Bancolombia

Procedimiento para la estandarización de los equipos dentro del dominio Bancolombia.

Indice

Objetivo:

El propósito de este documento es informar sobre el proceso para el correcto ingreso de los equipos al dominio de Bancolombia, teniendo en cuenta los criterios establecidos según el estándar de nombres para cada área y sede.

A continuación, se detalla el procedimiento a seguir:

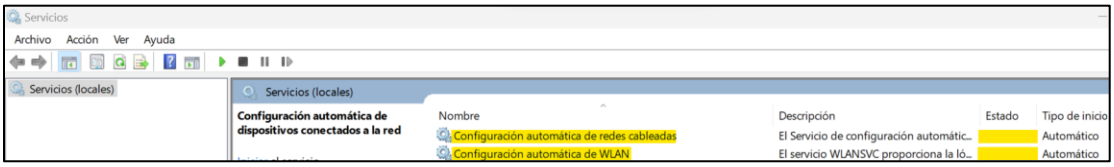
Bancolombia

Para todo alistamiento e ingreso de equipos al dominio de Bancolombia, es fundamental seguir el orden de los puntos que se presentan en este manual.

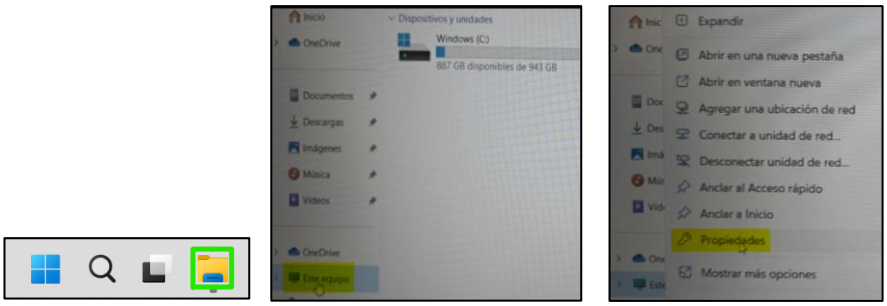
1. Inicio y Alistamiento inicial del equipo.

- Sin conectar el equipo al cable de red, se realiza el encendido e inicio de sesión utilizando la contraseña de Administrador.

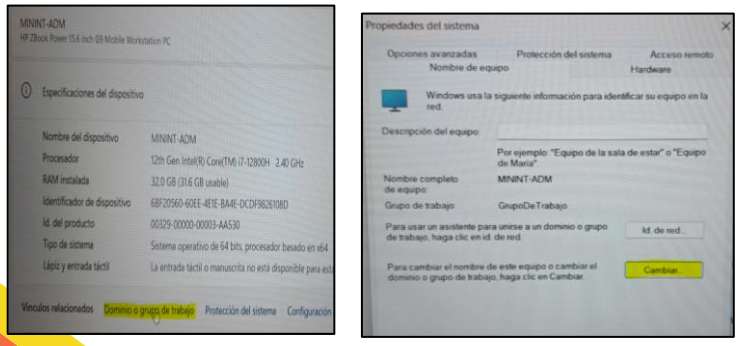
- Debemos garantizar que los servicios de **“Configuración automática de redes CABLEADAS y WLAN”,** se encuentren **Detenidos Antes de conectar el cable de red**, tal como se muestra a continuación:



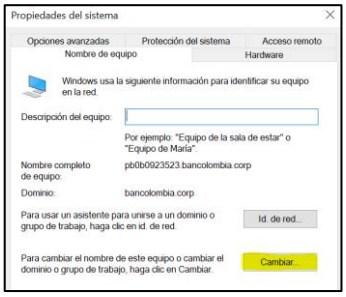
- Luego, abrimos el explorador de archivos, hacemos clic derecho en la opción “**Este Equipo**” y seleccionamos “**Propiedades**”.



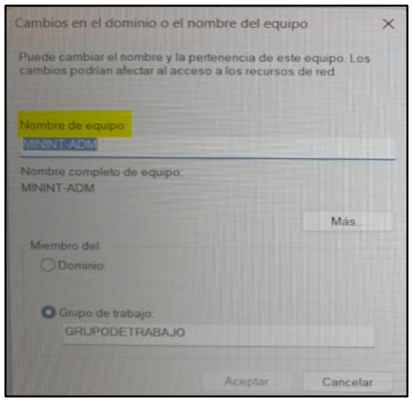
- En Windows 11, seleccionamos la opción “**Dominio o grupo de trabajo**” y, en el siguiente recuadro, hacemos clic en la opción “**Cambiar**”.



- En Windows 10, seleccionamos la opción “**Cambiar el nombre de este equipo (avanzado)**” y, en el siguiente recuadro, hacemos clic en la opción “**Cambiar**”.



- En el siguiente recuadro, certificamos que el nombre de equipo “**MININT**” corresponda con el estándar de cada sede. Luego, hacemos clic en “**Aceptar**” y realizamos el primer reinicio.



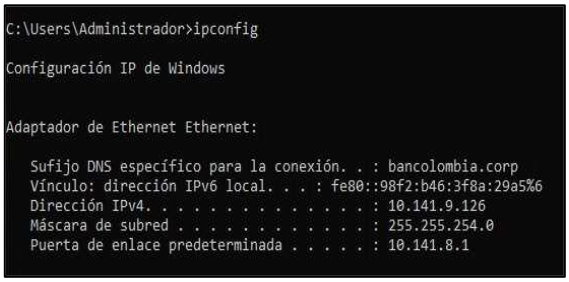
MININT-ADM	**(Sedes Administrativas)**
MININT-SUC	**(sucursales)**
MININT-GZ	**(Gerencias de Zonas)**

2. Toma de red para aprovisionamiento e instalación de certificados.

Para todo el proceso de alistamiento, ingreso al dominio, configuración de perfiles y aplicación de políticas, el equipo debe estar siempre conectado al cable de red.

- Después del primer reinicio, conectamos el equipo al cable de red y volvemos a iniciar sesión como Administrador. Verificamos que el equipo haya obtenido una IP para alistamiento, que debe estar en el rango “**10.141.x.x**”, como se muestra en la imagen siguiente. Este proceso puede tardar de 3 a 5 minutos en completarse.

Se abre el CMD y se ejecuta el comando **ipconfig**



- Si después de 5 minutos obtienes una IP APIPA (169.x.x), es necesario comunicarte con Nivel 1 TIGO Mesa de Bancolombia al (444 94 53, opción 3) para solicitar la eliminación del endpoint de ClearPass de la red cableada y wifi. Debes proporcionar la dirección MAC del equipo. Después de realizar esta solicitud, desconecta y vuelve a conectar el cable de red.

- “Durante esta desconexión, se llevará a cabo el proceso de perfilamiento de la máquina, por lo que debes esperar aproximadamente 3 a 5 minutos. Desconecta y conecta el cable nuevamente para que se le asigne la dirección IP correcta en el rango 10.141.x.x.”

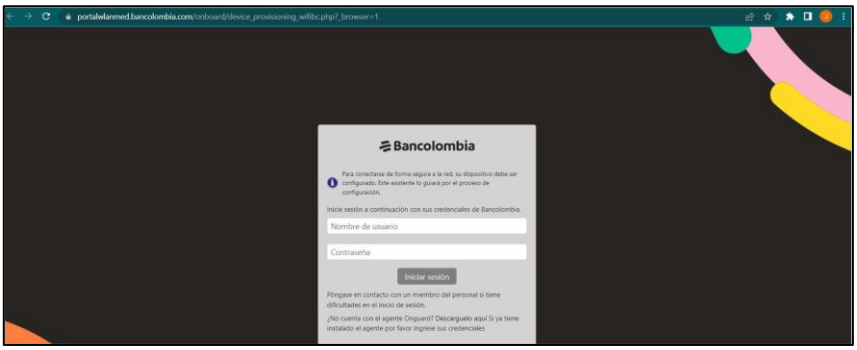
Plantilla de escalamiento:

· Incidente/Orden:
· Nombre del dispositivo:
· Mac Address:
· Equipo: Nuevo/Existente
· Estado del servicio Configuración automática de redes cableadas:
· Certificados en el repositorio de maquina: Si - No - N/A
· Certificados en el repositorio usuario: Si - No - N/A
· Breve descripción de la falla que presentada:

- Luego, procedemos a cargar el portal de Onboarding utilizando la siguiente URL, que abrirá la página correspondiente:

En la carpeta “TEMP” del equipo, encontraremos un archivo llamado “Onboarding Clear Pass”, el cual contiene la URL. En caso de no encontrar este archivo, deberás ingresar la URL manualmente.

https://portalwlanmed.bancolombia.com/onboard/device_provisioning_wifibc.php



- Se ingresa el usuario y la contraseña de red de Bancolombia proporcionados por el ingeniero de Unisys. Tras la autenticación, se descargará el ejecutable QuickConnect. Selecciona la opción “Iniciar QuickConnect” para proceder.

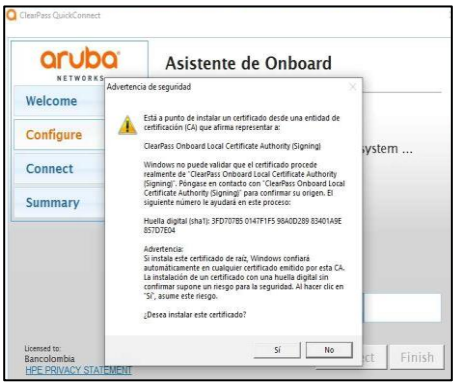
- Durante el proceso de descarga, verifica que el archivo se haya descargado completamente. En algunos modelos de máquinas, es necesario hacer clic en "Conservar" en la opción de descargas del navegador para asegurar que la descarga se complete correctamente.

- Luego, ejecuta el asistente Quick Connect y sigue los pasos que se indican a continuación.

- Haz clic en "Next" (Siguiente).

- El asistente iniciará solicitando la instalación de los certificados de root de Bancolombia y Onboarding

"Selecciona la opción "**Si**" desea instalarlos. Este proceso tendrá una duración aproximada de 5 minutos.



- Para los "Portátiles", se mostrarán las opciones "Wi-Fi" y "Ethernet". Para las "CPU", solo se mostrará la opción "Ethernet"**.**

- A partir de este momento, la máquina queda configurada con las tarjetas de red correspondientes: (Ethernet y Wi-Fi) o solo (Ethernet), dependiendo del tipo de máquina y del certificado aprovisionado.

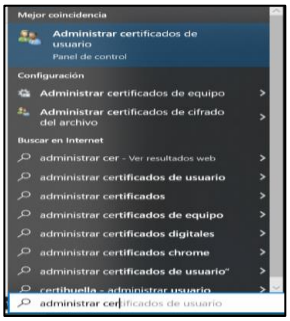
Bancolombia

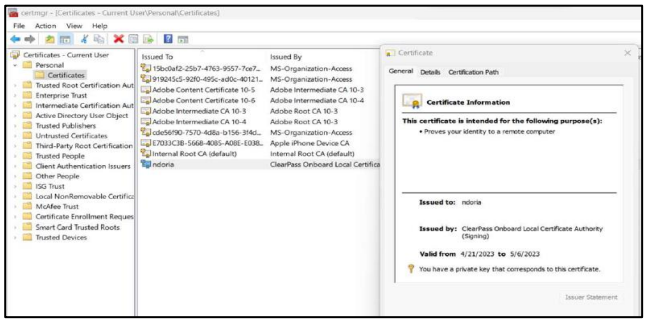
Estos certificados son únicamente para el aprovisionamiento. Es importante asegurarse de que la máquina obtenga los certificados correspondientes para el usuario y el equipo, que son "BCUSUARIOS" y "BCESTACIONES". Estos certificados se mostrarán más adelante.

3. Certificados para aprovisionamiento y configuración de la tarjeta de red.

3.1. Confirmar la instalación del certificado de usuario y configuración de tarjetas de red.

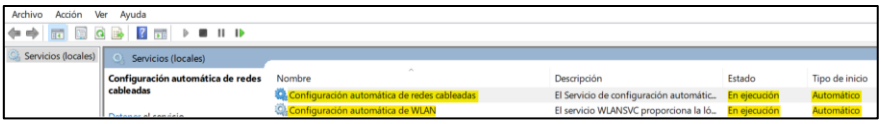
- Procedemos a acceder al repositorio de certificados de usuarios. Hacemos clic en "Personal" y luego en "Certificados". Confirmamos el certificado para aprovisionamiento denominado "**ClearPass Onboard Local".**



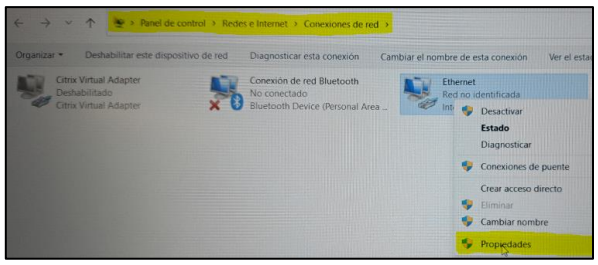


3.2. Configuración de las tarjetas de red.

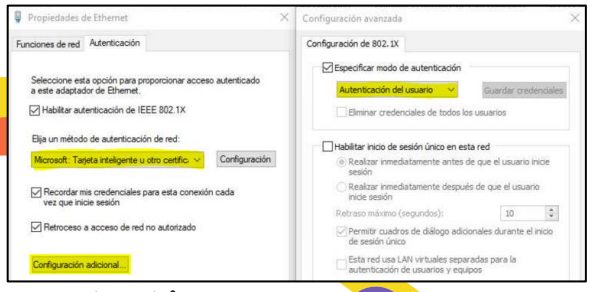
- Debemos garantizar que los servicios de **"Configuración automática de redes CABLEADAS y WLAN",** estén en ejecución y configurados para iniciarse automáticamente, como se muestra a continuación:

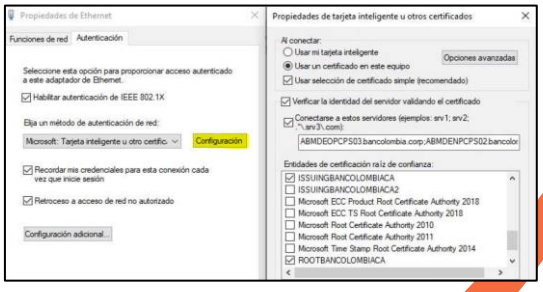


- Luego, accedemos al Panel de control, seleccionamos "Centro de redes y recursos compartidos", y luego "Cambiar la configuración del adaptador". Finalmente, hacemos clic derecho en "Propiedades" de la tarjeta de red Ethernet. **(Las opciones están resaltadas en amarillo en la imagen).**



- Verificamos que las configuraciones de la tarjeta de red aparezcan como se muestra a continuación. **(Las opciones están resaltadas en amarillo en la imagen)**.





- Después de realizar estas validaciones, procedemos a verificar en CMD. La IP debe estar en el segmento 10.99.x.x y 10.100.x.x, como se muestra a continuación.

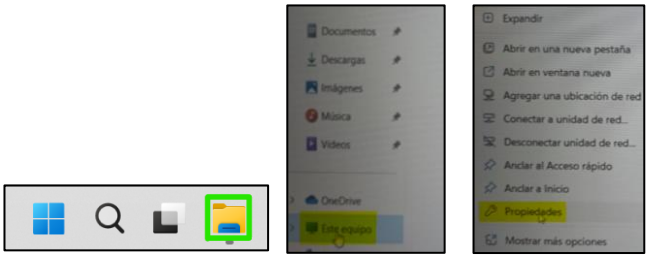
- Si no recibes una IP, procede a desconectar el cable, esperar 1 o 2 minutos y luego volver a conectarlo.

- Si después de 5 minutos no obtienes una IP en el rango 10.99.x.x o 10.100.x.x, es necesario comunicarte con Nivel 1 TIGO Mesa de Bancolombia al (444 94 53, opción 3) y proporcionar la dirección MAC del equipo. Luego, desconecta y vuelve a conectar el cable.

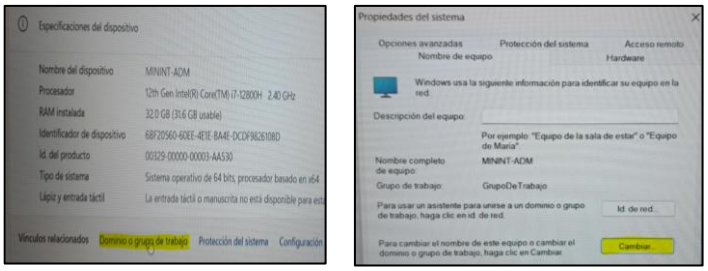
4. Ingreso al Dominio y grupos de seguridad.

4.1. Ingreso del equipo al Dominio.

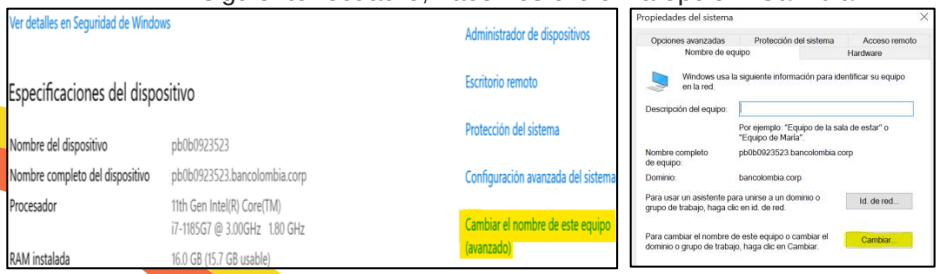
- Abrimos el explorador de archivos, hacemos clic derecho en **“Este Equipo”,** luego **“propiedades”.**



- En **Windows 11**, seleccionamos la opción “**Dominio o grupo de trabajo**” y, en el siguiente recuadro, hacemos clic en la opción “**Cambiar**”.



- En **Windows 10**, seleccionamos la opción “**Cambiar el nombre de este equipo (avanzado)**” y, en el siguiente recuadro, hacemos clic en la opción “**Cambiar**”.



- En el siguiente recuadro, donde dice **“Nombre de Equipo”,** ingresamos el nombre correspondiente según el Manual oficial “**Anexo Estándar Nombres Servidores y Estaciones**”, ubicado en el servidor de medios en la siguiente ruta:

- **\\sbmdedsa02v\Instaladores\Estaciones\Estandar nombre de estaciones**

IMPORTANTE: Debes tener en cuenta a cuál organización pertenecerá el colaborador para nombrar el equipo correctamente. En el siguiente recuadro de organizaciones encontrarás ejemplos actuales.

Ejemplos:

EQUIPOS ADMINISTRATIVOS: “pb0b0923523”, “pf0f923465”, “pn0b0925342”, “mb0b0993123”, “rb0b0883123”, “ib0b0773123”, “tb0b0663123”.

Organizaciones
b0 “Bancolombia”
l0 “Leasing Colombia”
f0 “Fiduciaria”
v0 “Valores Bancolombia”
n0 “Nequi”

EJEMPLO DE LA PLACA

Tipo de Dispositivo	Indicativo	Organizaciones	Placa del equipo= Se debe agregar la placa del equipo
“portátil”	p	b0	b0123456
“Desktop”	d	l0	l0123456
“MAC portátil”	m	f0	f1234567
“MAC Desktop”	e	b0	b0123456
“Robot”	r	v0	v0123456
“IPad”	i	b0	b0123456
“Tablet Administrativa”	t	b0	b0123456

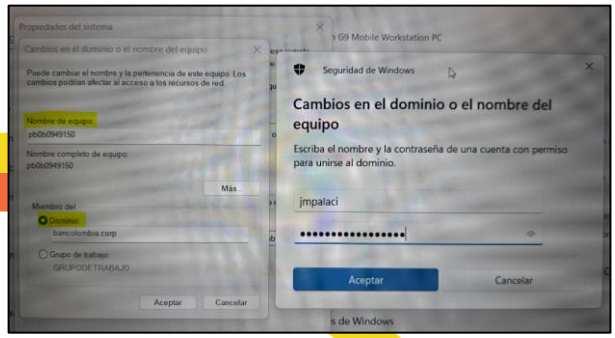
EQUIPOS SUCURSALES: “b0348as01”, “bt0001edu01”.

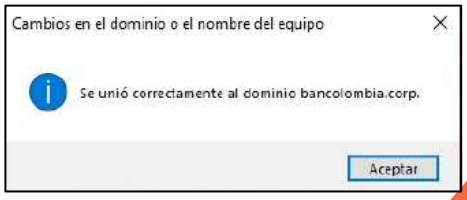
TIPO DE DISPOSITIVO	INDICATIVO	CODIGÓ SUCURSAL	CARGO	CONSECUTIVO
“Portátil y Desktop Sucursal”	b	0348	as	01
“Tablet Sucursal”	bt	0001	edu	01

EQUIPOS AUTOPILOT: “PBA02128WZ2”, “DBA02128WZ2”

Tipo de Dispositivo	Indicativo	Organizaciones	Alistamiento= A significa (Autopilot)	Serial del equipo= Se debe certificar que tenga el serial del equipo
“portátil”	p	b	a0	2128WZ2
“Desktop”	d	b	a0	2128WZ2

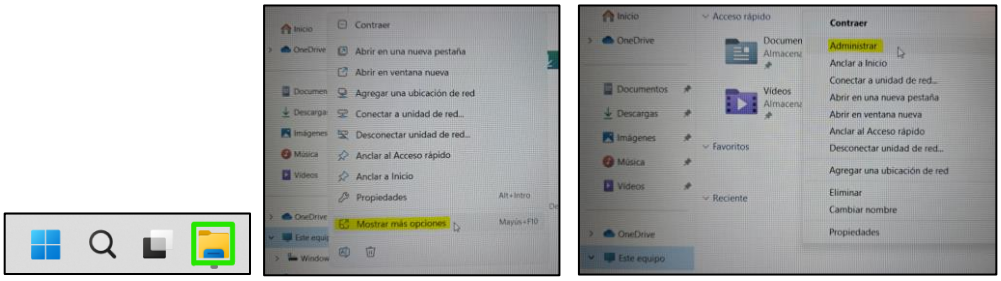
- Ingresamos el nombre del equipo y el dominio, que en este caso es “**bancolombia.corp**”. Hacemos clic en “Aceptar”, y aparecerá un recuadro solicitando usuario y contraseña. Introducimos las credenciales del ingeniero, hacemos clic en “Aceptar” y deberíamos recibir un mensaje de confirmación.



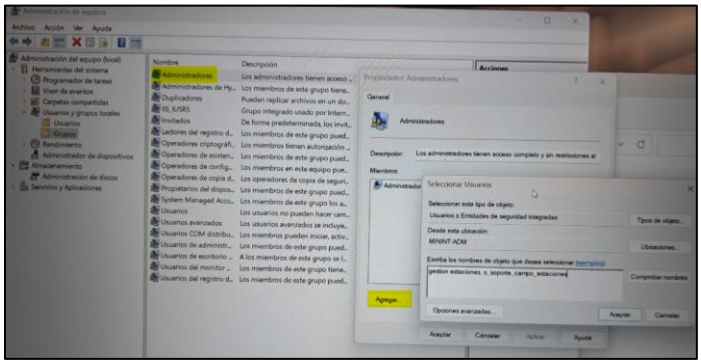


4.2. Asignación de los grupos de seguridad “Gestión Estaciones y s_soporte_campo_estaciones”.

- Abrimos el explorador de archivos y hacemos clic derecho en **“Este Equipo”.** En Windows 11, seleccionamos “Más opciones” y luego “Administrar”. En Windows 10, simplemente hacemos clic derecho y seleccionamos “Administrar”.



- Procedemos a ingresar a “Usuarios y grupos”, luego a “Grupos”, seleccionamos “Administradores” y hacemos clic en “Agregar”. Allí debemos ingresar los grupos “**Gestión Estaciones**” y “**S_SOPORTE_CAMPO_ESTACIONES**” de manera individual.

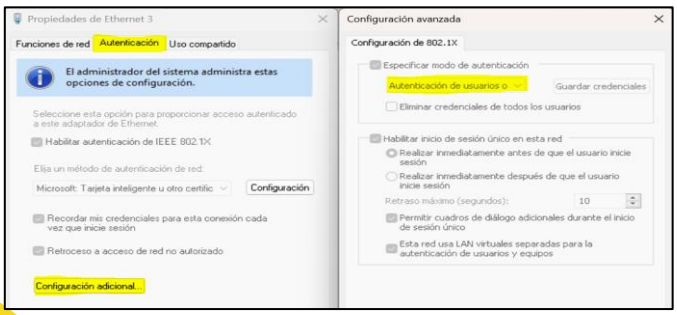


- Después de agregar los grupos, hacemos clic en “Aceptar” y cerramos las ventanas.

4.3. Modificación de parámetros en la tarjeta de red.

- Debemos modificar el parámetro de autenticación nuevamente desde el Panel de control.

Autenticación >configuración adicional >Configuración de 802.1x> Autenticación de usuarios o equipos



- Después de confirmar, procedemos con el segundo reinicio para continuar con el inicio de sesión del ingeniero.

Bancolombia

5. Configuraciones, carga de políticas de dominio y aplicaciones de línea base.

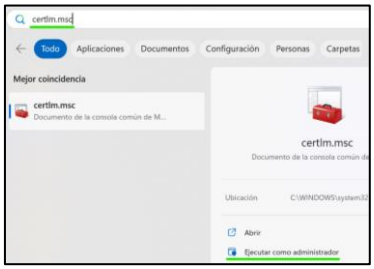
En este punto, se debe esperar exactamente 20 minutos para que el equipo se mueva a la OU correspondiente y se apliquen las políticas de dominio. Después de este tiempo, procedemos con el tercer reinicio.

- Si el inicio de sesión con el perfil del ingeniero no funciona, procede a iniciar sesión nuevamente con el perfil de administrador. Luego, continúa con el paso 5.2 del manual, espera los 20 minutos y realiza un reinicio.

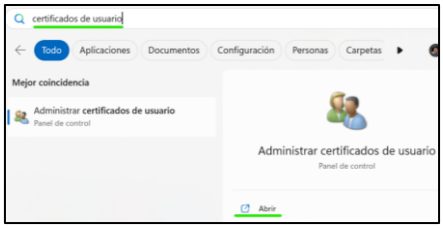
5.1. Inicio de sesión con el perfil del ingeniero.

- Procedemos a verificar que el equipo tenga los certificados de red adecuados:

- Para el certificado de equipo, abrimos el buscador, digitamos certlm.msc y lo ejecutamos como administrador. Debería mostrarse el certificado de equipo llamado "**BCESTACIONES_(SHA2)".**



- Para el certificado de usuario, en el buscador digitamos "certificados de usuario" y buscamos el certificado llamado **"BCUSUARIOS_(SHA2)".**



- Si por algún motivo el equipo queda sin conexión de red después de unos minutos, esto puede deberse a que el usuario no tiene el certificado correspondiente en la sesión iniciada. Para restablecer la conexión de red, es necesario confirmar el certificado de usuario y asegurarse de que se apliquen las GPO de red.

- Este certificado debería importarse automáticamente. Si no es así, solicita una excepción a Nivel 1 TIGO Mesa de Bancolombia (444 94 53, opción 3), indicando que se requiere importar el certificado de red. Para esto, proporciona la dirección MAC de la red cableada. Después, es necesario desconectar y volver a conectar el cable.

Plantilla de escalamiento:

· Incidente/Orden:
· Nombre del dispositivo:
· Mac Address:
· Equipo: Nuevo/Existente
· Estado del servicio Configuración automática de redes cableadas:
· Certificados en el repositorio de maquina: Si - No - N/A
· Certificados en el repositorio usuario: Si - No - N/A
· Breve descripción de la falla que presentada:

5.2. Validación de aplicaciones para línea Base.

- En este punto, se debe garantizar que las aplicaciones de línea base estén instaladas. Si no están presentes, deben instalarse. A continuación, se presentan las aplicaciones de línea base que deben certificarse en los equipos de Bancolombia:

ITEM	Software X imagen estándar Bancolombia	Versión	Estándar Administrativo	Estándar Sucursal
1	Sistema Operativo	Windows 10 y 11 (22H2)	X	X
2	Unido al dominio	bancolombia.corp	X	X
3	Adobe Acrobat Reader DC - Español		X	X
4	Aplicaciones de Microsoft 365 para empresas es-es		X	X
5	Atención al cliente		X	X
6	Citrix Workspace		X	X
7	ClearPass OnGuard MSI Extractor		X	X
8	Cloudflare WARP		X	X
9	Configuration Manager Client		X	X
10	CrowdStrike Windows Sensor		X	X
11	HP Insights	Tech Pulse (Herramienta predictiva)	X	X
12	HP Insights Analytics		X	X
13	HP Insights Analytics - Dependencies		X	X
14	Lexmark Phone Book		X	X
15	Lexmark Printer Driver Configuration Utility		X	X
16	Lexmark ScanBack Utility		X	X
17	Local Administrator Password Solution		X	X
18	Microsoft Azure Information Protection		X	X
19	Microsoft Edge		X	X
20	Microsoft Silverlight		X	X
21	Microsoft Teams		X	X
22	Microsoft Visual C++ 2008 Redistributable (x86)			X
23	Microsoft Visual C++ 2013 Redistributable (x64)		X	X
24	Microsoft Visual C++ 2013 Redistributable (x86)		X	X
25	Microsoft Visual C++ 2013 x86 Additional Runtime			X
26	Microsoft Visual C++ 2013 x86 Minimum Runtime			X
27	Microsoft Visual C++ 2015-2022 Redistributable (x64)		X	X
28	Microsoft Visual C++ 2015-2022 Redistributable (x86)		X	X
29	Nessus Agent (x64)		X	X
30	Netskope Client		X	X
31	Paquete de controladores de Windows - Lexmark international Printer		X	X
32	Paquete de controladores de Windows - Lexmark international Printer		X	X
33	Remote Help		X	X
34	Webex		X	X
35	WebView2 Runtinede Microsoft Edge		X	X
36	Automation Anywhere Enterprise Client			X
37	Golf Sif Branch			X
38	Hclient			X
39	IBM Ondemand Clients			X
40	Micro Focus My Extra (AS400)			X
41	Who is Who Bancolombia			X

Bancolombia

6. Inicio de sesión con el perfil del usuario final.

Si en este punto el equipo aún se encuentra en la OU de Aprovisionamiento, debe moverse manualmente desde el Power APP. Para esto, sigue el punto 10 del Manual. Es importante asegurar que el equipo esté en la OU correspondiente para que los demás procesos se ejecuten correctamente.

6.1. Inicio de sesión con el perfil del usuario final y revisión de la Unidad Organizacional.

- Se realiza el inicio de sesión con el perfil del usuario final. En este punto, se debe esperar 25 minutos antes de realizar el cuarto reinicio. Durante este tiempo, se deben revisar la OU, personalizar el perfil, y finalizar cualquier instalación adicional, entre otros.

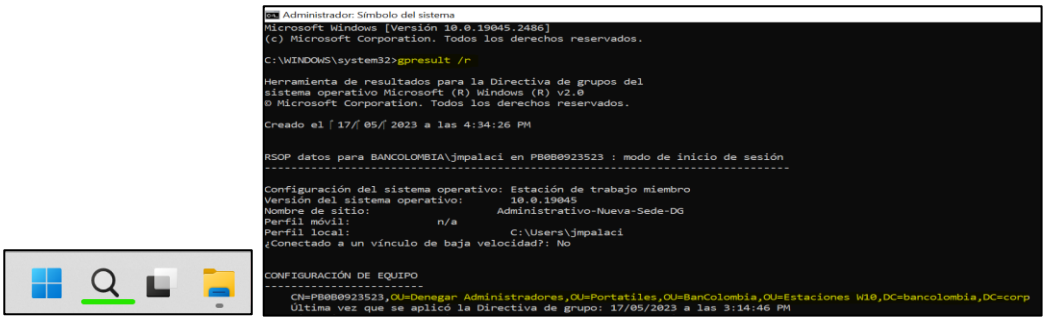
Tipos de OU:

Tipo de dispositivo	OU (Unidad Organizacional)
Desktop Administrativo	OU=Denegar Administradores, OU=Administrativas, OU=Bancolombia, OU=Estaciones W10, DC=Bancolombia, DC=corp
Portátil Administrativo	OU=Denegar Administradores, OU=Portátiles, OU=Bancolombia, OU=Estaciones W10, DC=Bancolombia, DC=corp
Desktop y Portátil Sucursal	OU=Denegar Administradores, OU=Sucursales, OU=Bancolombia, OU=Estaciones W10, DC=Bancolombia, DC=corp
RPA "Robótica"	OU=RPA, OU=Especiales, OU=Bancolombia, OU=Estaciones W10, DC=Bancolombia, DC=corp
Tablet Administrativa y Sucursal	OU=Tablets, OU=Especiales, OU=Bancolombia, OU=Estaciones W10, DC=Bancolombia, DC=corp

Tipo de dispositivo	OU (Unidad Organizacional)
Desktop Nequi	OU=Denegar Administradores, OU=Administrativas, OU=Nequi, OU=Estaciones W10, DC=Bancolombia, DC=corp
Portátil Nequi	OU=Denegar Administradores, OU=Portátiles, OU=Nequi, OU=Estaciones W10, DC=Bancolombia, DC=corp

- Para ejecutar el comando **GPRESULT /R**, debes asegurarte de que la sesión del ingeniero ya esté iniciada en el equipo; de lo contrario, no se obtendrá la información del equipo.

- En el buscador, digitamos "CMD", abrimos el símbolo del sistema como administrador y ejecutamos el comando **GPRESULT /R**. Esto debe mostrar la OU actual del equipo.



6.2. Verificación de políticas de dominio, directivas de seguridad y grupos de seguridad.

- Procedemos a abrir el símbolo del sistema (CMD) como Administrador y ejecutamos el comando gpresult /r. Esto debe mostrar la siguiente información:

6.2.1. Para equipos con Windows 11, debemos garantizar que aparezcan los siguientes grupos en la sección correspondiente:

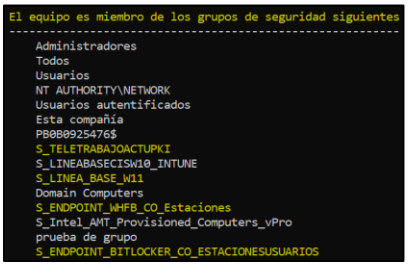
"El equipo es miembro de los grupos de seguridad siguientes"

S_LINEA_BASE_W11 (Este es el grupo principal que identifica el sistema operativo del equipo y, en función de este criterio, aplica las políticas de red correspondientes).

S_TELETRABAJOACTUPKI (Este es el grupo encargado de aplicar la autenticación en la red mediante un certificado).

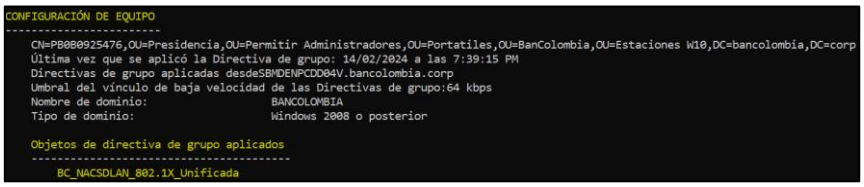
S_ENDPOINT_WHFB_CO_Estaciones (Este es el grupo encargado de aplicar configuración del Windows Hellow).

S_ENDPOINT_BITLOCKER_CO_ESTACIONESUSUARIOS (Este es el grupo encargado de ejecutar la sincronización para el cifrado de discos).



“objetos de directiva de grupo aplicados”

BC_NACSDLAN_802.1X_Unificada (Esta es la política encargada de gestionar la autenticación para equipos con Windows mediante certificados de red, aplicando tanto a equipos portátiles como de escritorio).



6.2.2. Para equipos con Windows 10, debemos garantizar que aparezcan los siguientes grupos en la sección correspondiente:

“el equipo es miembro de los grupos de seguridad siguientes”

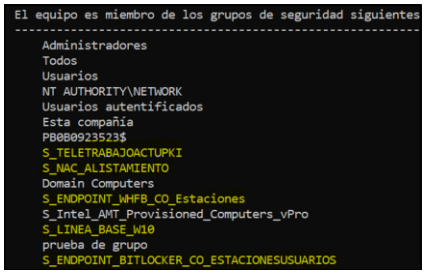
S_LINEA_BASE_W10 (Este es el grupo principal que identifica el sistema operativo del equipo y, en función de este criterio, aplica las políticas de red correspondientes).

S_TELETRABAJOACTUPKI (Este es el grupo encargado de aplicar la autenticación en la red mediante un certificado).

S_NAC_ALISTAMIENTO (Este es el grupo encargado de aplicar la política de autenticación en la red mediante certificados para equipos con Windows 10).

S_ENDPOINT_WHFB_CO_Estaciones (Este es el grupo encargado de aplicar configuración del Windows Hellow).

S_ENDPOINT_BITLOCKER_CO_ESTACIONESUSUARIOS (Este es el grupo encargado de ejecutar la sincronización para el cifrado de discos).



“objetos de directiva de grupo aplicados”

BC_NACSDLAN_802.1X_Unificada (Esta es la política encargada de gestionar la autenticación para equipos con Windows mediante certificados de red, aplicando tanto a equipos portátiles como de escritorio).

BC_NAC_ETH_802.1X (Esta política se encarga de gestionar la autenticación para equipos con Windows 10 mediante EAP, aplicando tanto a equipos portátiles como de escritorio).

BC_NAC_WIFI_802.1X (Esta política se encarga de gestionar la autenticación para equipos con Windows 10 mediante EAP, aplicando a aquellos equipos que cuenten con una tarjeta de red Wi-Fi).

```
CONFIGURACIÓN DE EQUIPO
-----------------------
    CN=PB0B0925476,OU=Presidencia,OU=Permitir Administradores,OU=Portatiles,OU=BanColombia,OU=Estaciones W10,DC=bancolombia,DC=corp
    Última vez que se aplicó la Directiva de grupo: 14/02/2024 a las 7:39:15 PM
    Directivas de grupo aplicadas desdeSBMDENPCDD04V.bancolombia.corp
    Umbral del vínculo de baja velocidad de las Directivas de grupo:64 kbps
    Nombre de dominio:                  BANCOLOMBIA
    Tipo de dominio:                    Windows 2008 o posterior

    Objetos de directiva de grupo aplicados
    ---------------------------------------
        BC_NACSDLAN_802.1X_Unificada
        Estaciones Windows10 Presidencia
        BC_ESP_MaquinasBancolombia_W10
        BC_NAC_WIFI_802.1X
        BC_Contingencia_Covid19_Computer
        BC_NAC_ETH_802.1X
```

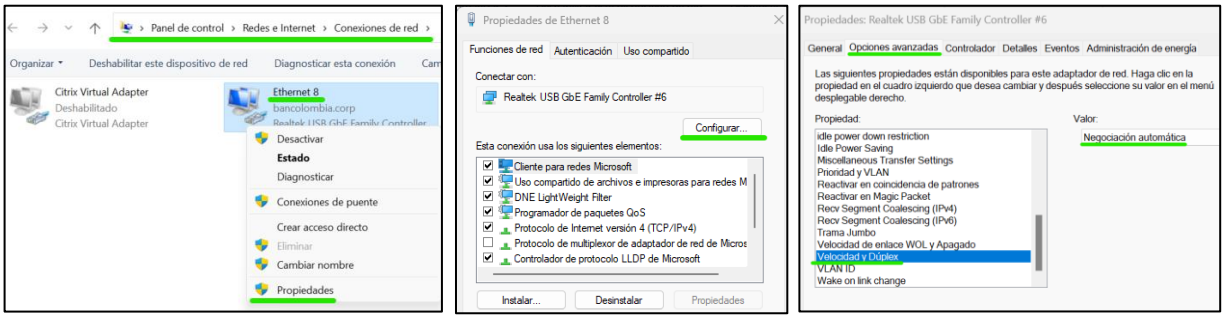
7. Configuración de parámetros finales en las tarjetas de red.

Siempre que se realice una intervención en un equipo de cómputo, se debe garantizar la actualización de todos los drivers y controladores, ya sea que el equipo sea nuevo o que ya esté en operación. Es crucial que el equipo esté conectado a la energía para completar el proceso de actualización.

- Para realizar la correcta actualización de los drivers y controladores, se debe seguir el paso a paso del manual titulado “Actualización de Drivers y Controladores en Equipos Bancolombia”.

7.1. Tarjeta de red Cableada.

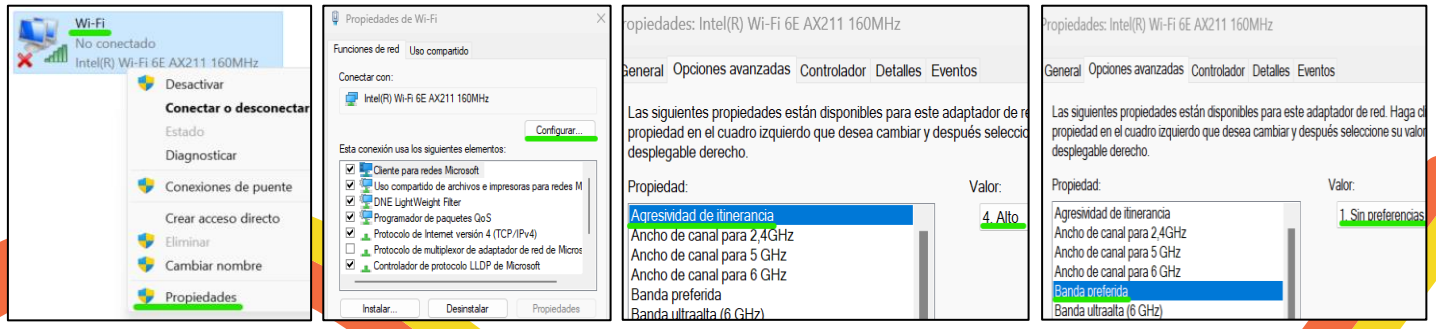
- Procedemos a ir al Panel de control, luego a “Centro de redes y recursos compartidos”, seleccionamos “Cambiar configuraciones del adaptador”, y hacemos clic derecho en “Propiedades” de la tarjeta de red Ethernet. Asegúrate de que la opción esté configurada en “Negociación automática”.



7.2. Tarjeta de red Wifi.

- Procedemos a ir al Panel de control, luego a “Centro de redes y recursos compartidos”, seleccionamos “Cambiar configuraciones del adaptador” y hacemos clic derecho en “Propiedades” de la tarjeta de red Wi-Fi.

- Debes configurar la “Agresividad de itinerancia” en “Alto” y la “Banda preferida” en “Sin Preferencias”.



8. Procedimiento para la clave de la BIOS en equipos HP.

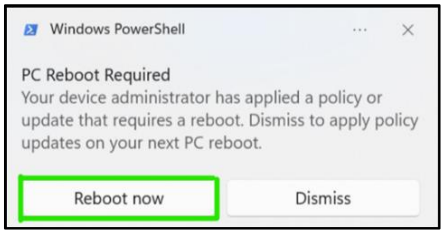
8.1. Certificación de clave de BIOS.

- Reinicia el equipo e ingresa a las diferentes opciones de la BIOS presionando las teclas F9, F10, F11, o F12 durante el arranque.

- Si el equipo ya tiene una clave de BIOS establecida, al intentar acceder a la configuración de la BIOS, se te pedirá ingresar la contraseña:

8.2. Certificación del proceso para la clave de BIOS.

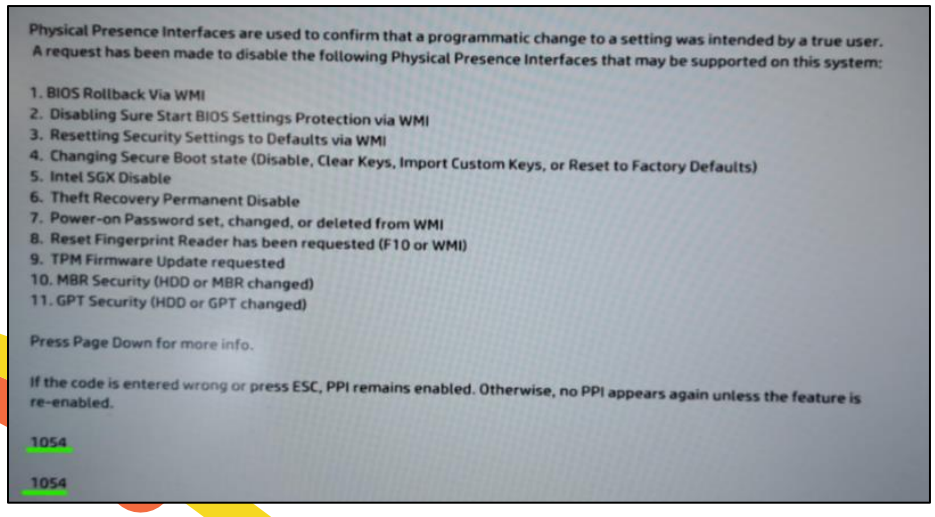
- Si no se cumple con el paso anterior durante la estandarización del equipo, debes estar atento al siguiente mensaje. Selecciona la opción “Reboot Now” para realizar un reinicio del equipo.



- Luego del reinicio, debería aparecer una ventana en blanco, como se muestra a continuación:

IMPORTANTE: Se debe identificar el código que se muestra en la pantalla al momento de reiniciar (este código es aleatorio). Debes ingresarlo utilizando el teclado numérico del equipo y, finalmente, presionar “Enter”.

Imagen Ejemplo

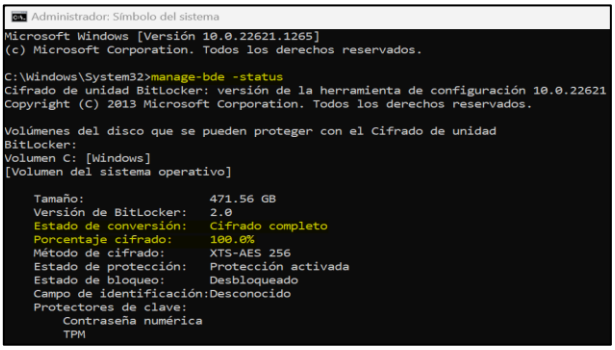


9. Validar estado del Bitlocker y Modo hibrido.

9.1. Bitlocker

- Procedemos a ejecutar un CMD como Administrador y ejecutamos el comando manage-bde -status. Este comando debe proporcionar la siguiente información:

- El estado del cifrado debe mostrar un “% en proceso" o "100%" en los discos, tal como se ilustra en la imagen siguiente.

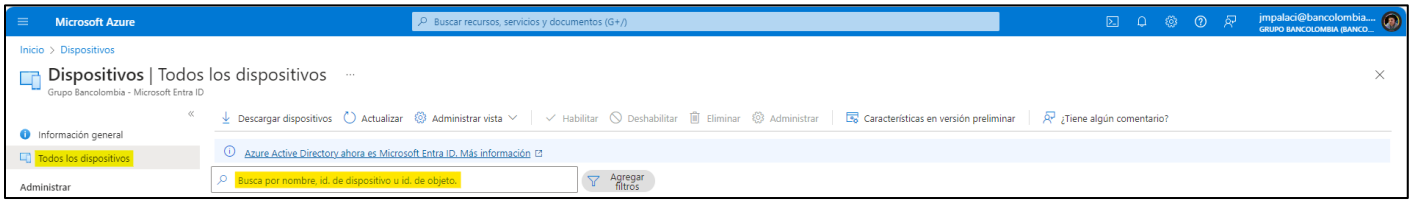


9.2. Modo hibrido

- Para verificar si el Modo Híbrido ya está operativo, debemos ingresar a la siguiente URL:

[Dispositivos - Microsoft Azure]

- Seleccionamos la opción “Todos los Dispositivos” y luego utilizamos la lupa en “Buscar por nombre” para ingresar el nombre del equipo. Debemos esperar a que el equipo aparezca en Azure con la “Versión” y el “Tipo de combinación”, tal como se muestra en la imagen siguiente:



- Para que el procedimiento finalice de manera exitosa, no se debe forzar ningún proceso; es importante realizar las verificaciones en Azure.

- Mientras el equipo completa sus sincronizaciones con los diferentes servidores y consolas, continúa con la estandarización del equipo, la configuración del perfil, la instalación y configuración de aplicaciones faltantes, y la prueba de los aplicativos ya instalados y configurados. Al finalizar este proceso, reinicia el equipo.

- Si el equipo entra en modo Híbrido antes de lo previsto, el colaborador puede concluir las configuraciones y pruebas, y luego proceder con la entrega final.

10. Movimiento y Borrado de equipos.

El movimiento desde la Power APP solo debe utilizarse en caso de contingencia, cuando el proceso de movimiento automático no esté funcionando. Por ejemplo, si después de los primeros 20 minutos el equipo aún no ha tomado la OU correspondiente.

- Ingresamos al siguiente enlace.:

APB043356_RANGERS_AUTOGESTIÓN - Power Apps

- Para profundizar en las funcionalidades, se debe consultar el manual titulado “Manual_Portal_Autogestion_Usuarios”.

- A continuación, una breve explicación de las siguientes funcionalidades:

1- **Eliminación de máquinas:** Este punto nos ayudará con la eliminación de los equipos registrados en Configuration Manager, por ejemplo, para el montaje de imágenes.

2- Uso exclusivo de la célula Ranger.

3- **Asignación de Máquinas:** Este punto ayudará con la asignación del equipo en Azure al usuario correspondiente, permitiendo así que pueda autogestionar su contraseña de BitLocker.

4- **Validar Maquinas:** Este punto nos ayudará a consultar el estado actual del equipo en, Configuration Manager, Intune y en el directorio activo, incluyendo información como el nombre completo y el usuario de red que está utilizando el equipo, en qué OU se encuentra el equipo, entre otros detalles.

5- **Eliminación de Maquinas:** Este punto nos ayudará a borrar los equipos de manera automática de las plataformas de Directorio Activo, Azure, Intune y Autopilot.

6- Uso exclusivo de la célula Ranger.

7- **Grupos de seguridad:** Este punto nos ayudara a conocer los grupos de seguridad para usuarios y equipos.

8- **Movimiento de máquinas:** Este punto nos ayudara a realizar el movimiento de los equipos cuando el proceso automático no funcione, por ejemplo, falla en el movimiento de unidad Organizacional.

IMPORTANTE: Se debe garantizar el borrado del equipo utilizando los puntos #1 y #5 de la Power App, siempre que se realice un cambio, formateo o retiro de cualquier equipo de la operación.

Bancolombia

11. Puntos importantes.

1- **Condiciones del Equipo**:

- **Nuevo o en Excelente Estado**: Verificar que el equipo esté nuevo o en óptimas condiciones, sin daños visibles ni signos de desgaste.
- **Condiciones:** Confirmar que las especificaciones del equipo cumplen con los requisitos establecidos por Bancolombia (Mínimo de 16 GB de memoria RAM, el disco duro debe estar configurado con una sola partición, la imagen del equipo debe estar actualizada, y no debe tener más de 1 mes de antigüedad si no está en uso, etc.).

2- **Configuración del Sistema**:

- **Sistema Operativo**: Asegúrese de que el sistema operativo del equipo esté correctamente instalado, actualizado y configurado según los estándares de Bancolombia, versión Windows 10 y 11 (22H2).
- **Drivers y controladores:** Asegúrese de que el equipo sea entregado con todos los drivers y controladores actualizados a sus últimas versiones.
- **Seguridad y Antivirus:** Instalar y configurar las herramientas de seguridad requeridas, incluyendo antivirus y software de protección adicional (Clear Pass, Nessus Tenable, Netskope).

3- **Accesorios y Periféricos**:

- **Entrega Todos los Accesorios**: Verificar que el equipo venga con todos los accesorios necesarios (cargador, cables, conversores de red, guaya, etc.).
- **Periféricos Adicionales:** Confirmar que cualquier periférico adicional solicitado (ratón, teclado, base para portátil, etc.) esté incluido y funcionando.

4- **Pruebas de Funcionamiento**:

- **Encendido y Arranque:** Verificar que el equipo encienda correctamente y arranque sin problemas.
- **Pruebas de Rendimiento:** Realizar pruebas básicas de rendimiento para asegurar que el equipo funcione de manera adecuada.

5- **Configuración de Red y Accesos**:

- **Conexión a Red:** Configurar la conexión a la red de Bancolombia, garantizar los parámetros de red establecidos, asegurando el acceso a recursos y servicios necesarios.
- **Accesos y Permisos:** Configurar las credenciales de acceso y permisos necesarios según las políticas de seguridad de Bancolombia.

6- Instrucciones finales y Soporte:

- **Soporte Técnico:** Brindar información de contactos y ubicaciones para soporte técnico en caso de problemas posteriores a la entrega.
- **Firma de Recepción:** Es esencial garantizar la firma de recepción del usuario final para confirmar la entrega del equipo de manera satisfactoria.
- **Revisión Final:** Para asegurar que todos los puntos anteriores se han cumplido satisfactoriamente, realice una revisión final junto al usuario.

12. Asignación final del equipo en Azure.

- Como proceso final, se debe garantizar la asignación del equipo al usuario final en Azure. Para esto:

1. **Acceso a Power App**: Ingrese a Power App en el punto #3.
2. **Documentación**: Documente los datos necesarios para la asignación.

- Si no se conoce el nombre del usuario final, espere hasta la fecha de entrega y asegúrese de completar la actualización antes de que el usuario inicie sesión.

APB043356_RANGERS_AUTOGESTIÓN - Power Apps

13. Procedimientos y tiempos.

- Los tiempos presentados en este documento se basan en pruebas reales de campo. Cabe resaltar que estos tiempos pueden variar y, en algunos casos, pueden ser menores.

1- **Autogestión para toma de red productiva:** Este proceso toma de 5 a 15 minutos.

2- **Ingreso al dominio:** Este proceso toma de 5 a 10 Minutos.

3- **Movimiento de OU correspondiente:** Este proceso es automático y toma de 15 a 20 Minutos.

4- **Mono Hibrido:** Este proceso es Automático y toma de 25 a 45 minutos.

5- **Configuración perfil del colaborador final:** Este proceso toma de 20 a 30 minutos, ya que se realiza durante la carga del Modo Híbrido y BitLocker. Estas configuraciones se integran al tiempo de sincronización del Modo Híbrido, por lo que no se considera un tiempo adicional, sino parte del tiempo total del Modo Híbrido.

- Suma de los tiempos:

Primer escenario: 1 Hora 30 minutos.
Segundo Escenario: 2 Horas.
Tercer escenario: Mas de 2 Horas
(Caso especial donde se presente la instalación y configuración de aplicaciones muy pesadas)

14. Bibliografía.

Título	Ubicación
Manual de aprovisionamiento de máquinas fuera de dominio “Controles de red TIGO”	\\sbmdedsa02v\1. SOFTWARE LINEA BASE -Semilla Estaciones\Controles_Ciberseguridad\Agente ClearPass_NAC\Manual equipos que vienen de bodega para aprovisionamiento
Manual Nombres de equipos “Anexo Estándar Nombres Servidores y Estaciones”.	**Local** \\sbmdedsa02v\Instaladores\Estaciones\Estandar nombre de estaciones **Web** Estándar de Nombres para Dispositivos - Overview (visualstudio.com)
Manual Portal de Autogestión Celula Ranger	\\sbmdedsa02v\Estaciones\1. SOFTWARE LINEA BASE - Semilla Estaciones\Manuales\Portal de autogestión Celula Ranger
Manual Actualización de Drivers y Controladores en Equipos Bancolombia.	\\sbmdedsa02v\Estaciones\1. SOFTWARE LINEA BASE - Semilla Estaciones\Manuales\Actualización de Drivers y Controladores

Bancolombia

15. Control de Cambios.

Fecha de versión	Descripción	Elaborado por
21/06/2023	Versión inicial	Jhonatan Mauricio Palacio López
28/06/2023	Modificación	Jhonatan Mauricio Palacio López Néstor Javier Doria Herrera
13/08/2024	Actualización	Jhonatan Mauricio Palacio López

16. Agradecimientos.

Soporte Campo TI Bancolombia

Jhonatan Mauricio Palacio López

Controles de Ciberseguridad de red Bancolombia

Daniel Mejia Castillo

Controles de red Tigo

Néstor Javier Doria Herrera