

Cuentas de Windows

Transcribed on August 3, 2025 at 9:04 AM by Minutes AI

Speaker 1 (00:02)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las cuentas de Windows.

Vamos a hablar de las diferentes cuentas que podemos utilizar en un sistema operativo Windows, cómo seleccionar esas cuentas y qué implicaciones va a tener que seleccionemos una otra cuenta, vamos a ver cómo podemos administrar los usuarios de Windows y qué características vamos a tener disponibles para utilizar en el sistema operativo en función del tipo de usuario que nosotros elegimos.

Una de las primeras opciones que vamos a tener que decidir cuán estamos en el proceso de instalación del sistema operativo Windows es el tipo de cuenta que vamos a utilizar.

En las últimas versiones de los sistemas operativos WinWS, especialmente Windows 10 y Windows 11, se hace mucho hincapié en que la identidad que utilicemos para trabajar en el sistema operativo sea una identidad de la nube, es decir, una cuenta que puede ser una cuenta personal tipo una cuenta de una cuenta de una cuenta de Outlook o puede ser una cuenta empresarial tipo Office 365, lo que ahora se llama Microsoft 365 y esto nos va a permitir habilitar una serie de características, una serie de funcionalidades en el sistema operativo que nos van a ayudar a mejorar los diferentes aspectos de la utilización, la configuración, incluso algunos procesos de seguridad.

Otra de las opciones que tenemos es iniciar sesión con una cuenta local, es decir que vamos a iniciar sesión con una cuenta que o bien se va a almacenar en el dispositivo o bien se va a almacenar en un controlador de dominio si estamos en un entorno de dominio.

Basándonos en estas premisas vamos a tener por decirlo de alguna manera, dos tipos de identidades en Windows vamos a tener por un lado cuentas locales.

Estas cuentas locales no van a permitirnos en las últimas versiones del sistema operativo utilizar todas las características y características que como es lógico van a estar deshabilitadas, como por ejemplo la sincronización con OneDrive.

Si yo quiero sincronizar los datos del dispositivo con el almacenamiento que tengo en la nube, voy a precisar de una cuenta de la nube, no puedo hacerlo con una cuenta de usuario local.

Dentro de las cuentas de usuario local vamos a tener también dosos, aquellas cuentas para uso individual o para uso en el propio dispositivo, donde los secretos y las credenciales de esos usuarios se van almacenar en el propio dispositivo.

Todos los usuarios locales de un equipo Windows se almacena las credenciales y los secretos, las cuentas de ese usuario en un archivo de sistema que se llama el archivo SAM.

Ese archivo puede manipularse.

Hay herramientas que permiten desde un dispositivo que está apagado, habilitar acceso a ese archivo SAM.

Desde ahí incluso se pueden activar las cuentas de usuario, se pueden cambiar contraseñas, es decir, se puede vulnerar la seguridad de una identidad de una forma bastante elemental, bastante sencilla.

Por eso es importante cifrar el volumen del sistema.

Realmente es importante cifrar el disco duro, todos los discos duros que haya en los dispositivos.

De esta manera vamos a ayudar especialmente a proteger las identidades locales para que no se puedan utilizar estas herramientas, sino poder iniciar sesión con un usuario local del equipo.

Es una tarea trivial para cualquier atacante.

Y luego tenemos los usuarios de dominio, que también se almacenan de forma local, pero los usuarios de dominio no pertenecen a la identidad del equipo.

Los usuarios de dominio se van a almacenar de forma centralizada en un servidor que es el que gestiona el dominio, que se llaman controladores de dominio.

Estos controladores de dominio son los que van a tener una base de datos donde se van a almacenar los usuarios y los secretos y contraseñas de estos usuarios.

De tal forma que aunque hay ataques conocidos sobre las credenciales o más bien sobre los tokens que utilizan los usuarios dentro del directorio activo, generalmente no vamos a poder acceder a la clave o activar o desactivar el usuario desde el equipo local, desde el dispositivo cliente.

Tendríamos que atacar el controlador de dominio, que normalmente es una tarea bastante más compleja.

Si no queremos utilizar estos usuarios locales, tenemos la posibilidad hoy en día de trabajar con usuarios que estén en LAUB, pueden ser cuentas personales, por ejemplo, yo puedo crear una cuenta de Outlook o puedo crear una cuenta o puedo utilizar mi propia cuenta de Google para iniciar sesión en el equipo y de esta manera voy a poder sincronizar pues una serie de características o una serie de herramientas que voy a poder

En algunos casos se requiere una cuenta de Microsoft, es decir, que tiene que ser una cuenta de audio, por ejemplo, si yo quiero sincronizar con OneDrive, pues entonces tengo que utilizar esa cuenta DEO.

En algunos entornos o en entornos profesionales, normalmente se utiliza la cuenta de Microsoft 365 y este tipo de cuentas, las licencias y las características o productos que van a haber disponibles para cada usuario van a depender por un lado del tipo de cuenta en diferentes categorías de cuenta, una i, una i, etcetera, etcétera, o va a depender también de la configuración que se haga en la organización para estas identidades o para este tipo de cuentas.

Una vez que nosotros tenemos seleccionada la cuenta, vamos a poder administrar estas cuentas desde la consola de administración en la parte de configuración dentro de la parte de configuración de windows 10 o de windows 11 vamos a tener la posibilidad de crear cuentas, de administrar estas cuentas y básicamente vamos a trabajar con dos tipos de permisos en esas cuentas, cuentas que se hagan con privilegios de administrador o cuentas que sean tu usuario están lo recomendable es utilizar cuentas de usuario estándar y suelen utilizar cuentas como administrador para aquellas tareas específicas que requieran esos privilegios también.