Autenticación

La autenticación es la etapa que permite verificar la identidad de una entidad (persona, ordenador, etc.) para darle acceso a los recursos (archivos, aplicaciones, etc.).

Durante la fase de verificación se llama a un protocolo de autenticación, como Kerberos.

Existen tres tipos de autenticación gestionados por Windows 10:

- La autenticación simple: se tiene en cuenta un único elemento (por ejemplo: una contraseña) durante el proceso.
- La autenticación fuerte: basada en al menos dos de los siguientes elementos:
  - Lo que el usuario sabe (contraseña, código PIN).
  - Lo que tiene (tarjeta inteligente, smartphone, memoria flash USB, etc.).
  - Lo que es (huella dactilar, reconocimiento facial, etc.).
  - Lo que sabe hacer (movimiento).
- La autenticación SSO (*Single Sign-On*): basta con una única autenticación para acceder a diferentes aplicaciones o programas.

Windows 10 presenta la autenticación basada no solamente en el conocimiento (conocer una contraseña), sino en algo que se debe hacer: el usuario debe efectuar una serie de acciones sobre una imagen seleccionada para poder abrir una sesión.

1. Contraseña de imagen

La contraseña de imagen requiere preferiblemente una pantalla táctil para crear una combinación de círculos, puntos y líneas rectas.

Esta funcionalidad es opcional y se convierte en una alternativa práctica para las tabletas táctiles, aunque posee fallos de seguridad como:

- Posibilidad de capturar en video (o visualmente) los gestos del usuario.
- Observación de las huellas dejadas por los dedos en la pantalla; esto puede resolverse limpiando la pantalla regularmente.

La ejecución de tres movimientos es fácil de memorizar y rápida de ejecutar.

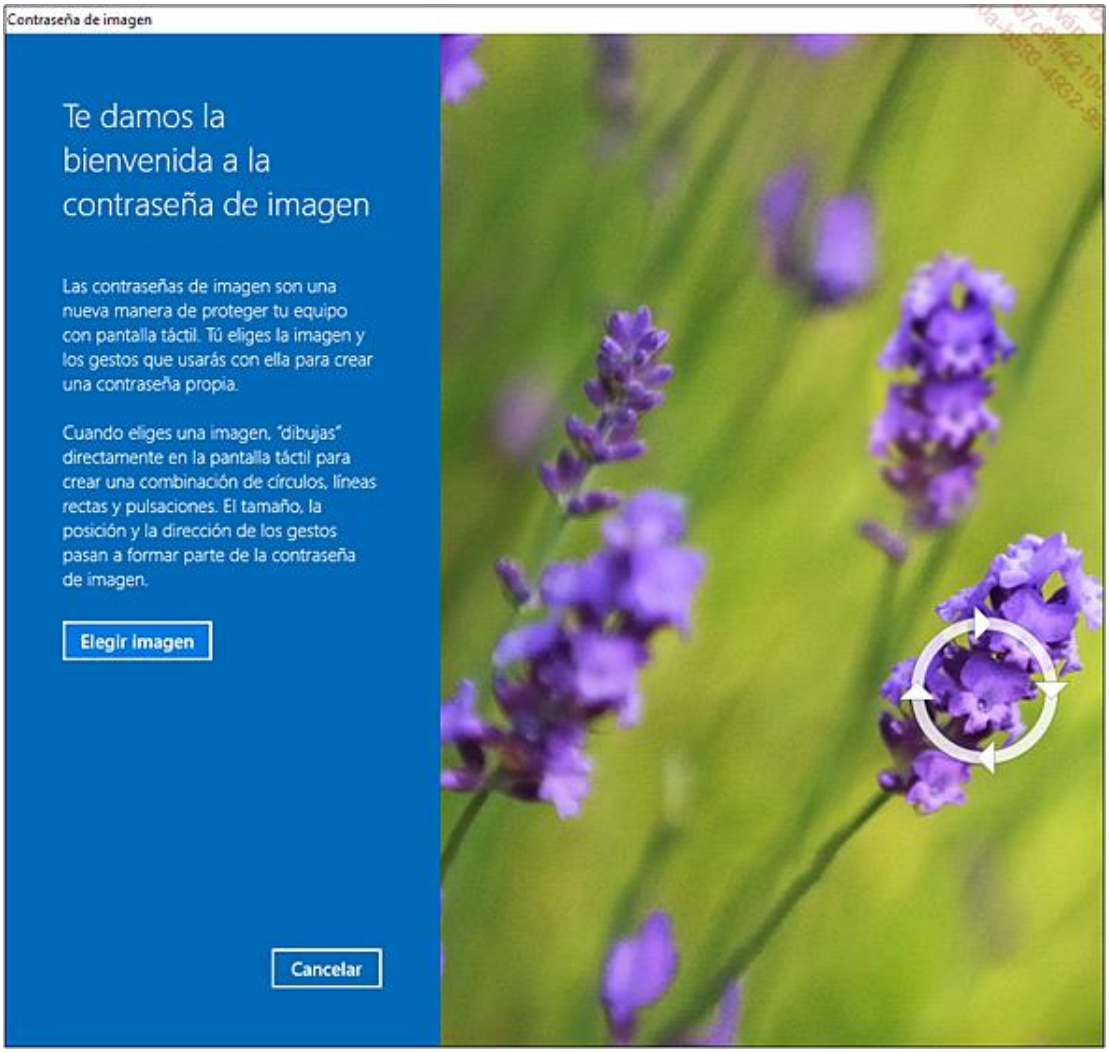
Si el usuario se equivoca cinco veces en el momento de la autenticación, la funcionalidad se deshabilita hasta que introduzca su contraseña principal. Además, este método no está disponible si se accede a la red usando una cuenta que soporte contraseña mediante imagen.

Un usuario habitual puede utilizar una contraseña de imagen realizando el siguiente procedimiento:

Haga clic en el menú **Inicio** y, a continuación, haga clic en **Configuración**, y luego en **Cuentas**. En la sección **Opciones de inicio de sesión** haga clic en el botón **Agregar** del campo **Contraseña de imagen**. Antes de activar la característica, el sistema solicitará que confirme su contraseña actual; a continuación pulse **Aceptar**.

Si la cuenta deseada no tiene contraseña, deberá crear una.

- Haga clic en el botón **Elegir imagen**, seleccione la imagen que usará para autenticarse y active **Abrir**.



- Haga clic en **Usar esta imagen**, cree movimientos (círculos, líneas o puntos) sobre ella, repita la operación una segunda vez. Haga clic en el botón **Finalizar**.

La autenticación por contraseña de imagen funciona también sin pantalla táctil empleando un ratón, haciendo clic con el botón izquierdo para crear puntos y manteniendo el botón pulsado para crear un círculo o una línea.

Durante el inicio de sesión, en adelante tendrá la opción de teclear una contraseña o bien realizar la serie de gestos sobre la imagen seleccionada.

Mediante un objeto de directiva de grupo, el administrador puede prohibir el uso de esta característica. Se trata del parámetro **Desactivar inicio de sesión con contraseña de imagen** del nodo **Configuración del equipo\Plantillas administrativas\Sistema\Inicio de sesión**.

2. Windows Hello

La biometría es una tecnología cada vez más corriente que permite acceder fácilmente a los sistemas, servicios y recursos. Consiste en medir una característica física inalterable de una persona para identificarla de manera unívoca. Las huellas digitales forman parte de las características biométricas más utilizadas, especialmente con los millones de lectores de huella digital integrados en los ordenadores personales y otros periféricos.

Lamentablemente, esta funcionalidad requiere de un hardware específico: una cámara infraroja activa para el reconocimiento facial o del iris, y un lector de huella digital compatible con Windows Biometric Framework.

Windows Hello permite conectar sus dispositivos de Windows 10 de forma más segura, con un simple reconocimiento del iris, facial o de huellas digitales.

a. Huellas digitales

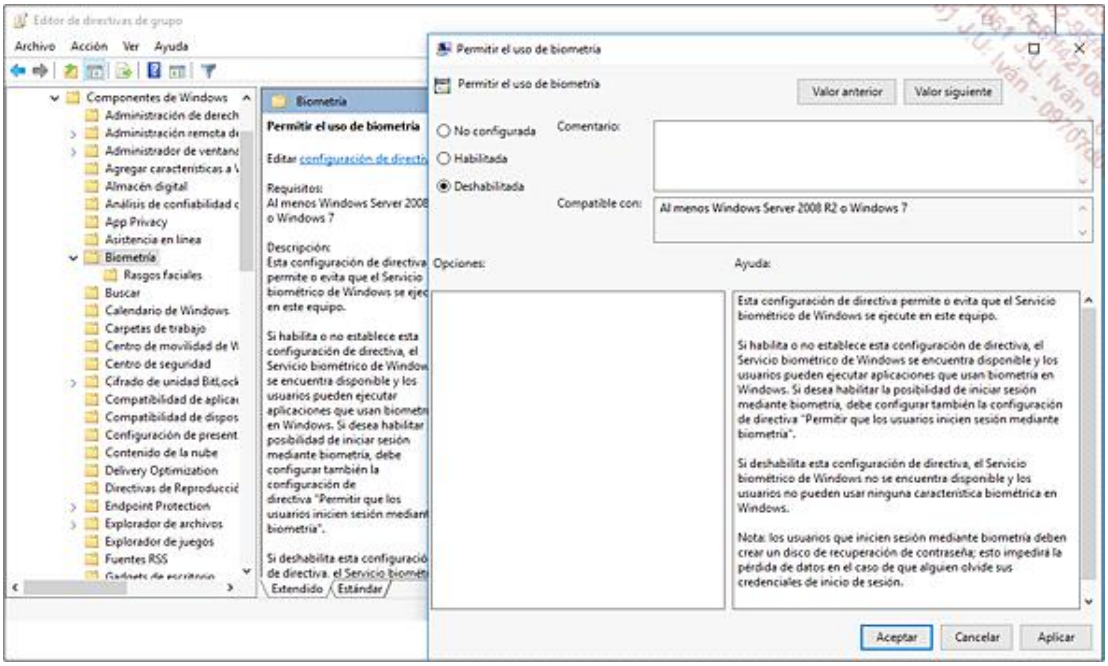
Windows 10 integra los controladores y aplicaciones necesarios para la gestión de huellas digitales, ofreciendo al usuario un método simple, rápido y seguro de autenticarse localmente o en un dominio Active Directory.

Para configurar su huella, asegúrese de contar con un lector de huellas conectado a su equipo:

Haga clic en el menú **Inicio** y, a continuación, haga clic en **Configuración** y **Cuentas**. En la sección **Opciones de inicio de sesión**, haga clic en el botón **Agregar** desde la sección **Huella digital**.

Durante la adquisición de una app en la Tienda de Windows, el usuario puede, en adelante, autenticar su cuenta mediante su huella digital.

Es posible deshabilitar el uso de las huellas digitales para la autenticación mediante el parámetro de la directiva de grupo **Configuración del equipo\plantillas administrativas\Componentes de Windows\Biometría**.



b. Reconocimiento facial o del iris

Windows Hello permite conectarse a dispositivos de Windows 10 de forma más segura, utilizando el procedimiento de reconocimiento facial o del iris del propietario del equipo. De esta forma, el empleo de una contraseña, generalmente poco seguro, ya no es un requisito previo para la autenticación.

El iris es la parte de color visible del ojo y contiene información única que permite reconocer a su propietario.

Para configurar el reconocimiento del iris, siga el procedimiento siguiente (asegúrese de haber conectado el hardware compatible mencionado previamente a su equipo):

- Haga clic en el menú **Inicio**, luego en **Configuración**, **Cuentas** y **Opciones de inicio de sesión**. En la sección **Windows Hello**, seleccione la opción correspondiente para el reconocimiento facial o del iris.

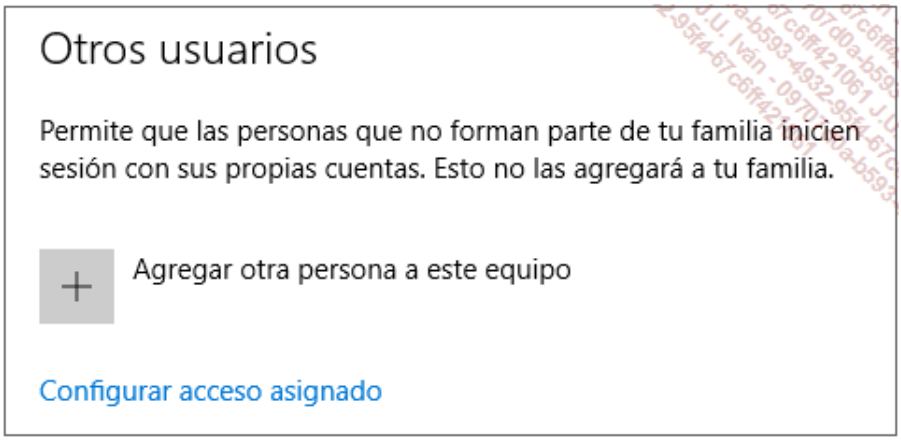
3. Acceso asignado

La funcionalidad **Acceso asignado** permite activar la ejecución de una única aplicación de la Tienda de Windows para una cuenta de usuario específica. De esta forma, un niño no podrá jugar más que con una aplicación educativa en su tableta, o una empresa podrá proporcionar acceso a su aplicación en forma de particiones estancas.

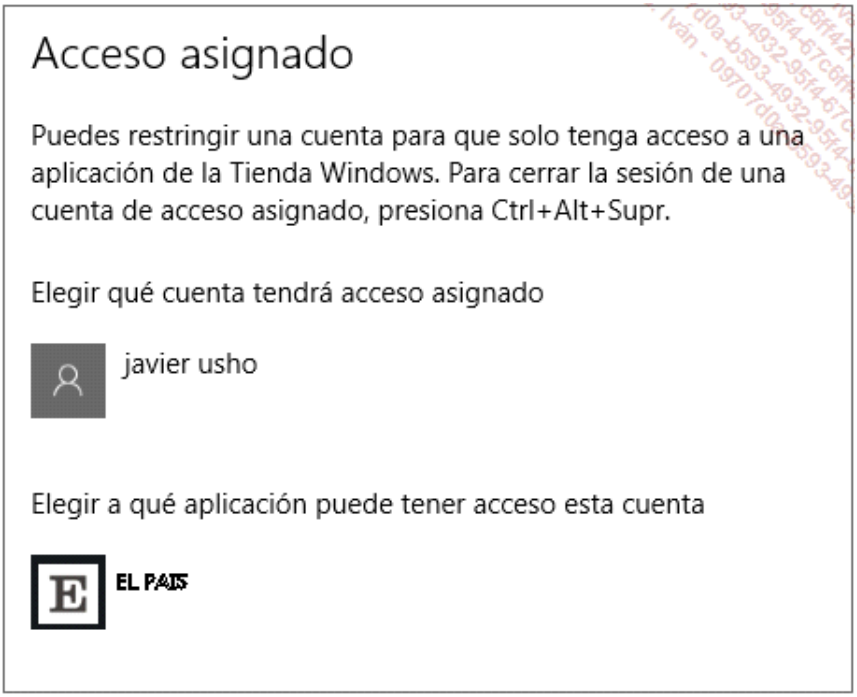
La funcionalidad requiere el uso de una cuenta Microsoft (Windows LiveID) que haya abierto sesión al menos una vez en el equipo con Windows 10.

Para configurar este tipo de acceso, he aquí el procedimiento:

- Haga clic en el menú **Inicio** y, a continuación, haga clic en **Configuración**, **Cuentas** y **Familia y otros usuarios**. Luego haga clic en **Configurar acceso asignado**. En la sección **Otros usuarios**, haga clic en **Agregar otra persona a este equipo**.



- Escriba la dirección de correo electrónico de su cuenta Microsoft (en nuestro ejemplo, añadiremos la cuenta **javierucho1@outlook.es** como cuenta con un acceso asignado) y, a continuación, haga clic en los botones **Siguiente** y **Finalizar**.
- Abra sesión con la cuenta previamente configurada, pero ignore la etapa de creación de un código PIN. Instale una aplicación desde el icono **Windows Store**; en nuestro ejemplo, la app **El País**. Cierre la sesión y, a continuación, abra sesión con una cuenta local. Haga clic en el menú **Inicio** y luego haga clic en **Configuración**, **Cuentas** y **Familia y otros usuarios**. Luego haga clic en **Configurar acceso asignado** y **Elegir una cuenta** y seleccione la cuenta previamente vinculada a Windows 10, en nuestro ejemplo **javierucho1@outlook.es**.
- A continuación, haga clic en **Elegir una aplicación** y seleccione la aplicación ya instalada (en nuestro ejemplo la app **El país.es**).



El usuario definido solo podrá, en adelante, ejecutar la aplicación seleccionada al abrir su sesión.

4. Código PIN

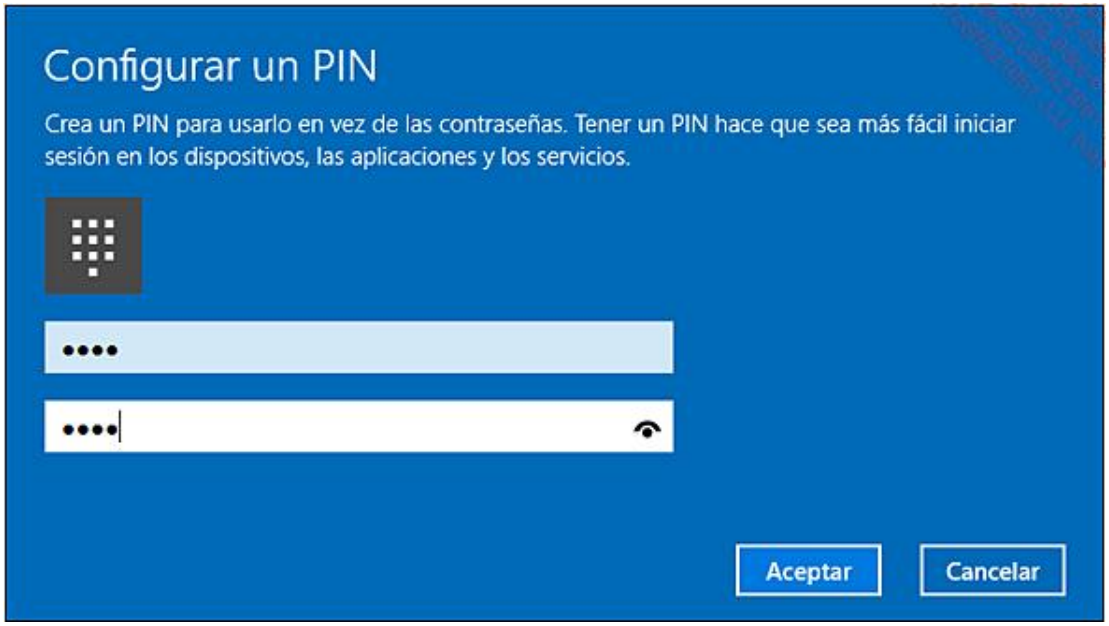
Usando un código de cuatro cifras, el usuario puede abrir una sesión con rapidez. Lamentablemente, no es posible combinar los métodos de autenticación (contraseña, contraseña de imagen) para mejorar la seguridad del equipo.

El teclado numérico es fácilmente accesible desde una tableta o un teclado; sin embargo, este método de inicio de sesión presenta importantes puntos débiles:

- Número de combinaciones escaso: código PIN con valores comprendidos entre 0000 y 9999, o sea, 10.000 combinaciones posibles.
- Código PIN trivial: el usuario se acuerda de un código fácil de memorizar (fecha de nacimiento), que puede adivinarse rápidamente.
- Rastro del PIN: el desgaste de las teclas puede proporcionar una pista sobre las cuatro cifras utilizadas, lo que limita el número de combinaciones a 24.

La creación de un código PIN durante el inicio de sesión se realiza de manera sencilla:

Haga clic en el menú **Inicio** y haga clic en **Configuración**, **Cuentas** y **Opciones de inicio de sesión**. En la sección **PIN** haga clic en el botón **Agregar** del campo **PIN**. Antes de activar la característica, el sistema le solicitará que confirme su contraseña actual y que confirme, a continuación, haciendo clic en **Aceptar**.



Introduzca el código, que debe ser de al menos cuatro cifras, confírmelo y haga clic en **Finalizar**.

Cuanto mayor es la longitud del código PIN, más segura es la autenticación del usuario.

Durante la fase de autenticación, el usuario puede introducir su PIN; el icono que lo identifica es un teclado numérico:

Mediante un objeto de directiva de grupo, el administrador puede prohibir el uso de esta característica. Se trata del parámetro **Activa inicio de sesión con PIN** del nodo **Configuración del equipo\Plantillas de administración\Sistema\Inicio de sesión**.

5. Usuarios y grupos locales

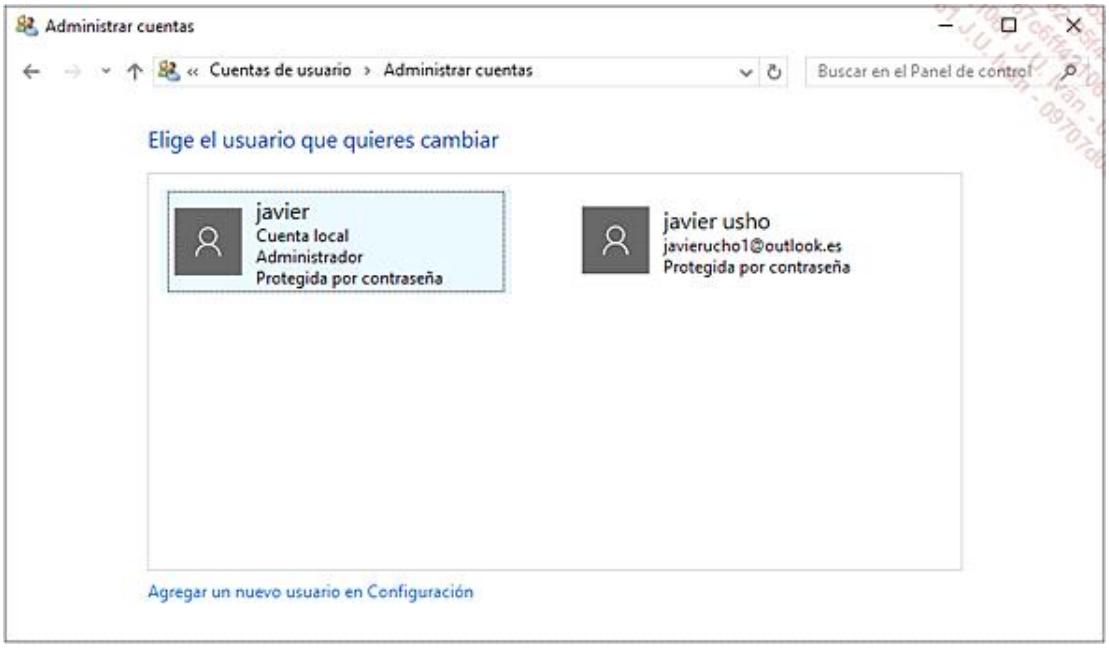
Al igual que en las versiones anteriores de los sistemas cliente de Microsoft, Windows 10 posee una base de datos con las cuentas y grupos locales, llamada SAM (*Security Account Manager*). El archivo SAM se almacena en la carpeta %systemroot%\System32\Config. El administrador puede, de esta forma, definir autorizaciones y permisos para una cuenta de usuario o de un grupo local en un ordenador específico.

Existen varios métodos que permiten administrar usuarios y grupos locales creados en un puesto de trabajo:

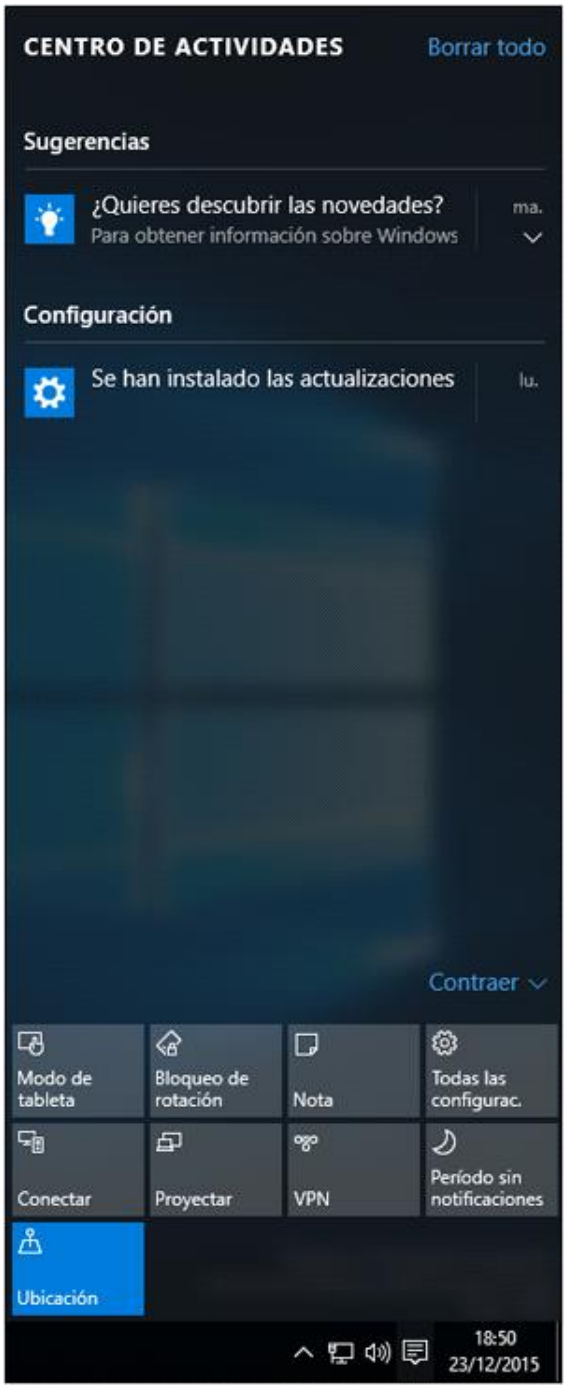
- Desde la consola **Administración de equipos**, pulsando las teclas  y **R** y escribiendo **compmgmt.msc**: despliegue el nodo **Usuarios y grupos locales**.
- Desde el panel de control: haga clic con el botón derecho en el menú **Inicio**, a continuación en **Panel de control**.

En el marco de las demostraciones presentadas en este libro, el autor usará los iconos pequeños para acceder más rápidamente al conjunto de funcionalidades presentadas en el Panel de control.

Haga clic en **Cuentas de usuario** de la **Ventana principal del panel de control** y, a continuación, en **Administrar otra cuenta**.



- Desde la configuración del PC: accesible de dos formas: haga clic en el menú **Inicio**, **Configuración** y luego en **Cuentas** o bien desde la esquina derecha de la barra de tareas, haga clic en el icono **Notificaciones** y luego en **Todas las configurac**.



Se crean tres cuentas que están deshabilitadas por defecto:

- Administrador: esta cuenta posee el control total del puesto con Windows 10 y permite definir autorizaciones suplementarias a los usuarios. Es aconsejable cambiarle el nombre. Durante el inicio de una sesión en modo seguro, incluso estando desactivada, esta cuenta puede ser utilizada. No puede borrarse.
- Invitado: esta cuenta se utiliza frecuentemente por personas sin cuenta en el ordenador. Tiene un radio de acción limitado.
- DefaultAccount: cuenta de usuario gestionada por el sistema.

Los siguientes grupos se crean durante la instalación de Windows 10 y permiten a sus miembros realizar acciones específicas:

- Administradores: incluye a los usuarios con privilegios de administrador.

- Administradores Hyper-V: acceso completo a las funciones de virtualización de Windows 10.
- Duplicadores: gestionan la replicación de archivos cuando el puesto es miembro de un dominio.
- IIS_IUSRS: utilizado por el servidor web Microsoft IIS.
- Invitados: contiene a los usuarios con privilegios limitados.
- Lectores del registro de eventos: visualización en modo lectura de los registros de eventos.
- Operadores de asistencia de control de acceso: requieren de forma remota los atributos de autorización y las autorizaciones a los recursos.
- Operadores criptográficos: están autorizados a cifrar los datos.
- Operadores de configuración de red: gestionan la configuración TCP/IPv4 y TCP/IPv6.
- Operadores de copia de seguridad: copian y restauran los datos en el ordenador.
- System Managed Accounts Group: los miembros de este grupo son gestionados por el sistema.
- Usuarios: poseen acciones limitadas, como la ejecución de programas o la impresión desde una impresora local.
- Usuarios avanzados: poseen permisos de administración limitados.
- Usuarios de administración remota: acceso a los recursos WMI por medio de los protocolos de gestión.
- Usuarios del monitor del sistema: visualizan los contadores.
- Usuarios del escritorio remoto: permiten conectarse de forma remota al equipo empleando el cliente de conexión remota.
- Usuarios del registro de rendimiento: configuran los contadores de rendimiento y los registran.
- Usuarios de COM distribuido: ejecutan y gestionan los objetos DCOM.

Cuando un usuario abre una sesión usando una cuenta con permisos limitados, puede utilizar el comando **runas** (ejecutado como) para incrementar su nivel de privilegios temporalmente y, de este modo, acceder a un recurso necesario. Se le solicitarán datos de identificación.

Usar el parámetro **/profile** con el comando **runas** permite cargar el perfil del usuario especificado. Para no cargarlo y de esta forma ejecutar la aplicación más rápidamente, utilice el parámetro **/noprofile**.

Dos métodos permiten ejecutar una funcionalidad con permisos aumentados: la primera desde la interfaz de usuario y la segunda empleando el comando mencionado previamente.

Cree una cuenta de usuario estándar y, a continuación, abra una sesión con ella:

- Haga clic en el menú **Inicio** con el botón derecho del ratón en **Símbolo de sistema (administrador)**. Haga clic en el botón **Sí** al aparecer la ventana de control de cuentas de usuario.
- La ventana **Símbolo de sistema** se ejecuta con privilegios avanzados. Cierre la ventana usando el comando **Exit** y, a continuación, haga clic en el menú **Inicio** con el botón derecho del ratón y luego en **Símbolo de sistema**.
- Escriba el comando: **runas /user:suloginadministrador explorer.exe** y, a continuación, introduzca la contraseña vinculada a la cuenta de administrador.

El explorador de Windows estará, en adelante, accesible como administrador.

Observe que, empleando el comando **winrs.exe**, el administrador puede ejecutar un comando en un equipo remoto con Windows 10. Este deberá autorizar el protocolo WS-Management creando una excepción en el firewall, con el comando **winrm quickconfig**.

Por ejemplo, para ejecutar el comando **ipconfig** en un equipo remoto: **winrs -r :EQUIPOREMOTO ipconfig**

6. Cuenta Microsoft

Mediante su cuenta Microsoft, al igual que con una cuenta de correo electrónico de Hotmail, el usuario puede abrir una sesión y recuperar sus propios parámetros y aplicaciones, así como sus documentos desde cualquier ordenador provisto de Windows 10. Este servicio está basado en Cloud Computing o la nube, que es un acceso bajo demanda a servidores virtuales mutualizados y disponibles desde la red Internet.

La ubicación de los datos del usuario en la nube es desconocida para él.

La autenticación mediante una cuenta Microsoft sincroniza los siguientes elementos:

- Aplicaciones descargadas desde Windows Store.
- Favoritos, temas, preferencias lingüísticas.
- Actualizaciones de sus redes sociales Facebook, Hotmail, Twitter, etc.
- Fotos y otros archivos almacenados en servicios como OneDrive, Flickr, etc.

La creación y configuración de la cuenta Microsoft puede iniciarse durante la fase de instalación de Windows 10 (consulte la sección DVD de instalación, de este capítulo), siempre que exista una conexión activa a Internet.

No obstante, el usuario puede utilizar este servicio después de la instalación del sistema siguiendo el procedimiento siguiente:

Haga clic en el menú **Inicio**, luego en **Configuración**, y a continuación en **Cuentas**. Haga clic en el botón **Conectarse a una cuenta Microsoft**.

Se invita al usuario a introducir su dirección de correo electrónico de Microsoft, o a crear una. Se requiere una conexión a Internet.

7. Protección infantil

Los niños usan cada vez más los ordenadores para jugar y aprender, pero también para chatear mediante las redes sociales. Los padres, preocupados por garantizar la protección de sus hijos, a menudo buscan una solución para controlar la actividad de estos en Internet. Puede ser interesante aportar una respuesta pedagógica a los problemas de seguridad creados por Internet y colocar el ordenador familiar en una habitación común. Sin embargo, la verificación regular de las acciones del niño tranquilizará a los padres. Windows 10 proporciona la funcionalidad **Protección infantil**, que emplea una cuenta Microsoft para hacer un seguimiento de la actividad del niño, sea cual sea la máquina desde la que inicia la sesión.

Se generan informes semanales de la actividad que luego se envían al correo electrónico de los padres. Cada modificación de la configuración del control parental se replica en todos los puestos mediante la nube y el sitio http://familysafety.microsoft.com.

El niño debe tener una cuenta estándar sin permisos de administrador para evitar que él mismo pueda modificar la configuración o instalar un malware.

En adelante, es posible definir las horas de uso del ordenador en función del día de la semana.

Para activar el control parental es necesario crear una cuenta en el ordenador:

- Haga clic en el menú **Inicio**, luego en **Configuración** y en **Cuentas**. Haga clic en **Familia y otros usuarios**. Haga clic en **Agregar familiar** y seleccione **Agregar un menor**. Introduzca la dirección e-mail del menor para que Windows 10 le envíe una invitación.
- El menor debe aceptar la invitación por e-mail y luego abrir una sesión en el equipo con Windows 10 empleando su dirección de e-mail.

Ahora procederemos a configurar los parámetros de la característica:

- Haga clic en el menú **Inicio**, luego en **Configuración** y **Cuentas**. Haga clic en **Administrar la configuración de la familia en línea** y seleccione los parámetros que se deben activar para la cuenta del menor según cuatro criterios:
  - **Actividad reciente**: permite visualizar los sitios visitados por el menor. Se pueden efectuar envíos semanales por e-mail de informes de actividad según su criterio.
  - **Exploración Web**: activa las restricciones relativas a los sitios web que pueden ser visitados por el menor en función de su edad o de una lista predefinida por Ud.
  - **Aplicaciones, juegos y multimedia**: activa restricciones para las aplicaciones y los juegos.
  - **Tiempo de pantalla**: permite definir los límites respecto a los horarios del día en que el menor puede utilizar los dispositivos de Windows, al igual que la duración máxima del tiempo que puede pasar diariamente frente a la pantalla.

En la sección **Familia y otros usuarios**, puede bloquear el acceso a su equipo de trabajo. No puede bloquear su propio nombre si es el único adulto. En ese caso, deberá crear antes una cuenta de adulto en el equipo con Windows 10.