer 5.5 o superior. Pase el dedo por el sensor. Se le solicitará que seleccione el formulario de destino para el registro.

D. Acaba de cumplimentar el formulario A y hace clic fuera del formulario de forma que ningún formulario está activo, pero está utilizando una versión de IE anterior. No se producirá ninguna acción.

Repetición de registros de sitios Web con varios formularios :

Un registro existente se repite de forma automática si visualiza la página desde **Biomenú > Sitios registrados**. Si visualizó la página de forma manual y ahora desea repetir el registro, pase el dedo por el sensor.

- *Si sólo existe un registro para la página (independientemente del número total de formularios existentes), se repite el registro.*
- *Si existen varios formularios registrados y uno de ellos está activo, se repite dicho formulario.*
- *Si no hay formularios activos, todos los registros existentes de la página están disponibles para su repetición.*

Registrar y repetir cuadros de diálogo complejos

El Banco de contraseñas está principalmente pensado para el registro de cuadros de diálogo sencillos que contengan un campo de nombre de usuario y contraseña, que son los cuadros de diálogo típicos para iniciar una sesión en varias aplicaciones.

Quizás no sea compatible con cuadros de diálogo más complejos. Los campos de texto y los de contraseña se pueden registrar siempre. Los registros guardan controles que no está ocultos, desactivados, minimizados, etc. Los botones de opción, casillas de verificación, cuadros combinados y selecciones en cuadros de lista se registran para aplicaciones que utilizan controles estándar de Windows (por ejemplo cuadros de diálogo del sistema). Toda la información registrada se puede editar (por ejemplo, cuando se realizar un cambio forzado de contraseña).

Es posible que experimente problemas con los diálogos que contengan varias páginas. En algunos casos, todas las páginas se registran en un solo registro. El Banco de contraseñas no puede administrar correctamente los diálogos que no crean controles antes de utilizarse, sino que sólo los muestran. El ejemplo típico son algunos cuadros de diálogo de Microsoft Office.

Cuando repita un cuadro de diálogo registrado, si algún cambio de control invoca una acción que requiera la reacción del usuario, el Banco de contraseñas esperará (con el cuadro de diálogo) y la repetición solo se completará una vez finalizada la acción.

Administración de registros

A veces es útil editar un registro existente - por ejemplo, si cambia el domicilio de su empresa y desea actualizar sus registros. También puede eliminar su registro o activar o desactivar el envío automático de registros repetidos. Puede exportar su registro, por ejemplo, para que sea utilizado en otro equipo. Un registro exportado es un archivo con una extensión ***.pb** y puede ser importado posteriormente.

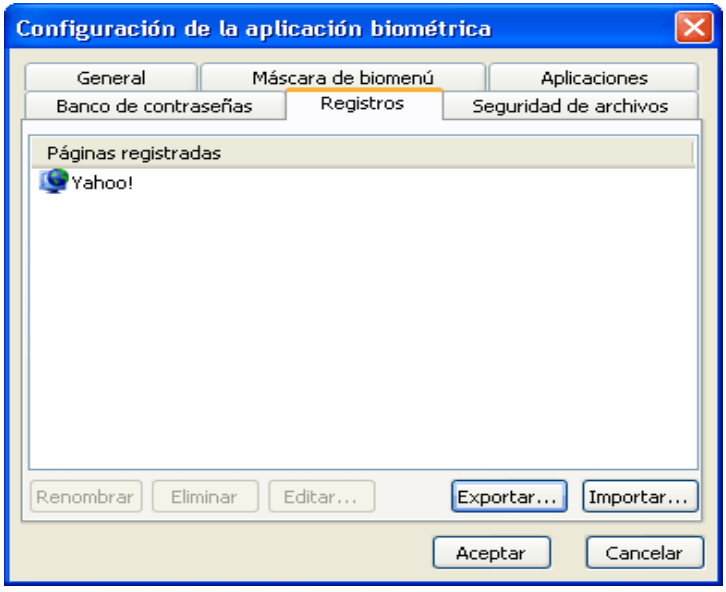
Para administrar registros:

1 *Haga clic en **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

Pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***

2 *Seleccione* ***Configuración > Configuración de usuario****. Seleccione* ***Configuración > Configuración de usuario****. Es necesario autentificación. Pase el dedo por el sensor de huellas digitales cuando se le solicite.*

3 *Seleccione la pestaña* ***Registros****.*



4 *Seleccione un registro con el que desee trabajar.*

• Haga clic en el botón ***Renombrar*** *para cambiar el nombre predeterminado almacenado con su registro. El nombre que escriba es sólo una descripción que aparecerá en el* ***Biomenú****, no afecta a la información guardada con el registro.*

• Haga clic en el botón ***Eliminar*** *para eliminar el registro.*

• Haga clic en el botón ***Editar*** *para cambiar los detalles del registro almacenado (por ejemplo, su nombre de usuario o contraseña han cambiado y desea reflejar esto en el registro existente). La casilla de verificación* ***Enviar formulario automáticamente*** *controla el envío automático del formulario después de reproducir los datos almacenados en el registro. Si la selecciona, el registro se repetirá automáticamente*

después de pasar el dedo. Si no la selecciona, aparece un cuadro de diálogo solicitándole confirmación de la repetición. Esto ocurre cada vez que accede al sitio o cuadro de diálogo registrado.

*• Haga clic en el botón **Exportar** para exportar su registro, por ejemplo, para usarlo en otro equipo. O bien, seleccione los registros que desea exportar o todos los registros existentes se exportarán automáticamente. Para seleccionar más registros, mantenga pulsada la tecla **Ctrl** o **Mayús** cuando seleccione registros. A continuación, seleccione un archivo de destino e introduzca una contraseña. Esta contraseña se solicitará al importar estos registros. La extensión de archivo del Banco de contraseñas es ***.pb**.*

*• Haga clic en el botón **Importar** para importar registros de un archivo de Banco de contraseñas. Seleccione el archivo ***.pb** de fuente. Si alguno de los registros que está importando ya existe, elija si desea sobrescribir los existentes con los importados o bien agregar los importados a la lista de registros. (Si mantiene los registros e importa registros con los mismos nombres, los nuevos registros del archivo ***.pb** se indicarán con un número después del nombre del registro.) Introduzca la contraseña creada durante la exportación.*

Activar o desactivar indicaciones en el Banco de contraseñas

El Banco de contraseñas muestra indicaciones al usuario siempre que pueda realizar alguna acción: registrar un cuadro de diálogo, repetir un cuadro de diálogo, etc. Estas indicaciones se pueden activar o desactivar en la opción **Configuración de usuario** Si el usuario inicia sesión en Windows usando un nombre de usuario y una contraseña, las indicaciones no están activas hasta que se realice una correcta verificación de las huellas digitales.

Para activar/desactivar indicaciones:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Seleccione **Configuración > Configuración de usuario**. Es necesario autentificación. Pase el dedo por el sensor de huellas digitales cuando se le solicite.*
3. *Seleccione **Banco de contraseñas**.*
4. *Seleccione las indicaciones que quiere que aparezcan.*

• ***Enviarme una alerta cuando se repita el registro:*** *este aviso informa al usuario que la repetición del registro está por comenzar. Este aviso es útil en los casos en los que desee crear más registros del mismo formulario o cuadro de diálogo y no desee sobrescribir los datos ya introducidos.*

• ***Enviarme una alerta cuando se haya creado un registro:*** *este aviso informa al usuario que el registro se creó satisfactoriamente. Haga clic en* ***Editar*** *para editar el registro directamente en este cuadro de diálogo de indicación.*

• ***Enviarme una alerta cuando se modifique el campo de clave de acceso:*** *este aviso informa al usuario que el campo de clave de acceso se activará de manera legible.*

• ***Enviarme una alerta si el cuadro de diálogo puede repetirse:*** *este aviso informa al usuario que se puede repetir el registro.*

• ***Enviarme una alerta si un cuadro de diálogo es adecuado para el registro:*** *este aviso informa al usuario de que el cuadro de diálogo contiene un campo de contraseña que se puede registrar.*

• ***Enviarme una alerta si el cuadro de diálogo puede repetirse:*** *este aviso informa al usuario que se puede repetir el registro.*

• ***Enviarme una alerta si una página de Internet es adecuada para el registro:*** *este aviso informa al usuario de que la página contiene un campo de contraseña que se puede registrar.*

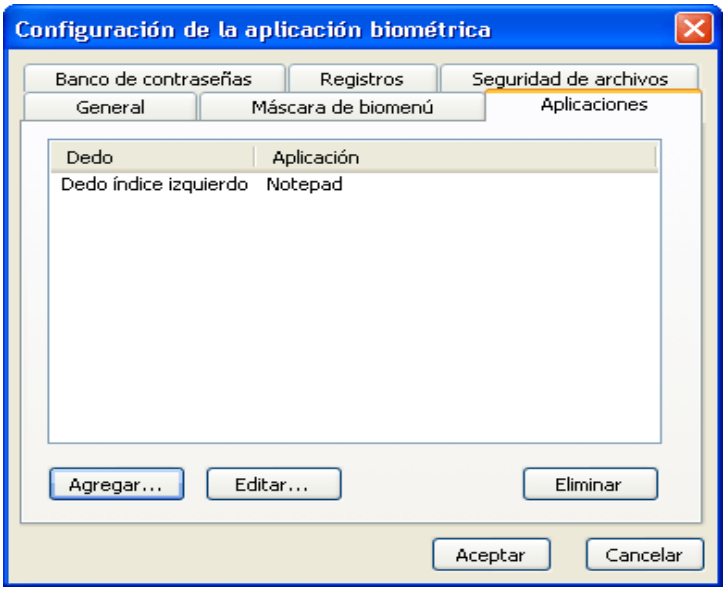
Iniciador de aplicaciones

El Iniciador de aplicaciones es una función opcional de Protector Suite QL.

Una vez instalado, le permite iniciar aplicaciones registradas con sólo pasar el dedo por el sensor.

Debe quedar sin asignar al menos un dedo incluido para mostrar el Biomenú. El número máximo de aplicaciones que puede iniciar de esta manera es igual al número de dedos incluidos - 1.

Si desea anular el inicio de la aplicación (e invocar el **Biomenú** en su lugar), mantenga pulsada la tecla **Mayús** al pasar el dedo.



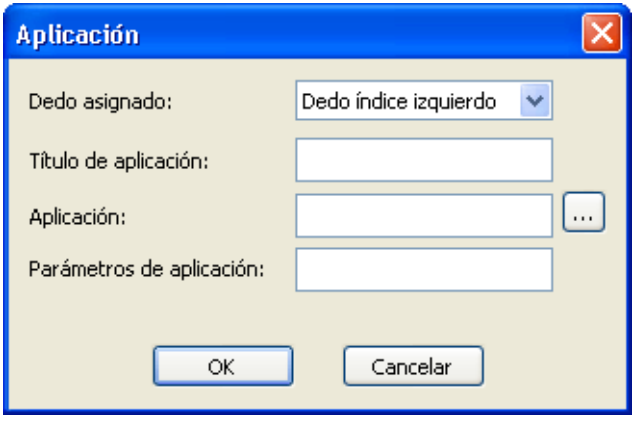
Para crear la asociación entre un dedo incluido y una aplicación:

1. *Haga clic en **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Seleccione **Configuración > Configuración de usuario**. Es necesario autentificación. Pase el dedo sobre el sensor de huellas digitales cuando se lo solicite.*
3. *Seleccione la pestaña **Aplicaciones**.*
4. *Haga clic en el botón **Agregar**. Se abrirá el cuadro de diálogo **Aplicación**.*
5. *Seleccione un dedo incluido que esté libre. Aparece un cuadro de diálogo solicitándole incluir más dedos si ninguno está disponible.*
6. *Escriba el nombre de la aplicación. (Este nombre se muestra en el cuadro de diálogo **Aplicaciones** de **Configuración de usuario**.)*
7. *Localice el archivo que desee ejecutar. Puede ser cualquier archivo ejecutable (por ejemplo Iexplorer.exe).*
8. *Opcionalmente, los parámetros adicionales se pueden introducir en el campo Parámetros de la aplicación. Si no está seguro, deje este campo vacío. Consulte abajo ejemplos de parámetros de la aplicación.*
9. *Haga clic en **Aceptar**.*

Ejemplos de parámetros de la aplicación

- *Se puede abrir un sitio web al iniciar un explorador Web como por ejemplo Internet Explorer. Escriba una dirección de sitio web (por ejemplo www.upek.com) en el campo Parámetros de la aplicación y se iniciará el sitio web cada vez que pase su dedo asignado e inicie el explorador.*



- *Un archivo se puede abrir con una aplicación como Microsoft Word. Escriba una ruta al archivo entre comillas (por ejemplo "C:\Documents and Settings\your.account\Mis documentos\document.doc"). El archivo document.doc se abrirá con Word cada vez que pase su dedo. Se puede utilizar más de un parámetro para una aplicación.*

Para editar la combinación de huella y aplicación más adelante:

1. *Seleccione una aplicación en el cuadro de diálogo **Aplicaciones.***
2. *Haga clic en el botón **Editar.***
3. *Haga los cambios necesarios en la pestaña **Aplicación**.*
4. *Haga clic en **Aceptar**.*

Para borrar la combinación de huella y aplicación:

1. *Seleccione una aplicación en el cuadro de diálogo **Aplicaciones.***
2. *Haga clic en el botón **Eliminar**.*

Los cambios realizados en la pestaña **Aplicaciones** sólo se guardan cuando hace clic en **Aceptar** en el cuadro de diálogo **Configuración de usuario**.

Seguridad de archivos

Seguridad de archivos es una función opcional de Protector Suite QL.

Le permite guardar los archivos en un archivo cifrado en su disco duro. Los archivos cifrados pueden contener archivos o carpetas y están protegidos con la verificación mediante huellas digitales o una contraseña si la establece al crear un archivo. Si un archivo de seguridad de archivos está desbloqueado, puede trabajar con el archivo de archivos como si fuera una carpeta estándar (eliminar, copiar o renombrar archivos, etc.). También se puede utilizar la función arrastrar y colocar. Puede simplemente copiar y pegar o arrastrar los archivos al archivo desbloqueado y cuando lo bloquee de nuevo, los archivos estarán cifrados. Si sólo tiene un archivo cifrado en un archivo y está desbloqueado, haciendo clic en el archivo lo ejecutará. También puede compartir sus archivos cifrados con otros usuarios que tengan huellas digitales incluidas.

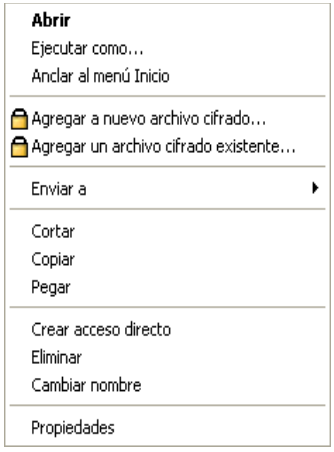
Cifrado de archivos (adición de archivos o carpetas a un archivo de seguridad de archivos)

Inicia sesión en el equipo y desea agregar archivos a un archivo cifrado.

Nota: Debe tener las huellas digitales incluidas antes de crear un archivo. De lo contrario, aparecerá la advertencia de que no hay ningún usuario seleccionado. Consulte Inclusión de huellas digitales para obtener información sobre cómo incluirlas.

Para agregar archivos o carpetas a un nuevo archivo de seguridad de archivos:

1. *Busque los archivos o carpetas que desea cifrar (utilizando el Explorador de Windows u otro cuadro de diálogo de Windows).*
2. *Seleccione los archivos o carpetas (utilizando el mouse y la tecla Mayús o Ctrl) y con el botón derecho haga clic para ver el menú contextual.*
3. *Seleccione **Agregar a nuevo archivo de cifrado.***



4 *Aparece un cuadro de diálogo pidiéndole que*

*• seleccione una carpeta de destino (haga clic en **...**para examinar y seleccione una carpeta)*

• Elija una contraseña. Consulte más a continuación.

*• **Avanzadas >>** Seleccione los usuarios que pueden tener acceso a los archivos cifrados.*

*• Pulse **Aceptar**. Se le solicitará que pase el dedo por el sensor para verificar su identidad.*

5 *Una vez cifrados los archivos, un cuadro de diálogo le solicitará que elija qué hacer con los archivos originales:*

*• **Mantener archivos originales** no eliminará los archivos originales, los cuales se guardarán tanto en el archivo cifrado como en el no cifrado en su ubicación original.*

*• **Eliminar archivos originales** eliminará los archivos originales y mantendrá los archivos sólo cifrados en el archivo.*

*• Seleccione **Limpiar los archivos antes de su eliminación** para sobrescribir los archivos que está eliminando con un contenido aleatorio y a continuación, elimínelos. Evitará que otra persona pueda recuperar los archivos eliminados.*

6 *Se ha creado el archivo cifrado (con una extensión ***.uea** o ***.ueaf** si sólo se ha cifrado un archivo).*

Tipos de contraseña:

- ***Sin contraseña de respaldo*** *protegerá el archivo mediante huellas digitales sólo. De esta manera no se puede acceder a los archivos guardados en el archivo de seguridad de archivos cuando la verificación de huellas digitales no es posible (en caso de heridas en los dedos, problemas en el dispositivo, etc.).*
- ***Usar contraseña de respaldo global*** *establecerá una contraseña global, es decir, una contraseña de respaldo que será común para todos los archivos. Esto es conveniente si desea evitar utilizar una contraseña diferente cada vez que cree un archivo. Si aún no ha establecido una contraseña de respaldo global, esta opción aparecerá atenuada. Aprenda cómo establecer o cambiar la contraseña de respaldo global en "Gestión de archivo de seguridad de archivos" en la página 47.*
- ***Usar la siguiente contraseña de respaldo*** *le permitirá crear una nueva contraseña para el archivo de seguridad de archivos actual.*

Se recomienda utilizar una contraseña de respaldo porque de lo contrario no podrá desbloquear los archivos cuando la verificación de huellas digitales no sea posible (en caso de heridas en los dedos, problemas en el dispositivo, etc.). Utilice una contraseña segura (es decir, ocho caracteres como mínimo, incluyendo caracteres no alfanuméricos, etc.).

En casos en que la verificación de huellas digitales no es posible, un cuadro de diálogo le pedirá una contraseña de respaldo. Puede forzar la aparición de este cuadro de diálogo y omitir la verificación mediante huellas digitales cerrando el cuadro de diálogo que le solicita pasar el dedo.

Nota: Si no establece una contraseña de respaldo y elimina las huellas digitales incluidas, no podrá abrir los archivos de seguridad de archivos bloqueados. Desbloquee los archivos de seguridad de archivos y mueva los archivos antes de eliminar las huellas digitales o establezca una contraseña de respaldo.

Para agregar archivos o carpetas a un archivo de seguridad de archivos:

1 *Busque los archivos o carpetas que desea cifrar (utilizando el Explorador de Windows u otro cuadro de diálogo de Windows).*

2 *Seleccione los archivos o carpetas (utilizando el mouse y la tecla Mayús o Ctrl) y con el botón derecho haga clic para ver el menú contextual.*

3 *Seleccione **Agregar a nuevo archivo de cifrado.***

4 *Examine y seleccione el archivo en el que desea guardar los archivos (el archivo tendrá la extensión ***.uea**).*

5 *Seleccione **Abrir**.*

6 *Pase el dedo sobre el sensor de huellas digitales cuando se lo solicite.*

7 *Una vez cifrados los archivos, un cuadro de diálogo le solicitará que elija qué hacer con los archivos originales:*

*• **Mantener archivos originales** no eliminará los archivos originales, los cuales se guardarán tanto en el archivo cifrado como en el no cifrado en su ubicación original.*

*• **Eliminar archivos originales** eliminará los archivos originales y mantendrá los archivos sólo cifrados en el archivo.*

*• Seleccione **Limpiar los archivos antes de su eliminación** para sobrescribir los archivos que está eliminando con un contenido aleatorio y a continuación, elimínelos. Esto evitará que otras personas recuperen los archivos eliminados. Los archivos ahora se agregan al archivo de seguridad de archivos.*

Bloqueo y desbloqueo de un archivo de seguridad de archivos

Inicia sesión en el equipo y desea bloquear o desbloquear el archivo de seguridad de archivos cifrado.

Si un archivo de seguridad de archivos está desbloqueado, puede trabajar con el archivo de archivos como si fuera una carpeta estándar (eliminar, copiar o renombrar archivos, etc.). También se puede utilizar la función arrastrar y colocar. Si sólo tiene un archivo cifrado en un archivo y está desbloqueado, haciendo clic en el archivo lo ejecutará. Desbloquéelo como un archivo de seguridad de archivos estándar.

Para desbloquear y abrir un archivo de seguridad de archivos:

1 *Seleccione el archivo de archivos **(*.uea o *.ueaf)** que desea abrir y haga clic con el botón derecho para ver el menú contextual.*

2 *Seleccione **Abrir** o **Desbloquear***

3 *Se le solicitará que pase el dedo o escriba una contraseña de respaldo para verificar su identidad. (Esto depende de las opciones que definió cuando creó el archivo.)*

4 *El archivo ahora está desbloqueado y puede trabajar con él como si se tratara de una carpeta estándar (eliminar, copiar o renombrar archivos etc.) o si es un archivo de archivo único (*.ueaf) el archivo del archivo se iniciará (por ejemplo un documento de texto se abrirá).*

Nota: Si hace doble clic en un archivo:

• si está bloqueado se le solicitará autorización (pasar el dedo, escribir contraseña) y, a continuación, desbloqueará y abrirá la carpeta de archivos.

• si ya está desbloqueado abrirá la carpeta de archivos.

• si sólo hay un archivo cifrado y bloqueado, solicitará autorización y, a continuación, ejecutará el archivo.

• si sólo hay un archivo cifrado y desbloqueado, ejecutará el archivo..

Para bloquear un archivo de seguridad de archivos:

1 *Seleccione un archivo de archivo desbloqueado **(*.uea** o ***.ueaf)** y haga clic con el botón derecho para ver el menú contextual.*

2 *Seleccione **Bloquear.** No es necesaria verificación alguna.*

3 *El archivo ahora está bloqueado.*

Para bloquear todos los archivos de seguridad de archivos:

1. *Pase el dedo por el sensor para abrir el **Biomenú.***
2. *Seleccione **Bloquear todos los archivos**. No es necesaria verificación alguna.*
3. *Todos los archivos desbloqueados están ahora bloqueados.*

Descifrado de archivos de un archivo de seguridad de archivos

Inicia sesión en el equipo y desea descifrar archivos o carpetas de un archivo de seguridad de archivos. Puede seleccionar el archivo de archivo de seguridad de archivos completo y descifrar todos los archivos, o seleccionar archivos diferentes del archivo y descifrarlos.

Para descifrar todos los archivos o carpetas de un archivo de seguridad de archivos al mismo tiempo

1. *Seleccione el archivo de archivos **(*.uea** o ***.ueaf)** que desea descifrar y haga clic con el botón derecho para ver el menú contextual.*
2. *Seleccione **Descifrar en...***
3. *Seleccione una ubicación de destino donde se guardarán los archivos descifrados.*
4. *Se le solicitará que pase el dedo o escriba una contraseña para verificar su identidad. (Esto depende de las opciones que definió cuando creó el archivo.)*
5. *Sus archivos ahora están descifrados en la ubicación de destino.*

Para cifrar archivos de nuevo o crear un nuevo archivo, consulte “Cifrado de archivos (adición de archivos o carpetas a un archivo de seguridad de archivos)” en la página 39.

Para descifrar archivos o carpetas seleccionados de un archivo de seguridad de archivos

1. *Seleccione el archivo de archivos **(*.uea)** que desea descifrar y ábralo (haga doble clic y si está bloqueado, verifíquese usted mismo).*
2. *Seleccione el archivo o archivos que desea descifrar (utilizando el mouse y la tecla **Mayús** o **Ctrl**) y con el botón derecho haga clic para ver el menú contextual.*

3 *Seleccione **Descifrar en...***

4 *Seleccione una ubicación de destino donde se guardarán los archivos descifrados.*

5 *Seleccione qué desea hacer con los archivos originales del archivo:*
***Eliminar archivos originales** - eliminará los archivos descifrados del archivo.*
***Mantener archivos originales** - se mantendrán los archivos en el archivo cifrado.*

6 *Sus archivos ahora están descifrados en la ubicación de destino.*
Para cifrar archivos de nuevo o crear un nuevo archivo, consulte “Cifrado de archivos (adición de archivos o carpetas a un archivo de seguridad de archivos)” en la página 39

Compartiendo acceso a archivo de seguridad de archivos

Los usuarios pueden compartir un archivo de seguridad de archivos. Cuando crea un archivo puede elegir los usuarios que podrán acceder al archivo compartido utilizando sus huellas digitales incluidas. A los usuarios se les puede otorgar (o denegar) el acceso más tarde en **Propiedades** de seguridad de archivos. Cualquier persona (no sólo los usuarios con derechos para compartir el archivo) puede acceder al archivo utilizando una contraseña de respaldo válida.

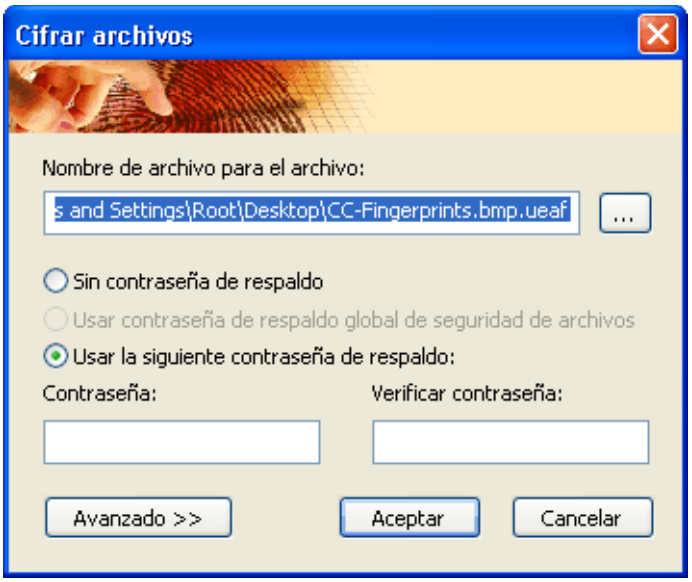
Importante: Todos los usuarios que comparten un archivo tienen los mismos derechos de acceso, incluyendo la capacidad de eliminar y agregar archivos, cambiar contraseña para acceder al archivo, o denegar el acceso a otros usuarios, etc.

Para conceder acceso a usuarios cuando crea un archivo

1 *Haga clic con el botón derecho en los archivos que desea cifrar y seleccione **Agregar a nuevo archivo cifrado** en el menú.*

2 *Establezca una contraseña de respaldo. Todos los usuarios utilizarán la misma contraseña de respaldo.*

3 *Haga clic en **Avanzado >>***



4 ***Aparecerá la ventana Cifrar para usuarios*** *con una lista de usuarios incluidos. Haga clic en los usuarios que compartirán el archivo.*

5 *Haga clic en* ***Aceptar****. Todos los usuarios seleccionados pueden desbloquear el archivo pasando el dedo por el sensor.*

Para conceder o denegar acceso a usuarios en Propiedades de seguridad de archivos:

1 *Seleccione un archivo de archivos* ***(*.uea*** *o* ****.ueaf)****.*

2 *Haga clic con el botón derecho para ver el menú contextual y seleccione* ***Propiedades.***

3 *Si el archivo está bloqueado, haga clic en* ***Desbloquear*** *para acceder a las opciones de Propiedades. Verifíquese con una huella digital o una contraseña de respaldo.*

4 *Aquí puede cambiar la contraseña del archivo. Esto cambiará la contraseña de todos los usuarios. En la ventana* ***Conceder acceso a usuarios*** *seleccione la persona o personas a las que desea conceder o denegar acceso. Todos los usuarios seleccionados pueden desbloquear el archivo pasando el dedo por el sensor.*

5 *Si desea bloquear el archivo, haga clic en* ***Bloquear.***

Si utiliza **Contraseña de respaldo global**, se establecerá la contraseña que se estableció en **Configuración de usuario** del usuario que creó el archivo. Cambiar esta contraseña no afecta al archivo de seguridad de archivos ya creado.

Si desea que otros usuarios puedan acceder a su seguridad de archivos, debe colocar el archivo de archivos en una carpeta compartida en su equipo.

Nota: Si un usuario que ha iniciado sesión desbloquea un archivo y, a continuación, intercambia usuarios sin cerrar sesión o reiniciar el equipo, el usuario que ahora inicie sesión no podrá acceder al archivo incluso si el acceso es compartido. Si desea compartir el archivo, bloquéelo antes de intercambiar usuarios.

Gestión de archivo de seguridad de archivos

Para acceder a las propiedades de archivo de seguridad de archivos

1. *Seleccione un archivo de archivos **(*.uea** o ***.ueaf)**.*
2. *Haga clic con el botón derecho para ver el menú contextual y seleccione **Propiedades.***
3. *Seleccione la pestaña **Seguridad de archivos**.*
4. *Si el archivo está bloqueado, haga clic en **Desbloquear** para acceder a las opciones de Propiedades. Verifíquese con una huella digital o una contraseña de respaldo.*

   Aquí puede cambiar el tipo de contraseña utilizada para el archivo y la concesión o denegación de acceso a otros usuarios.
5. *Haga clic en **Bloquear** para bloquear el archivo otra vez.*

Nota: El archivo debe ser desbloqueado para acceder a las propiedades. Si desea desbloquear el archivo, haga clic en Desbloquear en Propiedades o consulte Bloqueo/Desbloqueo de archivos.

Para cambiar la contraseña de respaldo de seguridad de archivos

1. *Seleccione un archivo de archivos **(*.uea** o ***.ueaf)**.*
2. *Haga clic con el botón derecho para ver el menú contextual y seleccione **Propiedades.***
3. *Seleccione la pestaña **Seguridad de archivos**.*

4 *Si el archivo está bloqueado, haga clic en* ***Desbloquear*** *para acceder a las opciones de Propiedades. Verifíquese con una huella digital o una contraseña de respaldo****.***

5 *Seleccione:*

• ***Borrar contraseña de respaldo*** *para eliminar la contraseña de respaldo.*

O

• ***Definir contraseña de respaldo*** *para definir una nueva contraseña o cambiarla si ya se ha definido. Seleccione****:***

- ***Usar contraseña de respaldo global*** *para utilizar una contraseña de respaldo que es común para todos los archivos que selecciona como protegidos por una contraseña de respaldo global. Esta contraseña se puede cambiar en Configuración de usuario.*
- ***Usar la siguiente contraseña de respaldo*** *para crear una nueva contraseña para el archivo.*

Importante: Esto cambiará la contraseña de respaldo para el archivo, es decir, para todos los usuarios que comparten el archivo. Cualquiera de los usuarios que tiene acceso al archivo puede cambiar la contraseña.

Para cambiar la contraseña de respaldo global en Configuración de usuario

1 *Haga clic en* ***Inicio*** > ***Todos los programas*** > ***Protector Suite QL*** > ***Centro de control***

o pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***

2 *Seleccione* ***Configuración > Configuración de usuario****. Seleccione* ***Configuración > Configuración de usuario****. Es necesario autentificación. Pase el dedo por el sensor de huellas digitales cuando se le solicite.*

3 *Seleccione la pestaña* ***Seguridad de archivos****.*

4 *Aquí puede cambiar o definir la **contraseña de respaldo global**. Esta contraseña es común a todos los archivos que selecciona como protegidos por la **contraseña de respaldo global** (cuando crea un archivo o en **Propiedades**).*

Cambiar esta contraseña no afecta a los archivos de seguridad de archivos ya creados. Los archivos que están actualmente bloqueados aún estarán protegidos por la contraseña antigua.

Capítulo 4
Gestión de Protector Suite QL

Existen tres maneras de gestionar las funciones y configuraciones de Protector Suite QL: mediante el cuadro de diálogo Centro de control , el icono de bandeja del sistema y el Biomenú (que aparece cuando pasa un dedo incluido por el sensor). Este capítulo le guiará a través de sus funciones.

Protector Suite QL También se puede acceder a sus funciones a través del menú **Inicio** de Windows. Seleccione **Inicio > Todos los programas > Protector Suite QL** para ver una lista de las funciones disponibles.

Centro de control

El Centro de control incluye varias funciones para la gestión de huellas digitales y la configuración del software de huellas digitales. Entre éstas se incluyen **Huellas digitales**, **Configuraciones** y **Ayuda**. Las opciones a las que se puede acceder dependen del estado del software, del hardware utilizado y de las aplicaciones instaladas.

Para ver Centro de control:

- *Seleccione **Inicio** >**Todos los programas** > **Protector Suite QL** > **Centro de control***
- *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
- *o haga clic con el botón derecho en el icono de bandeja y seleccione **Iniciar centro de control...***

Elevar privilegios administrativos para el usuario (para Windows Vista sólo).

Si desea acceder o hacer cambios en la configuración del sistema o gestionar y modificar las cuentas de otros usuarios (por ejemplo, poder incluir o eliminar huellas digitales de otros usuarios), debe ascender sus derechos administrativos, es decir, verificarse usted mismo como usuario autorizado.

1. *Haga clic en **Elevar privilegios administrativos para el usuario***
2. *Cuando aparezca el cuadro de diálogo Vista Control User Account introduzca sus credenciales para autenticarse en el sistema (o sólo permita que el programa continúe si ya ha iniciado sesión como administrador).*
3. *Volverá a aparecer el cuadro de diálogo Centro de control sin el icono de protección. Ahora están ascendidos sus derechos administrativos. Ahora puede acceder a **Configuración > Configuración del sistema** y hacer cambios.*

Debe repetir este procedimiento cada vez que ejecute el cuadro de diálogo Centro de control.

Huellas digitales

Puede incluir, editar y eliminar huellas digitales de los usuarios y, si está implementado el encendido seguro, gestionar huellas digitales presentes en la memoria del dispositivo. La lista de funciones a las que se puede acceder depende de la versión de Protector Suite QL instalada, el sensor de huellas digitales, los pasaportes y privilegios administrativos existentes del usuario actual.

Nota: Las funciones varían en función de los privilegios administrativos del usuario actual. En el Modo seguro, los usuarios definidos como administradores de huellas digitales (consulte “Modo de seguridad” en la página 62) pueden incluir o editar huellas digitales para todos los usuarios incluidos. En el Modo práctico, los usuarios pueden incluir o editar sólo sus propios pasaportes.

Incluir o editar huellas digitales

La inclusión es el proceso de creación de una correspondencia entre su nombre y contraseña de usuario y sus huellas digitales (computerizadas, de manera que resulte imposible reconstruir la imagen original), junto con claves de seguridad generadas automáticamente. Todos los datos se guardan en un pasaporte de huellas digitales de usuario.

Trás la inclusión, podrá usar sus huellas digitales en lugar de tener que escribir su nombre de usuario y contraseña.

Para incluir o editar un pasaporte (incluir o editar huellas digitales):

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

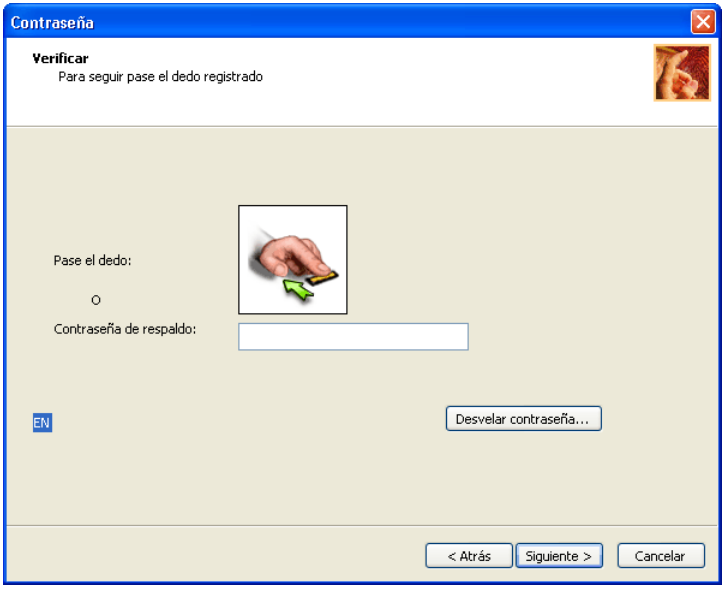
*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Haga clic en **Huellas digitales**.*

3 *Haga clic en **Incluir o editar huellas digitales**.*
*(Después de la instalación, pero antes de incluir al primer usuario, sólo se mostrará el asistente de **Inicializar** en esta sección. Una vez seleccionado el tipo de inclusión, el asistente de inclusión se inicia automáticamente.)*
*En el Modo seguro, (consulte “Modo de seguridad” en la página 62), el sistema muestra una lista de los pasaportes existentes. Seleccione el usuario y haga clic en el botón **Editar** para editar la huella digital de un usuario existente o haga clic en **Incluir** para incluir un nuevo usuario.*

4 *Aparece la pantalla **Asistente de inclusión**.*

5 *Pase el dedo por el sensor de huellas digitales o escriba la contraseña de respaldo de Windows/seguridad avanzada y haga clic en **Siguiente.***



6 *Realice una de las siguientes acciones:*

• Para incluir una nueva huella digital:
- Seleccione el dedo que desea incluir haciendo clic en el cuadro situado sobre el dedo.
- Pase el dedo seleccionado por el sensor de huellas digitales. Son necesarias tres imágenes correctas para incluir una huella digital (consulte Capítulo 3, “Inclusión de huellas digitales”, en la página 14 para obtener más información).

• Para eliminar una huella digital:
- Seleccione el dedo que desea eliminar haciendo clic en el cuadro situado sobre el dedo.
*- Haga clic en **Aceptar**.*

7 *(Opcional) Si se seleccionó la inclusión en el dispositivo y la configuración del sistema admite encendido seguro, también se utilizarán todas las huellas digitales incluidas para el encendido seguro.*

8 *(Opcional) Si se seleccionó la inclusión en el disco duro y la configuración del sistema admite encendido seguro, también se utilizarán todas las huellas digitales incluidas para el encendido seguro.*

9 *Como la memoria del dispositivo es limitada, el número máximo de huellas digitales que se pueden almacenar es 21. Si algunas de las huellas digitales incluidas en los pasaportes no se asignan al encendido seguro del dispositivo (por ejemplo otro dispositivo está conectado), aparece el botón **Encendido** encima de cada dedo. El botón Encendido aparece "minimizado" por defecto. Se utilizará el dedo correspondiente para el encendido seguro. Si no desea utilizar un dedo para el encendido seguro, sino sólo para el inicio de sesión, haga clic en el botón Encendido para eliminarlo de la memoria del dispositivo.*

10 *Haga clic en **Siguiente** para finalizar la inclusión o configurar opciones adicionales (como por ejemplo Seguridad avanzada, tal como se describe en “Inclusión de huellas digitales” en la página 14).*

Eliminar

Las funciones varían en función de los privilegios administrativos del usuario actual. En el Modo seguro (consulte “Modo de seguridad” en la página 62), sólo los usuarios definidos como administradores de huellas digitales pueden eliminar pasaportes de usuario.

Para eliminar un pasaporte existente (los datos de todos los usuarios):

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Haga clic en **Huellas digitales**.*

3 *Haga clic en **Eliminar**.*
En el Modo práctico, pase el dedo para realizar la verificación y confirmar el borrado del pasaporte actual.
En el Modo seguro, el sistema muestra una lista de los pasaportes existentes. Seleccione el pasaporte que desee eliminar y confirme el borrado.

Importar o exportar un pasaporte de usuario

Los datos existentes del usuario (incluyendo huellas digitales, claves de cifrado, credenciales de inicio de sesión) se pueden exportar al archivo *.vtp (un archivo de pasaporte) y volver a importar al software de huellas digitales. El archivo *.vtp se cifra y protege mediante la contraseña definida durante la exportación. No puede importar la contraseña de un usuario existente. En este caso es necesario eliminar el pasaporte del usuario primero.

Sugerencia: Se recomienda exportar el pasaporte para crear una copia de seguridad.

Para exportar un pasaporte existente:

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Haga clic en**Huellas digitales**.*

3 *Haga clic en **Importar o exportar datos de usuario**.*
*En el Modo seguro, el sistema muestra una lista de los pasaportes existentes. Seleccione el pasaporte que desee exportar y haga clic en **Exportar**.*

4 *Seleccione el archivo de destino **(*.vtp)**.*

5 *Defina una contraseña para proteger los datos exportados.*

6 *Verifique el dedo (incluido en el pasaporte que está exportando).*

Para importar un pasaporte:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Haga clic en **Huellas digitales**.*
3. *Haga clic en **Importar o exportar datos de usuario**. En el Modo seguro, el sistema muestra una lista de los pasaportes existentes. Haga clic en **Importar.***
4. *Busque el archivo de pasaporte **(.vtp).***
5. *Introduzca la contraseña (definida durante la exportación).*

Configuración

El cuadro de diálogo Protector Suite QLConfiguraciones incluye varias opciones de configuraciónProtector Suite QL. No todas las funciones del cuadro de diálogo Configuraciones descrito aquí se pueden visualizar, las funciones disponibles varían dependiendo de la versión instalada de Protector Suite QL y los privilegios administrativos del usuario actual.

Configuración del sistema

Configuración del sistema contiene la configuración común a todos los usuarios. El acceso a estos valores de configuración está limitado a los administradores. Las siguientes funciones se pueden configurar en Configuración del sistema:

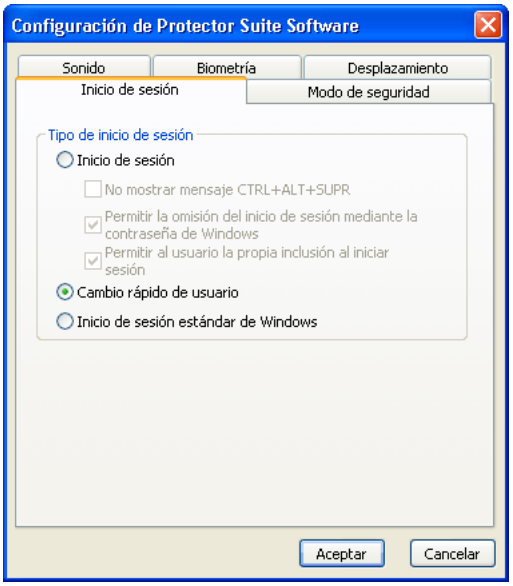
Inicio de sesión, Modo de seguridad, Sonido, Biometría, TPM (opcional), Desplazamiento..

Si está utilizando Windows Vista, haga clic en **Elevar privilegios administrativos para el usuario** en Centro de control para obtener derechos administrativos para hacer cambios en Configuración del sistema y en las cuentas de otros usuarios.

Inicio de sesión

Sólo los administradores pueden cambiar la configuración del inicio de sesión. Algunos cambios requieren que reinicie el equipo. La pantalla Configuración del inicio de sesión le permite:

- *Sustituir el inicio de sesión en Windows por un inicio de sesión protegido de huellas digitales*
- *Iniciar automáticamente la sesión del usuario verificado mediante la función de encendido seguro (opcional)*
- *Permitir el cambio rápido de usuario (opcional)*



Para cambiar la configuración del inicio de sesión:

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Vaya a **Configuración** > **Configuración del sistema > Inicio de sesión.***

3 *Seleccione:*

• ***Inicio de sesión mediante huellas digitales***
: si se selecciona esta opción, se activa el inicio de sesión mediante huellas digitales en el equipo.

•***No mostrar mensaje CTRL+ALT+SUPR***
: no se muestra el mensaje estándar CTRL+ALT+SUPR de Windows. Únicamente aparecerá una indicación para que el usuario pase un dedo por el sensor. (El cuadro de diálogo de inicio de sesión para introducir el nombre de usuario/dominio/contraseña se puede invocar si se presiona CTRL+ALT+SUPR de forma que el usuario pueda iniciar sesión mediante el nombre de usuario y contraseña.)

·***Permitir la omisión del inicio de sesión mediante la contraseña de Windows****: si está activada, se puede utilizar el inicio de sesión estándar de Windows. Si no lo está, únicamente los administradores de huellas digitales pueden iniciar sesión utilizando nombre y contraseña de usuario.*

·***Permitir al usuario la propia inclusión al iniciar sesión*** *: los usuarios pueden incluir sus dedos al iniciar sesión en el equipo.*

•Si está utilizando Windows Vista, haga clic en ***Detalles*** *para ver la configuración de los proveedores de credenciales, es decir, cómo el sistema administra la autenticación de usuario. Consulte "Proveedores de credenciales en Windows Vista" para obtener más información*

• ***Cambio rápido de usuario***
: si está seleccionada esta opción, está activado el cambio rápido de usuario biométrico controlado por huellas digitales (si es compatible con el sistema). Cuando se admite el cambio rápido de usuario pero no está activado, se le pedirá que lo active en el sistema. El cambio rápido de usuario no se puede activar si el ordenador es miembro de un dominio.

• ***Inicio de sesión estándar de Windows****: si se selecciona esta opción, se desactiva el inicio de sesión mediante huellas digitales y se utiliza el inicio de sesión estándar de Windows.*

• ***Activar inicio de sesión único de encendido seguro***
: seleccione esta opción para realizar la autenticación de huellas digitales del inicio de sesión y del encendido seguro en un único paso. Los usuarios verificados en el nivel de la BIOS inician sesión automáticamente en Windows.

4 *Haga clic en* ***Aceptar*** *y reinicie el equipo.*

Proveedores de credenciales en Windows Vista

Los proveedores de credenciales ofrecen varias maneras de poder autenticarse en el sistema. El proveedor de contraseñas de Microsoft requiere el nombre de usuario y la contraseña, el proveedor de huellas digitales necesita que pase el dedo por el sensor. La lista de proveedores de credenciales variará según la configuración de un sistema determinado.

Para ver la configuración de un proveedor:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Seleccione **Configuración > Configuración del sistema > Inicio de sesión.***
3. *Haga clic en **Detalles.***
4. *Las siguientes funciones son definidas por los proveedores de credenciales:*

   • ***Inicio de sesión** define el modo en que los usuarios se autentican cuando inician sesión en el sistema (por ejemplo mediante huellas digitales sólo, mediante nombre y contraseña, etc.)*

   • ***Desbloquear** define el modo en que los usuarios se autentican cuando desbloquean el equipo.*

   • ***Ejecutar como administrador** es una función de Windows Vista. Un usuario que inicia sesión como usuario limitado puede autenticarse como administrador y ejecutar una aplicación limitada a administradores.*

   • ***Cambiar contraseña** define el tipo de autenticación necesaria para cambiar la contraseña de usuario (por ejemplo verificación de huellas digitales, nombre y contraseña de usuario).*
5. *Seleccione:*

   • ***Marcar imagen de mosaico de usuario incluido** para mostrar un icono de huella digital sobre el mosaico de la cuenta de usuario para marcar que un usuario está incluido y que el inicio de sesión será administrado por una huella digital. Si no está seleccionado, el mosaico de la cuenta aparecerá como de costumbre. Esto establecerá el proveedor de contraseñas de Microsoft en "ajustado" (consulte a continuación).*

   • ***Permitir al usuario la propia inclusión al iniciar sesión**para que los usuarios que tengan una contraseña válida pero sin huellas digitales incluidas puedan incluir sus propios dedos cuando inicien sesión en el equipo.*
6. *Para cambiar la configuración de un proveedor, seleccione uno de la lista y haga clic en **Detalles**... (o haga doble clic en el proveedor).*

Nota: El proveedor de huellas digitales y el proveedor de contraseñas de Microsoft no pueden ser definidos por el usuario. Sus configuraciones están predefinidas.

7 *Aparecerá un cuadro de diálogo que permite ver las configuraciones del proveedor seleccionado. Las opciones son las siguientes:*

*• **Activado** activará el proveedor. Por ejemplo, cuando está establecido Activado para el proveedor de huellas digitales en la sección Inicio de sesión, se solicitará a los usuarios que se autentiquen pasando el dedo por el sensor cuando inicien sesión en el equipo.*

*• **Desactivado** desactivará el proveedor. Por ejemplo, cuando en la sección Inicio de sesión el proveedor de contraseñas de Microsoft está establecido en Desactivado y el proveedor de huellas digitales en Activado, sólo se permitirá la verificación con huellas digitales al iniciar sesión.*

*• **Ajustado** - para un usuario el proveedor ajustado parece estar aún Activado pero el proveedor de huellas digitales desactivará el control de sus funciones.*

Nota: El proveedor de huellas digitales no se puede definir como ajustado pero puede ajustar otros proveedores (como por ejemplo el proveedor de contraseñas de Microsoft).

Modo de seguridad

Protector Suite QL puede trabajar en tres modos de seguridad:

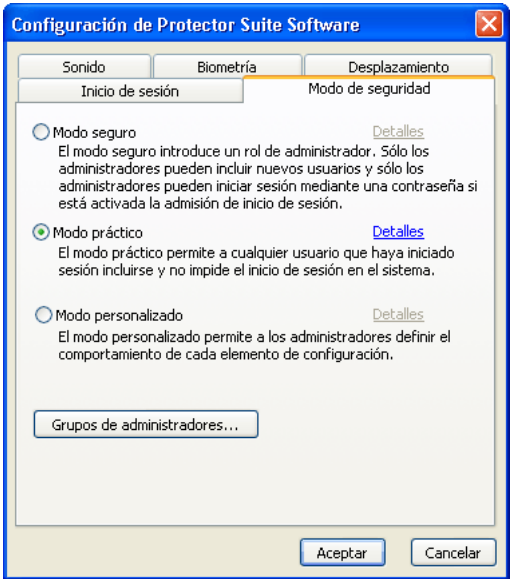
Modo seguro, Modo práctico y **Modo personalizado.**

Los modos de seguridad varían según los derechos concedidos a los usuarios. Entre estos derechos se encuentran por ejemplo permisos para incluir usuarios, eliminar o editar huellas digitales, etc.

Haga clic en **Detalles** para ver la configuración de las normativas de seguridad de cada modo. Sólo se pueden cambiar las normativas del Modo personalizado.

Grupos de administradores de huellas digitales

Contiene una lista de grupos de usuarios de seguridad local o de dominio definidos como "administradores de huellas digitales". Estos usuarios poseen derechos administrativos para gestionar Protector Suite QL Sus derechos se definen en las normativas del Modo de seguridad (consulte abajo).



Para seleccionar un modo de seguridad:

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Seleccione **Configuraciones > Configuración del sistema***

3 *Seleccione la pestaña **Modo de seguridad**. Seleccione:*

• ***Modo seguro.** En el Modo seguro sólo un administrador de huellas digitales tiene acceso ilimitado a todas las funciones de gestión de huellas digitales (por ejemplo, crear, eliminar pasaportes de huellas digitales para todos los usuarios), incluyendo Inspector de almacenamiento de huellas y Administración de encendido seguro.*

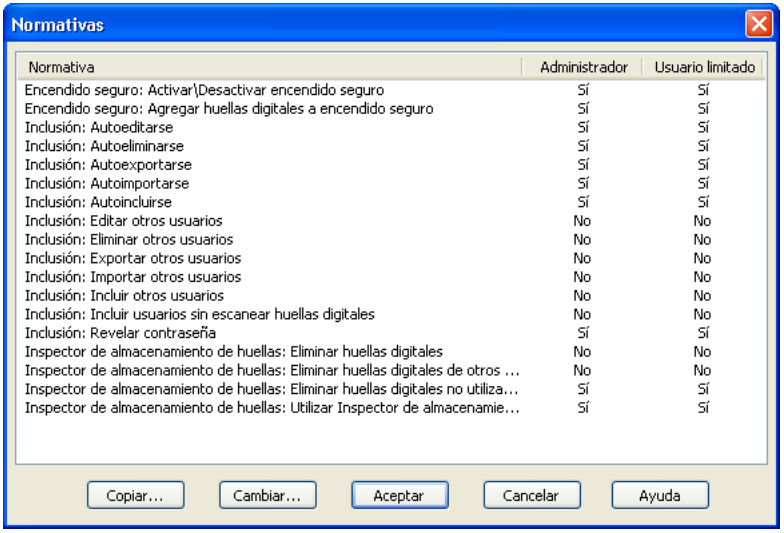
• ***Modo práctico.** En el Modo práctico, todos los usuarios comparten los mismo derechos. Por ejemplo, todos los usuarios pueden crear, editar o eliminar su propio pasaporte de huellas digitales.*

• ***Modo personalizado.*** *La configuración de las normativas del modo personalizado se puede establecer de manera diferente para los administradores y usuarios limitados.*

4 *Haga clic en* ***Aceptar*** *para cerrar el cuadro de diálogo.*

Normativas del modo de seguridad

Las normativas del Modo práctico y Modo Seguro están preestablecidas y no se pueden modificar. Sólo se pueden cambiar las normativas del Modo personalizado. Seleccione y haga doble clic en una normativa para ver sus detalles.



Para editar normativas en el modo personalizado:

1 *Seleccione* ***Inicio*** > ***Todos los programas*** > ***Protector Suite QL*** > ***Centro de control***

o pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***

2 *Seleccione* ***Configuraciones > Configuración del sistema***

3 *Seleccione la pestaña **Modo de seguridad**.*

4 *Haga clic en el botón de opción **Personalizar**y, a continuación, en **Detalles**. Aparecerá la ventana de normativas. Consulte los detalles de las normativas a continuación.*

5 *Haga clic en el botón **Cambiar** (o doble clic) para editar la configuración de las normativas.*

6 *Haga clic en **Aceptar** para cerrar el cuadro de diálogo.*

Las normativas se pueden definir de manera diferente para un administrador de huellas digitales y cuentas de usuario limitado. Seleccione **Permitir**/**denegar** para definir los derechos para cada grupo de usuarios.

Puede copiar la configuración de las normativas del modo seguro o práctico al modo personalizado y editarlas posteriormente. Esto es conveniente si desea hacer unos pocos cambios en la configuración de las normativas.

Para copiar las normativas del modo práctico al modo seguro:

1 *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

*o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***

2 *Haga clic en**Configuraciones > Configuración del sistema***

3 *Seleccione la pestaña **Modo de seguridad**.*

4 *Haga clic en el botón de opción **Personalizar** y, a continuación, en **Detalles**. Aparece la ventana de normativas. Consulte los detalles de las normativas a continuación.*

5 *Haga clic en el botón **Copiar** para copiar la configuración de las normativas.*

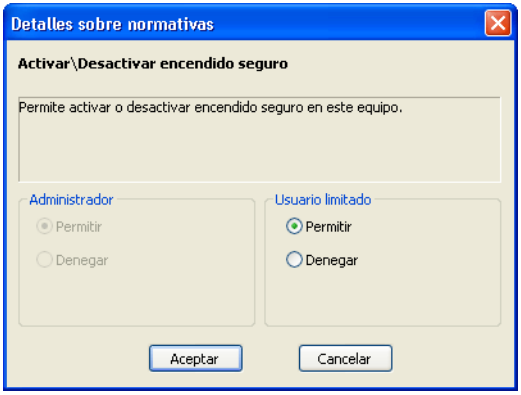
6 *Seleccione **Seguro** o **Modo práctico** y la configuración de las normativas se copiará del modo seleccionado.*

7 *Ahora puede editar las normativas utilizando el botón **Cambiar**.*

8 *Haga clic en **Aceptar** para cerrar el cuadro de diálogo.*

Detalles de las normativas:

Seleccione y haga doble clic en una normativa para ver sus detalles.



Inclusión:

- Eliminar otros usuarios: *permite la eliminación de un pasaporte de huellas digitales perteneciente a un usuario incluido en este equipo. No es necesaria verificación antes de eliminar los pasaportes.*
- Autoeliminarse: *después de la verificación permite eliminar un pasaporte de huellas digitales perteneciente al usuario que ha iniciado sesión actualmente*
- Editar otros usuarios: *permite la edición de un pasaporte de huellas digitales perteneciente a cualquier usuario incluido en este equipo, por ejemplo, agregar o eliminar huellas digitales incluidas.*
- Autoeditarse: *permite la edición de un pasaporte de huellas digitales perteneciente al usuario que ha iniciado sesión actualmente, por ejemplo agregar o eliminar huellas digitales incluidas.*
- Incluir otros usuarios: *permite que otros usuarios incluyan huellas digitales. Sólo pueden incluirse los usuarios con una cuenta de Windows válida.*
- Autoincluirse: *permite al usuario que ha iniciado sesión actualmente incluir huellas digitales.*
- Incluir usuarios sin escanear huellas digitales: *permite que los usuarios se incluyan sin escanear sus huellas digitales. Se les solicitará a los usuarios que escaneen sus huellas digitales la próxima vez que inicien sesión.*
- Exportar otros usuarios: *permite exportar un pasaporte de huellas digitales perteneciente a cualquier usuario incluido en este equipo.*

- Autoexportarse: *permite exportar un pasaporte de huellas digitales perteneciente al usuario que ha iniciado sesión actualmente.*
- Importar otros usuarios: *permite importar un pasaporte de huellas digitales perteneciente a cualquier usuario incluido en este equipo.*
- Autoimportarse: *permite importar un pasaporte de huellas digitales perteneciente al usuario que ha iniciado sesión actualmente.*
- Revelar contraseña: *permite revelar la contraseña de Windows de un usuario durante la inclusión de huellas digitales.*

Inspector de almacenamiento de huellas:

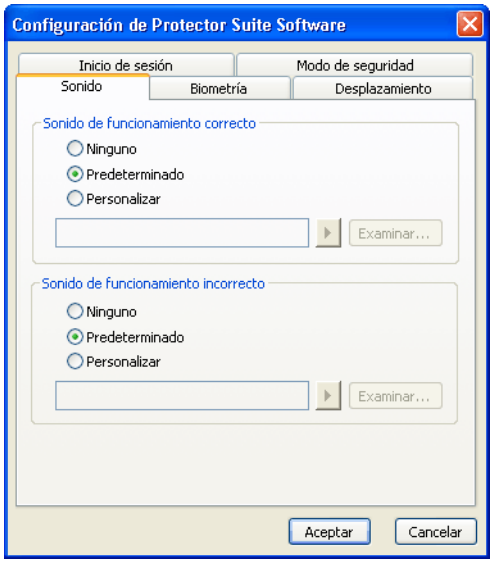
- Eliminar huellas digitales: *permite eliminar cualquier huella digital de su dispositivo. (La normativa Utilizar Inspector de almacenamiento de huellas debe estar activada para que surta efecto.)*
- Eliminar huellas digitales de otros usuarios: *permite eliminar huellas digitales de otros usuarios. Sin embargo, debe quedar como mínimo una huella digital incluida para cada usuario. (La normativa Utilizar Inspector de almacenamiento de huellas debe estar activada para que surta efecto.)*
- Eliminar huellas digitales no utilizadas: *permite que los registros de huellas digitales que no pertenecen a ningún usuario incluido localmente sean eliminados, por ejemplo, de la instalación anterior. (La normativa Utilizar Inspector de almacenamiento de huellas debe estar activada para que surta efecto.)*
- Utilizar Inspector de almacenamiento de huellas: *permite el uso de Inspector de almacenamiento de huellas, es decir, los usuarios pueden eliminar sólo sus propias huellas digitales (excepto la última, o lo que es lo mismo, debe quedar una huella digital incluida como mínimo).*

Encendido seguro:

- Agregar huellas digitales a encendido seguro: *permite agregar huellas digitales al encendido seguro durante la inclusión. Si está desactivado, las huellas digitales incluidas no se pueden utilizar para la verificación del encendido seguro.*
- Activar/desactivar encendido seguro: *permite activar o desactivar el encendido seguro en este equipo.*

Sonido

Se reproduce el sonido seleccionado cuando una operación de huella digital falla o se realiza satisfactoriamente. Puede utilizar los sonidos predeterminados del sistema, desactivar sonidos o buscar su archivo de audio favorito (formato .wav).



Biometría

La configuración biométrica le permite modificar la configuración del nivel de seguridad del sensor de huellas digitales. Es necesario reiniciar cada vez que realice algún cambio.

Para cambiar la configuración biométrica:

1 *Seleccione* ***Inicio*** > ***Todos los programas*** > ***Protector Suite QL*** > ***Centro de control***

o pase el dedo para mostrar ***Biomenú*** *y seleccione* ***Centro de control***

2 *Haga clic en* ***Configuraciones > Configuración del sistema*** *y vaya a* ***Modo de seguridad > Biometría***

- ***Bloqueo de intruso***

  - ***Cuenta de bloqueo:*** *establece el número permitido de intentos de verificación fallidos (pasos de dedos) antes de que el dispositivo se bloquee.*

•***Tiempo de bloqueo:*** *establece el tiempo en que el dispositivo quedará bloqueado. Transcurrido este tiempo, puede volver a utilizar el sensor de huellas digitales.*

• ***Rendimiento biométrico*** *define la precisión con que un escaneo de huella digital debe coincidir con las muestras incluidas. Tenga en cuenta que utilizando el nivel más bajo puede comprometer la seguridad del dispositivo. El nivel más alto, sin embargo, requiere una perfecta coincidencia con la muestra incluida y puede dar lugar a verificaciones fallidas continuadas también para los usuarios autorizados. Se recomienda el nivel predeterminado (medio).*

TPM (opcional)

Esta página se muestra cuando se detecta una aplicación de gestión TPM de terceros. La inicialización TPM permite el uso del módulo de seguridad TPM por parte de la función Seguridad avanzada. Consulte “Seguridad avanzada” en la página 23.

Para iniciar el módulo TPM:

1. *Haga clic en el botón **Iniciar TPM** para ejecutar el asistente de inicio de TPM.*
2. *Haga clic en **Siguiente** en la pantalla **Bienvenido**. Se realiza la inicialización.*
3. *Se muestra el resultado de la operación. Si la operación ha sido correcta, Protector Suite QL puede usar la seguridad TPM adicional.*
4. *Haga clic en el botón **Finalizar** para cerrar el asistente.*

Desplazamiento.

Puede utilizar el sensor de huellas digitales para desplazarse por el **Biomenú**(consulte página 81) o cualquier aplicación de Windows en lugar de la rueda del mouse. Puede definir opciones para el desplazamiento (velocidad, aceleración) así como la tecla de acceso rápido de desplazamiento predeterminada.

Para establecer las opciones de desplazamiento:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control.***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Seleccione la pestaña **Desplazamiento**.*

*• Haga clic en el botón **Probar despl.** para probar el desplazamiento con los valores seleccionados.*

*• **Velocidad**: desplace la barra deslizadora para ajustar la velocidad de desplazamiento. Esto define la velocidad a la que se desplazará el cursor cuando mueva el dedo sobre el sensor.*

*• **Aceleración**: mueva la barra deslizadora para definir la aceleración del desplazamiento. Cuanto más rápido pase sobre el sensor, más rápido será el desplazamiento.*

*• Puede definir la tecla de acceso rápido de cambio de desplazamiento en el campo **Tecla cambio despl.**. Pulse la(s) tecla(s) que desee utilizar para activar o desactivar la función de desplazamiento.*

3 *Haga clic en **Aceptar** para cerrar el cuadro de diálogo.*

Configuración de usuario

Configuración de usuario contiene la configuración de un usuario específico. Estos valores están protegidos por su huella digital.

Las siguientes funciones se pueden configurar en Configuración de usuario:

General, Máscara de biomenú, Banco de contraseñas, Registros, Seguridad de archivos y Aplicaciones.

General

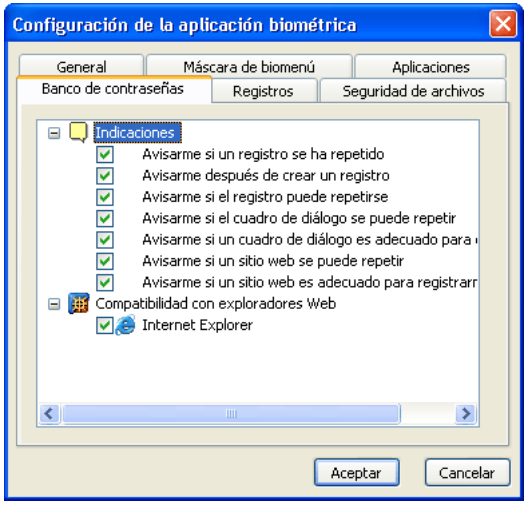
Marque la casilla de verificación **Mostrar icono en bandeja** para mostrar el icono de la bandeja que ofrece un acceso rápido a algunas funciones de Protector Suite QL. Consulte “Icono de la bandeja del sistema” en la página 80 para obtener más información sobre las funciones disponibles en el icono de la bandeja.

Máscara de biomenú

Seleccione una máscara (apariencia) para el Biomenú de Protector Suite QL. En la parte derecha de la página se muestra un ejemplo. (La vista previa de la máscara no se admite en Windows 2000.)

Banco de contraseñas

Este cuadro de diálogo consta de dos partes. La primera parte está visible para todos los usuarios. Contiene la configuración específica de usuario de las indicaciones que aparecen para informar al usuario de posibles acciones del Banco de contraseñas. Marque las indicaciones que desea que se muestren.



La segunda parte está visible sólo para los administradores. Si desea instalar la compatibilidad del Banco de contraseñas con un explorador, marque la casilla de verificación correspondiente.

Para obtener más información sobre el Banco de contraseñas, consulte Capítulo 3, “Banco de contraseñas”, en la página 29.

Registros

Este cuadro de diálogo enumera todos sus registros existentes. Se muestran tanto las páginas registradas como los cuadros de diálogo.

Seleccione un registro de la lista y haga clic en uno de los botones: **Renombrar** para renombrar el registro, **Editar** para editar el registro, **Eliminar** para eliminar el registro. Haga clic en **Exportar** para exportar los registros y usarlos en otro equipo, e **Importar** para importar registros de un archivo exportado.

Para obtener más información, consulte Capítulo 3, “Administración de registros”, en la página 33.

Seguridad de archivos

Puede definir o modificar la contraseña que protege los archivos guardados en los archivos de seguridad de archivos cifrados. Esta contraseña protegerá todos los archivos que desee proteger mediante una contraseña de respaldo global. Se recomienda utilizar una contraseña de respaldo porque de lo contrario, no podrá acceder a los archivos guardados en el archivo de seguridad de archivos cuando la verificación de huellas digitales no es posible (en el caso de heridas en el dedo, problemas con el dispositivo, etc.). Utilice una contraseña segura (es decir, ocho caracteres como mínimo, incluyendo caracteres no alfanuméricos, etc.).

Nota: Cambiar esta contraseña no afecta al archivo de seguridad de archivos ya creado.

Para obtener más información sobre contraseñas y seguridad de archivos consulte Capítulo 3, “Cifrado de archivos (adición de archivos o carpetas a un archivo de seguridad de archivos)”, en la página 39.

Aplicaciones

Muestra las aplicaciones que se pueden iniciar mediante las huellas digitales.

Debe quedar sin asignar al menos un dedo incluido para mostrar el Biomenú. El número máximo de aplicaciones que puede iniciar es igual al número de dedos incluidos menos uno, por ejemplo, si desea iniciar dos aplicaciones, debe tener tres dedos incluidos como mínimo.

Para iniciar una aplicación mediante una huella digital incluida:

1. *Haga clic en el botón **Agregar**. Se abrirá el cuadro de diálogo Aplicación.*
2. *Seleccione un dedo incluido que esté libre. Aparece un cuadro de diálogo solicitándole incluir más dedos si ninguno está disponible.*
3. *Escriba el nombre de la aplicación.*
4. *Localice el archivo que desee ejecutar. Puede ser cualquier archivo ejecutable (por ejemplo Iexplore.exe) .*
5. *Opcionalmente, los parámetros adicionales se pueden introducir en el campo **Parámetros de la aplicación** (consulte página 36).*
6. *Haga clic en **Aceptar**.*

Para obtener más información detallada sobre el Iniciador de aplicaciones y los parámetros de aplicaciones, consulte Capítulo 3, “Iniciador de aplicaciones”, en la página 36

Encendido seguro (opcional)

La función de encendido seguro evita el acceso no autorizado al equipo del usuario a nivel de BIOS. Los ordenadores con la función de encendido seguro activada no cargarán el sistema operativo desde el disco duro sin una autenticación correcta de las huellas digitales.

Las muestras de huellas digitales se almacenan en una memoria del dispositivo de huellas digitales. Durante el arranque del equipo, se le solicita una autenticación de huellas digitales. El tiempo para pasar el dedo por el sensor es limitado. El equipo sólo arrancará si la huella digital escaneada coincide con una muestra almacenada en la memoria del dispositivo. Tras una verificación correcta, el proceso de arranque continúa normalmente.

Activación del encendido seguro en Protector Suite QL

Las opciones para trabajar con el encendido seguro se muestran sólo si el equipo admite esta función (admitida principalmente en equipos portátiles). En la mayoría de las configuraciones, el encendido seguro se activa automáticamente tras incluir al primer usuario.

Para activar/desactivar el encendido seguro:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Haga clic en **Configuración > Encendido seguro**.*
3. *Seleccione **Sustituir las contraseñas del encendido seguro y del disco duro por el lector de huellas digitales**.*
4. *Haga clic en **Finalizar**.*

Si se ha configurado la inclusión en el disco duro, habrá más opciones disponibles en el cuadro de diálogo **Encendido seguro**. Las huellas digitales de la memoria de encendido seguro aparecen en la ventana **Huellas digitales autorizadas para el encendido seguro**. Aquí puede eliminar dedos de la memoria para la seguridad del arranque.

Para agregar huellas digitales al encendido seguro, consulte Capítulo 3, “Inclusión de huellas digitales”, en la página 14).

Inicio de sesión único en seguridad del arranque

El encendido seguro se puede configurar para que interopere con el inicio de sesión mediante huellas digitales. Si una huella digital utilizada para la función de encendido seguro coincide con una huella digital en algún pasaporte existente, el usuario correspondiente inicia la sesión automáticamente sin tener que introducir la contraseña de Windows o pasar el dedo una segunda vez.

Para activar el inicio de sesión de Windows automático para usuarios verificados mediante encendido seguro:

1. *Seleccione **Inicio** > **Todos los programas** > **Protector Suite QL** > **Centro de control***

   *o pase el dedo para mostrar **Biomenú** y seleccione **Centro de control***
2. *Haga clic en **Configuración** > **Configuración del sistema***
3. *Seleccione la pestaña **Inicio de sesión**.*
4. *Seleccione **Activar inicio de sesión único de encendido seguro.***

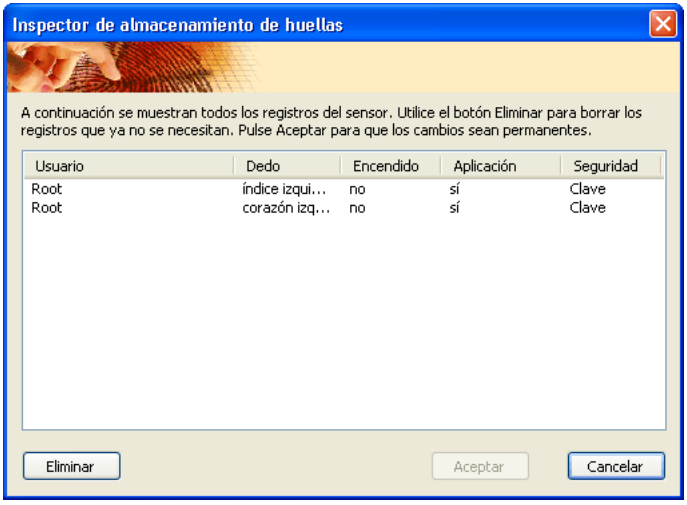
Nota: Su hardware debe ser compatible con el encendido seguro para poder utilizar esta función de inicio de sesión único y debe tener privilegios administrativos para cambiar la configuración.

Inspector de almacenamiento de huellas (opcional)

Esta función está disponible sólo cuando se utiliza la inclusión en el dispositivo.

El Inspector de almacenamiento de huellas es una herramienta que se utiliza para ver y editar el contenido almacenado en el dispositivo del sensor de huellas digitales. Se muestran todos los registros almacenados en el dispositivo.

Para cada huella digital, se muestra la descripción junto con la información de uso para el encendido seguro (autenticación previa al arranque), las aplicaciones (como el inicio de sesión) y el estado de la seguridad avanzada.



Para eliminar huellas digitales del dispositivo:

1. *Seleccione el registro que desea eliminar y haga clic en el botón **Eliminar.** La lista de registros se actualizará para reflejar el cambio.*
2. *Una vez que haya eliminado todos los registros que no necesite, haga clic en el botón **Aceptar** para hacer permanentes los cambios, o haga clic en **Cancelar** para descartar los cambios.*

*Se debe conservar al menos una huella digital para cada pasaporte. Para gestionar o eliminar todo un pasaporte, use el asistente **Incluir o editar huellas digitales** o **Eliminar** (consulte "Incluir o editar huellas digitales" en la página 53).*

Nota: La autorización para eliminar huellas digitales se define en la configuración de normativas del modo de seguridad (consulte "Modo de seguridad" en la página 62). Algunos derechos pueden limitarse a administradores de huellas digitales sólo.

Ayuda

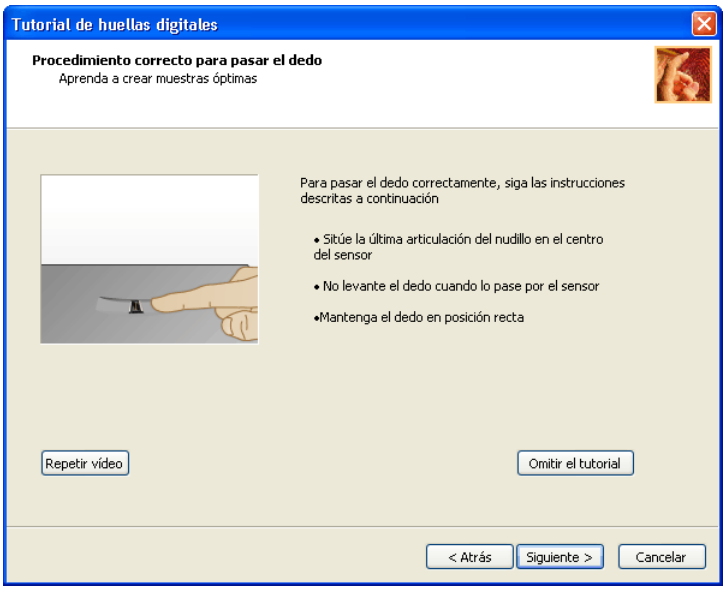
Introducción

Todas las funciones básicas de Protector Suite QL se resumen en la pantalla **Introducción**. Los vínculos del cuadro de diálogo le guiarán directamente a los temas de ayuda correspondientes.

Tutorial

Esto iniciará el Tutorial de huellas digitales.

El tutorial incluye un breve vídeo que muestra ejemplos de escaneado de huellas digitales correcto e incorrecto. A continuación, pruebe crear sus primeras muestras de huella digital.



Para obtener más información, consulte Capítulo 3, “Tutorial de huellas digitales”, en la página 20.

Nota: Para mostrar la ayuda basada en HTML, seleccione **Inicio >Todos los programas > Protector Suite QL > Ayuda** o haga clic en el icono **Ayuda** en el cuadro de diálogo Centro de control. Para ver la ayuda HTML contextual, pulse F1 en el cuadro de diálogo para el que necesita ayuda.

Biomenú

El **Biomenú** ofrece acceso a las funciones y configuraciones de Protector Suite QL. El número de elementos disponibles depende de los componentes instalados.

Para ver el Biomenú:

- *pase el dedo incluido por el sensor de huellas digitales.*

  *Para mostrar el **Biomenú** cuando la verificación de huellas realiza otra acción (por ejemplo, se vuelve a reproducir una página registrada), mantenga pulsado **Mayús** al pasar el dedo por el sensor.*

Utilice el ratón o el sensor para navegar. Si utiliza el sensor, mueva el dedo para navegar por el **Biomenú** y pulse el elemento resaltado para ejecutar la acción correspondiente. Puede configurar las opciones de desplazamiento en el cuadro de diálogo Configuración del sistema (consulte “Desplazamiento.” en la página 69).

El Biomenú está disponible en varias máscaras. Para ver o cambiar máscaras, abra **Centro de control** > **Configuración** > **Configuración de usuario**, pase el dedo para verificar y vaya a la ficha **Máscara de biomenú**.

•Bloquear equipo

*El primer elemento de menú contiene el comando **Bloquear equipo** y permite bloquear el equipo. Pase el dedo por el sensor para desbloquear el equipo de nuevo*

***•Páginas registradas** (opcional)*

Muestra una lista de las páginas Web registradas por el Banco de contraseñas. Para mostrar y cumplimentar una página registrada en el explorador Web predeterminado, haga clic en el nombre de la página Web en la lista.

***•Registrar...**(opcional)*

Registra una nueva ventana (página Web o cuadro de diálogo). Para obtener más información sobre el registro del Banco de contraseñas, consulte Capítulo 3, “Registro de páginas Web y cuadros de diálogo”, en la página 29.

- ***Bloquear todos los archivos** (opcional)*

  Bloquea todos los archivos de seguridad de archivos que están abiertos actualmente. Este elemento aparecerá sólo cuando haya dos archivos desbloqueados como mínimo.

- ***Centro de control...***

  muestra el cuadro de diálogo Centro de control (consulte “Centro de control” en la página 51).

- ***Ayuda***

  Muestra la ayuda HTML. Para ver la ayuda HTML contextual, pulse F1 en el cuadro de diálogo para el que necesita ayuda.

Icono de la bandeja del sistema

El icono de Protector Suite QL en la bandeja del sistema indica que el programa está en ejecución y proporciona el acceso a las funciones que no requieren la autenticación de las huellas digitales.

Editar huellas digitales...

Abre el asistente para la inclusión de huellas digitales.

También puede iniciar este asistente desde el Centro de control si selecciona **Huellas digitales > Incluir o editar huellas digitales.**Consulte **Capítulo 3, “Inclusión de huellas digitales”, en la página 14**para obtener información detallada sobre cómo incluir dedos.

Iniciar centro de control...

Inicia el Centro de control de Protector Suite QL (consulte página 51).

No utilizar sensor/Utilizar sensor

Permite separar temporalmente el dispositivo de huellas digitales de Protector Suite QL para que otra aplicación pueda utilizarlo. Este comando libera el dispositivo para la sesión de usuario actual. (El dispositivo sólo se puede utilizar por una aplicación en cada momento.)

Si selecciona la opción **No utilizar sensor**, Protector Suite QL no verificará las huellas digitales.

Importante: Esta función es sólo para usuarios avanzados, por ejemplo, programadores de otras aplicaciones biométricas.

Ayuda

Muestra la ayuda HTML. Para ver la ayuda HTML contextual, pulse F1 en el cuadro de diálogo para el que necesita ayuda.

Acerca de

Muestra la información de producto sobre Protector Suite QL.

Panel de información del lector de huellas digitales

El panel de información del lector de huellas digitales contiene información sobre el sensor y una ventana de prueba para el escaneo de huellas digitales. Puede utilizarlo para obtener información sobre el sensor en el caso de un problema de hardware de comunicación con el soporte técnico, por ejemplo..

Para ver el Panel de información del lector de huellas digitales

1. *Seleccione **Inicio** > **Panel de control***
2. *Haga clic en el icono **Sensor de huellas digitales**. Aparecerá el cuadro de diálogo **Panel de información del lector de huellas digitales**.*

   *• Seleccione la pestaña **Versión** para ver información sobre el sensor (como por ejemplo tipo de dispositivo, nombre, versión, etc.)*

   *Para exportar la información a un archivo de texto, haga clic en **Guardar** y seleccione una ubicación donde el archivo se guardará (FingerprintSensorVersion.txt por defecto).*

   *• Seleccione la pestaña **Prueba de huellas** para ver las imágenes de prueba de las huellas escaneadas al pasar su dedo por el sensor.*
3. *Haga clic en **Cerrar** para cerrar la ventana.*

Capítulo 5
Solución de problemas de Protector Suite QL

Instalación

No puedo instalar Protector Suite QL.

- *Compruebe sus privilegios. Aquel usuario que instale Protector Suite QL debe tener privilegios de administrador.*
- *Compruebe que cuenta con suficiente espacio libre en el disco. Para instalar Protector Suite QL, necesitará aproximadamente 40 MB.*
- *Compruebe el sistema. Únicamente Windows 2000, 2003, Windows XP y Windows Vista son compatibles.*

Protector Suite QL no funciona después de instalar.

- *Es necesario reiniciar después de instalar Protector Suite QL.*

Inclusión de huellas digitales

El dispositivo no funciona.

- *Compruebe la conexión del dispositivo.*
- *Compruebe si el controlador está correctamente instalado. Normalmente, los controladores se instalan durante la instalación de Protector Suite QL. Sin embargo, si experimenta algún problema, encontrará los controladores necesarios en la subcarpeta **Controladores** de la carpeta de instalación. Para obtener información específica sobre el dispositivo para la instalación del controlador, consulte Readme.txt en la carpeta **Controladores**. (Para comprobar el estado del dispositivo, haga clic con el botón derecho del ratón en **Mi PC**, seleccione **Propiedades** - **Hardware** y abra el **Administrador de dispositivos**.)*

No puedo incluir mis huellas digitales. Mis huellas digitales no son correctamente reconocidas.

- *Realice el tutorial de huellas digitales para aprender a crear muestras correctas. El tutorial de huellas digitales se puede ejecutar como parte del proceso de inclusión, o por separado, desde el menú **Inicio**.*
- *Pruebe a aplicar más o menos presión en el sensor.*
- *Pruebe a cambiar la velocidad de la pasada.*
- *Limpie el sensor. Use un paño húmedo sin hebras (con agua o loción hidratante sin perfume) y frótelo suavemente por el sensor. No use materiales abrasivos.*
- *Intente pasar el dedo. (Especialmente en climas calurosos.)*
- *Pruebe a usar otro dedo. El dedo índice normalmente es más fácil de incluir que el meñique.*

No puedo usar la autenticación de huellas digitales porque me he hecho daño en el único dedo incluido. Pruebe a incluir otro dedo.

Para poder usar Protector Suite QL al completo, deberá tener incluidos dos dedos útiles. Le recomendamos encarecidamente que incluya al menos dos dedos para evitar este problema.

Para actualizar los dedos incluidos, debe entrar en el asistente de **Incluir o editar huellas digitales**.

- *Si no utiliza seguridad avanzada, puede acceder usando la contraseña de Windows.*
- *Si usa seguridad avanzada con contraseña de respaldo, puede acceder usando ésta.*
- *Si usa seguridad avanzada sin contraseña de respaldo, desgraciadamente, no hay modo de añadir una huella digital diferente. En tal caso, le recomendamos que espere a poder usar el dedo de nuevo (cuando se cure la herida) o borre el pasaporte (**Asistente Borrar**) y vuelva a incluir nuevas huellas. Tenga en cuenta que en el segundo caso, sus datos secretos almacenados (contraseñas, claves de cifrado) se perderán. Para realizar la operación de borrado es necesario cancelar la operación de verificación de huellas digitales para pasar al cuadro de diálogo de contraseña, y a continuación introducir la contraseña de Windows.*
- *Si tiene seleccionado como tipo de seguridad **Clave del lector de huellas digitales** o **Clave del lector de huellas digitales con TPM** como tipo de seguridad avanzado, se le pedirá al final del proceso de inclusión que pase el dedo original para desbloquear los datos secretos del dispositivo. Como no puede hacerlo, tendrá que deshabilitar Seguridad avanzada antes de salir del asistente. Una vez que haya salido del asistente, podrá acceder a él de nuevo usando el dedo que acaba de incluir y a continuación habilitar de nuevo Seguridad avanzada. Estos pasos son necesarios para crear un nuevo conjunto de claves conectado a la huella nueva.*

Se me ha solicitado que pase de nuevo el dedo después de completar el proceso de inclusión. ¿Por qué?

La solicitud se muestra en casos en los que se ha usado la contraseña de respaldo de seguridad avanzada para entrar en el asistente **Incluir o editar huellas digitales**, **Clave del lector de huellas digitales** o **Clave del lector de huellas digitales con TPM** como tipo de seguridad avanzado, y ha añadido una huella nueva al pasaporte.

- *Este comportamiento es normal. Esta verificación es necesaria para crear un nuevo conjunto de claves conectado a la huella nueva.*

No puedo incluir un usuario en el modo seguro.

- *Compruebe que existe el pasaporte de usuario. El usuario probablemente ya está incluido. Cada usuario sólo puede tener un pasaporte.*

Importar usuario no funciona.

- *Compruebe que existe el pasaporte de usuario. Si desea importar datos para un usuario existente, primero debe borrar el pasaporte antiguo.*
- *Compruebe la memoria del dispositivo en **Inspector de almacenamiento de huellas** (**Centro de control** - **Configuración** - **Inspector de almacenamiento de huellas**). (Sólo si se usa la inclusión en el dispositivo.)*

¿Por qué debería exportar el pasaporte de usuario?

Los datos exportados pueden contener información de huellas digitales, credenciales de inicio de sesión, registros de Banco de contraseñas, información de cifrado para seguridad de archivos (pero no datos de seguridad de archivos).

- *Exporte los datos de usuario de forma regular como copia de seguridad de toda esta información.*

He perdido mi contraseña de respaldo de seguridad avanzada.

- *Para cambiar la contraseña de respaldo de seguridad avanzada, vaya al asistente **Incluir o editar huellas digitales**, pase el dedo y realice el proceso de inclusión de huellas digitales. En la página Seguridad avanzada, puede cambiar la contraseña de respaldo.*

Tengo que sustituir el sensor.

Si tiene que sustituir un sensor de huellas digitales o un lector que no funcionan, siga este procedimiento:

Inclusión en el disco duro:

- *Cuando se usa la inclusión en el disco duro, Protector Suite QL no almacena datos en el dispositivo; por lo tanto, no hace falta realizar ninguna acción después de sustituir el sensor. En caso de usar seguridad de arranque (autenticación antes del arranque), es posible que necesite usar el asistente **Incluir o editar huellas digitales** para actualizar los datos relacionados.*

Inclusión en el dispositivo:

- *Hay una conexión entre el pasaporte y el dispositivo de huellas digitales que requiere que sustituya el pasaporte actual por el pasaporte exportado previamente.*

Puede restaurar el pasaporte importando la copia de seguridad de éste al dispositivo nuevo:

1. *Borre el pasaporte.*
2. *Conecte el nuevo dispositivo (que funciona).*
3. *Importe el pasaporte desde un archivo de copia de seguridad.*

Sustitución de lectores externos:

- *El procedimiento descrito anteriormente también es válido si intenta usar múltiples lectores de huella digital con Protector Suite QL (por ejemplo, uno interno y uno externo, o dos lectores externos). Si usa la inclusión en el disco duro, normalmente no hay problemas con la posible excepción de la seguridad al arrancar (autenticación antes del arranque). Si usa la inclusión en el dispositivo, no debería sustituir los lectores a no ser que tenga una buena razón, y deberá borrar y volver a crear su pasaporte.*

Cuando use la inclusión en dispositivo, y el lector contenga datos (de una instalación anterior o diferente de Protector Suite QL) de un usuario que existe en el ordenador (y no se haya incluido aún), aparece una notificación que le pregunta si desea reutilizar estos datos.

Cuando el lector contenga datos (de una instalación anterior o diferente de Protector Suite QL) de un usuario que existe en el ordenador (y no se haya incluido aún), aparece una notificación que le pregunta si desea reutilizar estos datos.

Si el lector nuevo contiene los datos de un usuario que ya se ha incluido, éstos no se pueden reutilizar. En su lugar, se borran las huellas digitales del dispositivo por motivos de seguridad (para evitar agregar huellas digitales no verificadas).

Mi módulo TPM no funciona.

Si usa seguridad avanzada con TPM (Trusted Platform Module, módulo de plataforma de confianza) y se rompe, borra o deshabilita el módulo TPM, la seguridad avanzada no funcionará.

Si configura la contraseña de respaldo de seguridad avanzada, puede seguir estos pasos:

1. *Entre en el asistente **Incluir o editar huellas digitales** usando la contraseña de respaldo.*
2. *Deshabilite la seguridad avanzada y finalice.*

3 *Una vez reparado el TPM, o si se ha borrado, puede entrar de nuevo en el asistente **Incluir o editar huellas digitales** usando el dedo y rehabilitar la seguridad avanzada con TPM.*

Cambio rápido de usuario

El cambio rápido de usuario no se puede habilitar.

Esta opción sólo está visible en los equipos que utilicen el sistema Windows XP. Sólo puede utilizar la función Cambio rápido de usuario en los equipos que no sean miembros de un dominio.

- *Compruebe que su equipo no está en un dominio.*
- *La instalación de otro software (por ejemplo, Novell Client) puede impedir el cambio rápido de usuario.*

Inicio de sesión

No puedo iniciar sesión usando mi nombre de usuario y contraseña.

- *Compruebe el modo de seguridad. El inicio de sesión usando el nombre y la contraseña de usuario sólo es posible para todos los usuarios en el modo práctico. En el modo seguro, sólo los administradores cuentan con esta opción.*

No puedo cambiar la configuración de sistema de Protector Suite QL, aunque ésta se encuentra visible en Centro de control.

- *Compruebe sus privilegios de usuario. Los administradores son los únicos que pueden cambiar la **Configuración del sistema**. Ser el administrador local no es lo mismo que ser miembro del **Grupo de administradores** de Protector Suite QL. Los miembros del grupo pueden administrar pasaportes, huellas digitales, seguridad al arrancar y también iniciar sesión usando el nombre y la contraseña de usuario.*

Banco de contraseñas

Las páginas registradas se repiten en Internet Explorer después de un retraso.

Los registros se repiten sólo después de que la página está completamente cargada. Lamentablemente, a veces, Internet Explorer, muestra incorrectamente que la página ya está cargada (la animación en la esquina superior derecha se detiene), aunque no sea cierto. Si el usuario pulsa Detener para finalizar la carga, a veces, IE hace caso omiso del comando y no se detiene. En estas situaciones, espere hasta que la carga haya finalizado completamente. El mismo problema podría ocurrir con las páginas en las que, al pasar el ratón sobre algún elemento activo, (p.ej., una animación flash) comienza la carga del objeto, a pesar de que la página ya se ha cargado.

- *Espere hasta que la página se haya cargado del todo.*

No puedo registrar una página que ya estaba registrada. Al pasar el dedo, se activa la repetición.

- *Pulse MAYÚS al pasar el dedo para registrar una página o un cuadro de diálogo ya registrados (en lugar de repetir el registro).*

El banco de contraseñas no es capaz de registrar mi cuadro de diálogo.

El cuadro de contraseñas no puede manejar de forma correcta cuadros de diálogo que no contengan controles estándar. Un ejemplo serían los cuadros de diálogo de Microsoft Office.

- *El banco de contraseñas está diseñado principalmente para cuadros de diálogo estándar sencillos, que contienen nombre de usuario y contraseña. Los cuadros de diálogo complejos y no estándar pueden presentar problemas.*

Mi registro no se repite correctamente.

- *El Banco de contraseñas espera que la página usada para la repetición sea exactamente la misma que cuando se creó el registro. Por lo tanto, puede que se presenten problemas con páginas creadas dinámicamente usando JavaScript, o con formularios que parecen iguales, pero contienen diferencias internas.*