CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"Uso interno".**
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO.

Este manual proporciona instrucciones paso a paso para el inicio de sesión en un en el Pc asignado por la organización a un funcionario

2. ALCANCE.

Este manual se deberá aplicar para todos los funcionarios en el ingreso a los equipos del grupo empresarial que sean a los mismos.

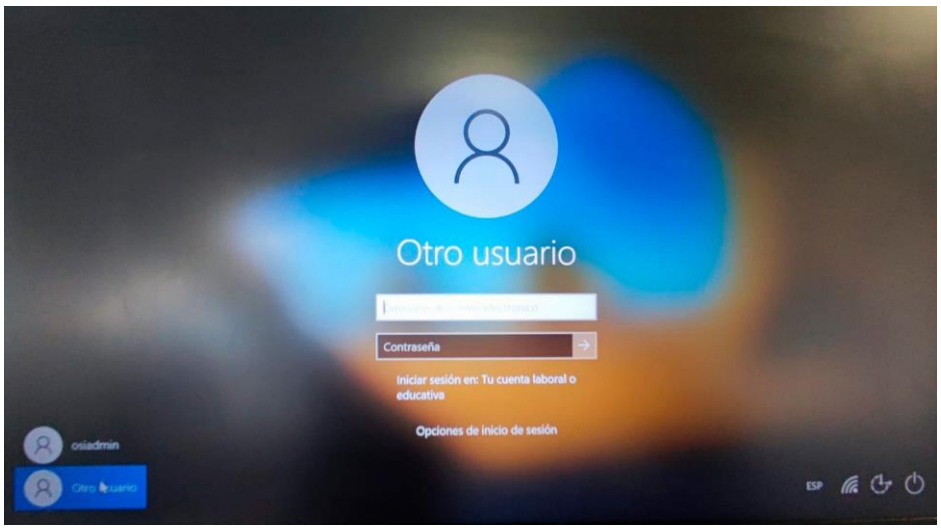
3. DEFINICIONES.

- **Equipo/PC:** Dispositivo electrónico que almacena y procesa información para después mostrarla en una interfaz a la disposición del usuario, permite una interacción del hardware (parte tangible) con el software (parte intangible).

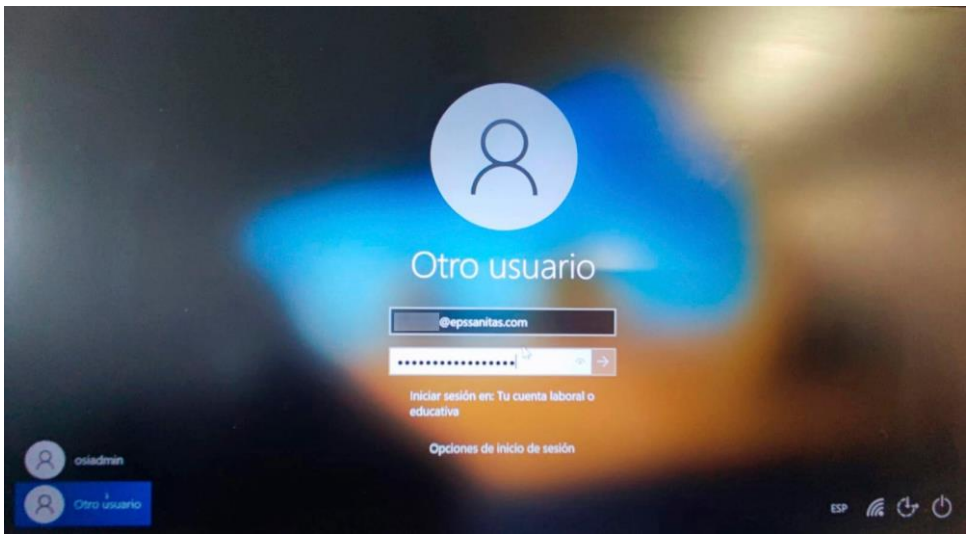
4. CONTENIDO.

4.1. Inicio de sesión en un Pc

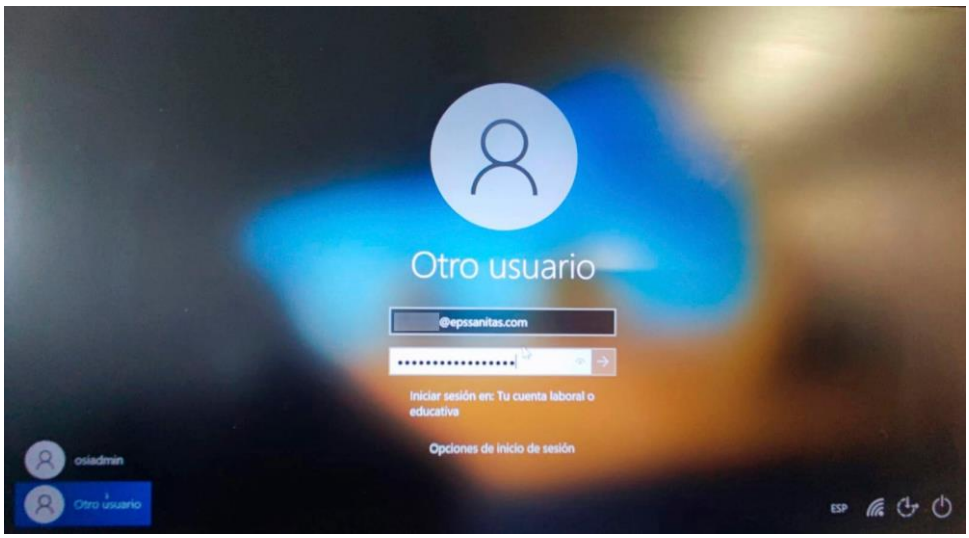
4.1.1. Enciende el equipo y asegúrate de que esté conectado a Internet



4.1.2. En la ventana de inicio de sesión, asegúrate de que el campo “Dominio” o “Dirección de correo electrónico” esté configurado correctamente con el dominio Azure al que perteneces. Por ejemplo, si tu dominio es “colsanitas.com”, ingresa tu dirección de correo electrónico como “usuario@colsanitas. com”.

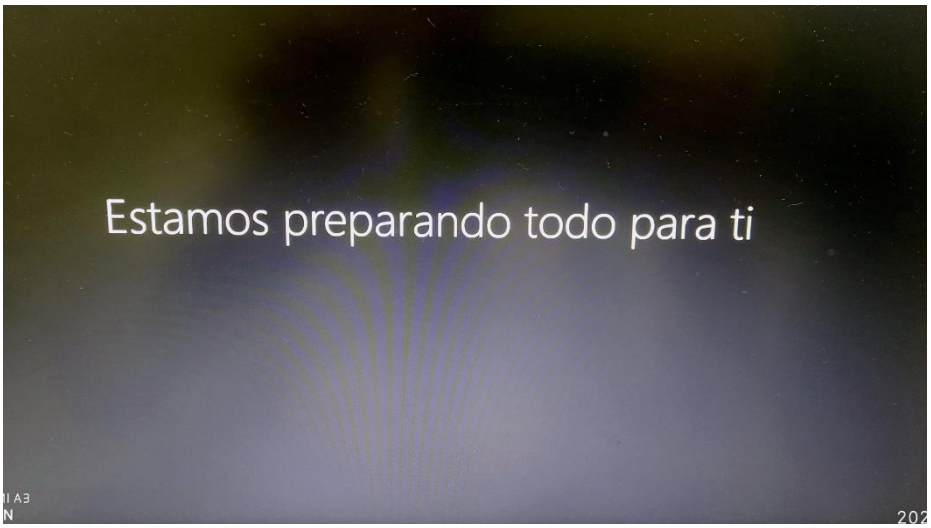


4.1.3. En la ventana de inicio de sesión, asegúrate de que el campo “Dominio” o “Dirección de correo electrónico” esté configurado correctamente con el dominio Azure al que perteneces. Por ejemplo, si tu dominio es “colsanitas.com”, ingresa tu dirección de correo electrónico “usuario@colsanitas. com”.



4.1.4. Ingresa tu contraseña en el campo correspondiente y asegúrate de que esté escrita correctamente. Haz clic en el botón “Iniciar sesión” o presiona la tecla “Enter” en tu teclado.

4.1.5. Si la información ingresada es correcta y el equipo puede conectarse al servidor de dominio Azure, se iniciará sesión en tu cuenta y se cargará el escritorio de Windows.



4.1.6. Si encuentras algún problema al iniciar sesión, asegúrate de verificar la siguiente información:

- La conexión a Internet está funcionando correctamente.
- La cuenta de usuario y la contraseña son válidas y están escritas correctamente.
- El equipo está correctamente configurado para unirse al dominio Azure.
- Si estás utilizando una cuenta de Microsoft Azure Active Directory (Azure AD), asegúrate de que lacuenta esté habilitada y permitida para iniciar sesión en el equipo.
- Si continúas teniendo problemas para iniciar sesión, es recomendable ponerse en contacto con eladministrador de tu dominio Azure para obtener ayuda adicional.

4.1.7. Si se te solicita, ingresa tu contraseña actual para verificar tu identidad.

4.1.8. A continuación, se te pedirá que coloques tu dedo en el lector de huellas dactilares. Sigue las instrucciones en pantalla y levanta y coloca el dedo varias veces hasta que se capture suficiente información de tu huella dactilar.

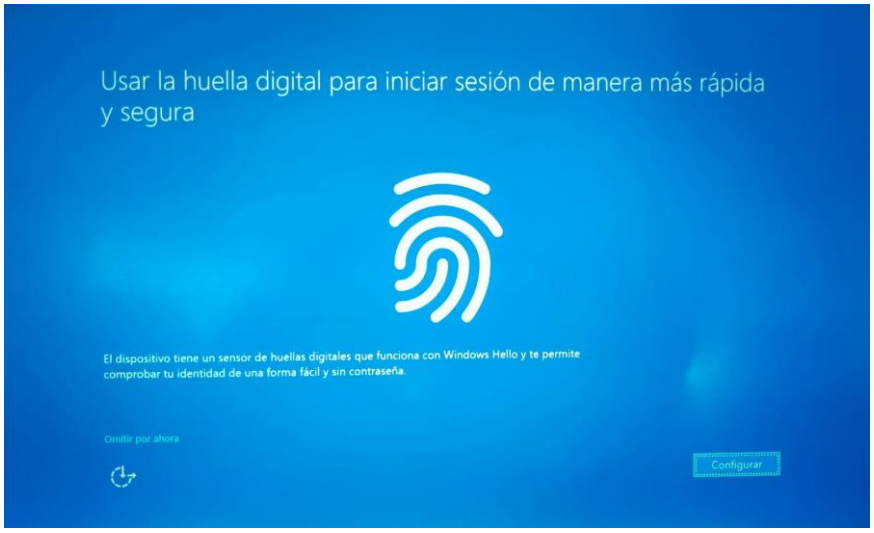
4.1.9. Una vez que se complete la configuración, se te mostrará un mensaje

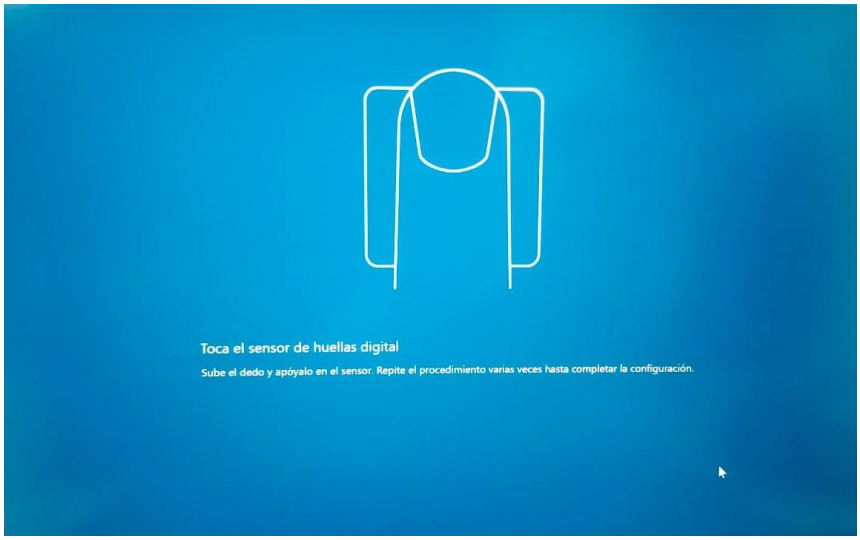
de éxito.

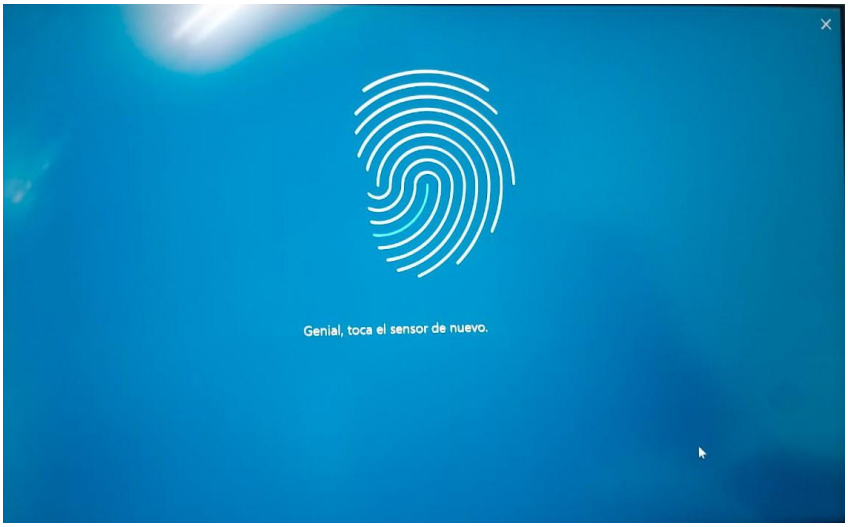
4.1.10. Ahora puedes reiniciar el equipo o bloquearlo para probar la función de inicio de sesión con huella dactilar.

4.1.11. Cuando llegues a la pantalla de inicio de sesión, coloca tu dedo en el lector de huellas dactilares y, si se reconoce correctamente, se iniciará sesión en tu cuenta de usuario.

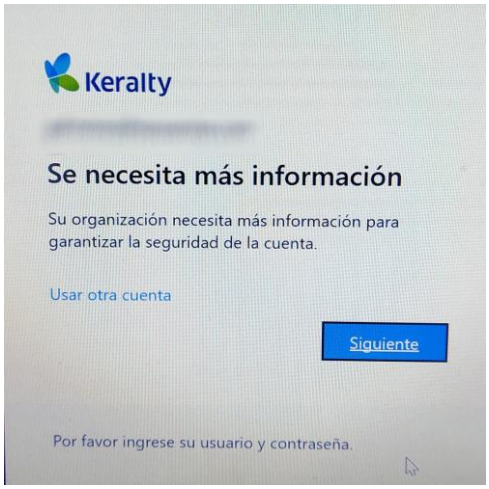
4.1.12. Es importante tener en cuenta que no todos los dispositivos admiten Windows Hello y la función de huella dactilar. Asegúrate de verificar las especificaciones de tu dispositivo y que los controladores adecuados estén instalados para el lector de huellas dactilares.

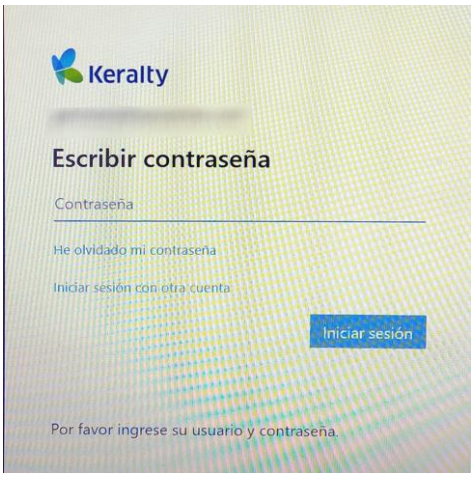






4.1.13. Cambio de Contraseña: Para cambiar la contraseña temporal por una definitiva que cumpla con los requisitos de seguridad (mínimo 10 dígitos, combinación de letras mayúsculas, minúsculas y números), siga los siguientes pasos:



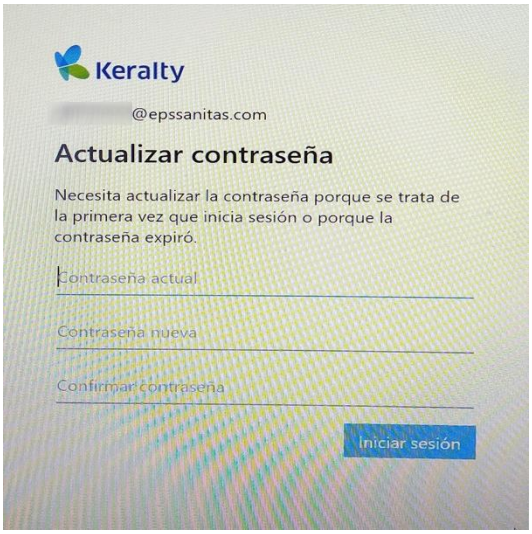


4.1.14. Paso 1: Inicie sesión con la contraseña temporal Ingrese su nombre de usuario y la contraseña temporal proporcionada. Haga clic en el botón “Iniciar sesión” para acceder al sistema.

4.1.15. Paso 2: Actualizar contraseña Ingrese la contraseña temporal Ingrese la nueva contraseña

4.1.16. Paso 3: Confirme la nueva contraseña en un campo adicional, se le pedirá que vuelva a ingresar la nueva contraseña exactamente igual para confirmarla.

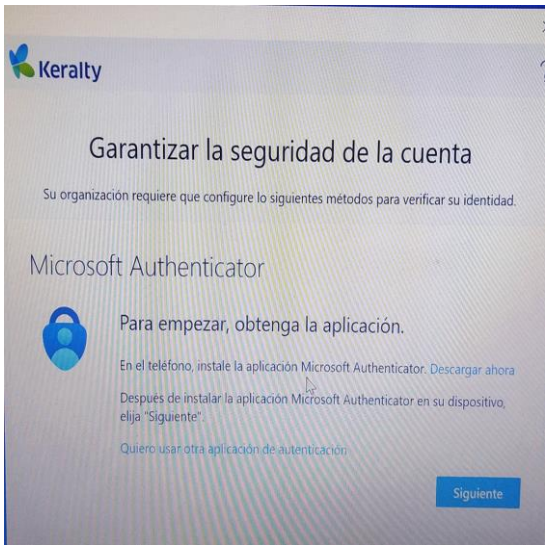
4.1.17. Paso 4: Iniciar sesión Haga clic en el botón “Iniciar Sesión” para comenzar con la nueva contraseña Recuerde que es importante elegir una contraseña segura y única para proteger su cuenta. Evite utilizar información personal obvia o contraseñas fáciles de adivinar.



4.1.18. Si tiene alguna dificultad para cambiar su contraseña o tiene problemas técnicos, le recomiendo comunicarse con el equipo de soporte técnico o el administrador del sistema para obtener asistencia adicional.

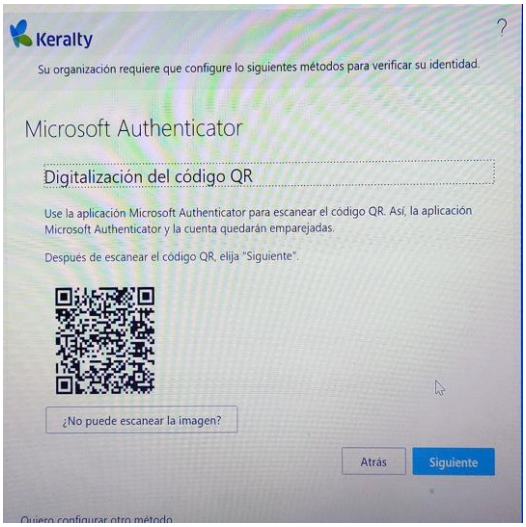
4.1.19. Autenticador Microsoft con QR Una vez realizado el cambio de contraseña, se inicia sesión con tu nombre de usuario y contraseña.

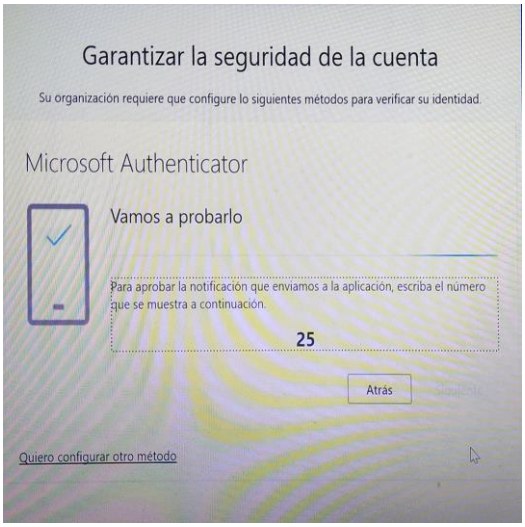
4.1.20. En la página de inicio de sesión, busca la opción de configuración de autenticación en dos pasos o verificación en dos pasos. Esta opción suele encontrarse en la sección de seguridad de tu cuenta. Selecciona la opción “Configurar la aplicación de autenticación”.



4.1.21. En tu dispositivo móvil, abre la aplicación Microsoft Authenticator y selecciona la opción de agregar una cuenta o escanear un código QR.

4.1.22. Escanea el código QR que se muestra en la pantalla de tu ordenador o ingresa manualmente el código de seguridad proporcionado.





4.1.23. La aplicación Microsoft Authenticator registrará tu cuenta y mostrará un código de verificación de seis dígitos.

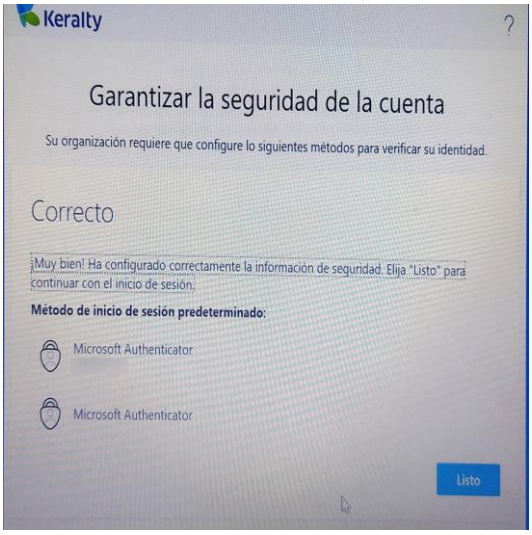
4.1.24. En la página de inicio de sesión de tu cuenta en el ordenador, ingresa el código de verificación que se muestra en la aplicación Microsoft Authenticator.

4.1.25. Confirma la configuración de la autenticación en dos pasos o verificación en dos pasos en tu cuenta Microsoft o en tu organización asociada a Azure.

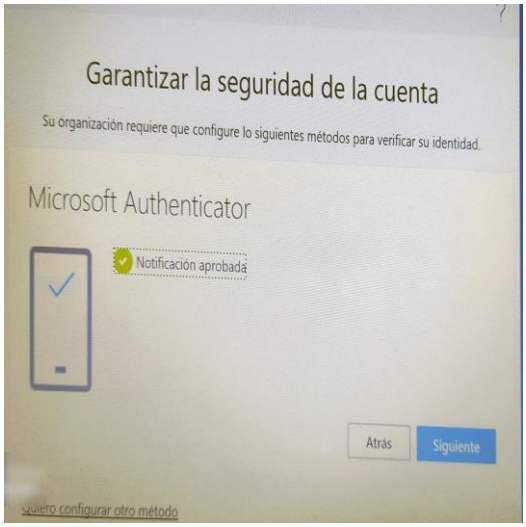
4.1.26. A partir de este momento, cuando intentes iniciar sesión en tu cuenta Microsoft o en servicios asociados, se te solicitará un código de verificación que deberás obtener de la aplicación Microsoft Authenticator en tu dispositivo móvil.

4.1.27. El Autenticador de Microsoft también puede ser utilizado para recibir notificaciones y aprobar o denegar solicitudes de inicio de sesión, lo que añade una capa adicional de seguridad.

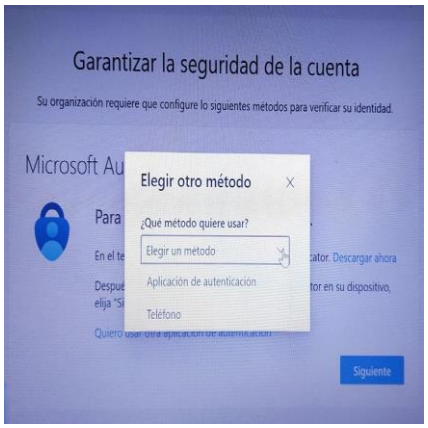
4.1.28. Recuerda que es importante guardar los códigos de respaldo que se te proporcionen durante el proceso de configuración en caso de que pierdas acceso a tu dispositivo móvil.

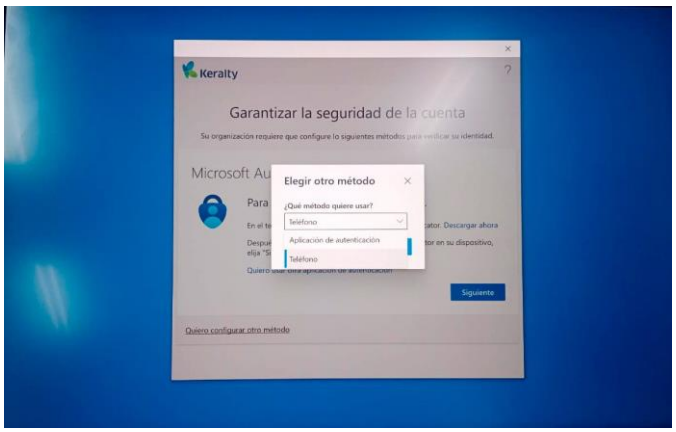


4.1.29. Inicia sesión con tu nombre de usuario y contraseña.



4.1.30. Busca la opción de configuración de autenticación en dos pasos o verificación en dos pasos. Por lo general, esta opción se encuentra en la sección de seguridad de tu cuenta.



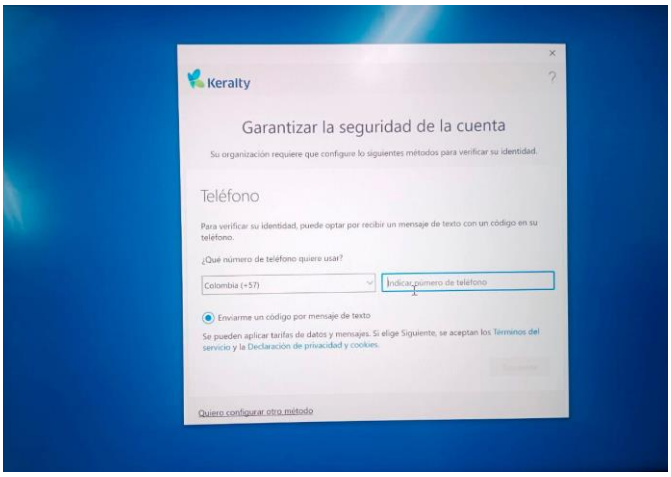


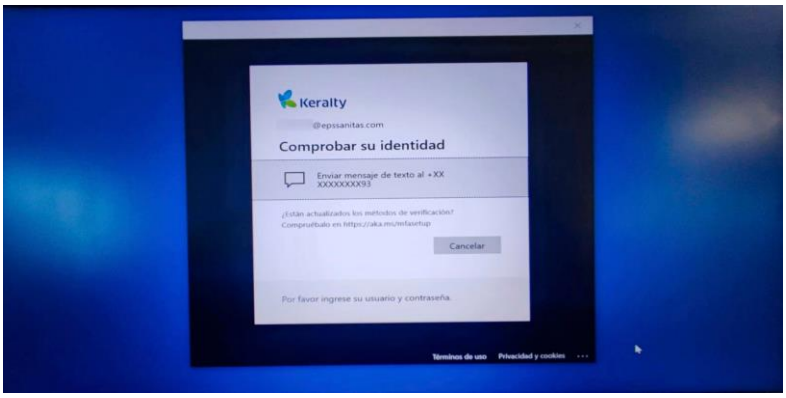
4.1.31. Selecciona la opción “Configurar la verificación en dos pasos” o “Configurar la autenticación en dos pasos” y elige la opción de usar el método de autenticación mediante SMS.

4.1.32. Verás una ventana emergente en la que se te solicitará que proporciones tu número de teléfono móvil. Ingresa tu número de teléfono y selecciona el botón para enviar el código.

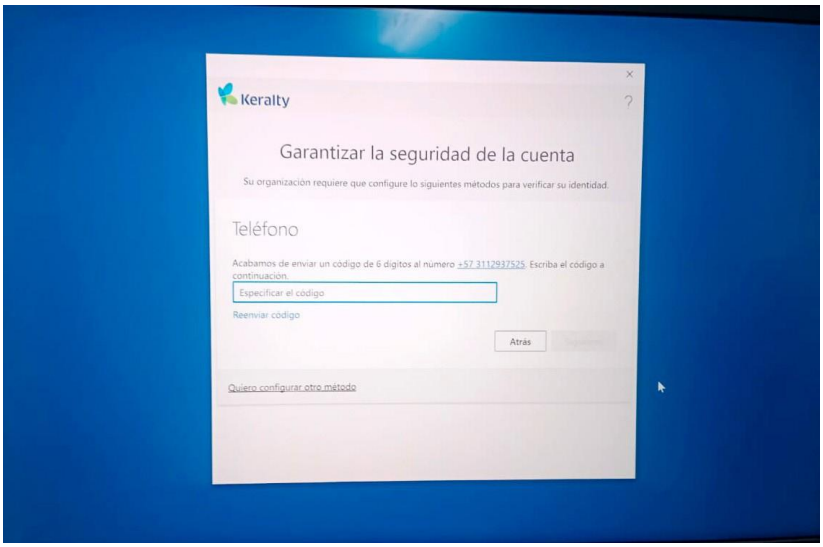
4.1.33. Recibirás un mensaje de texto en tu teléfono con un código de verificación.

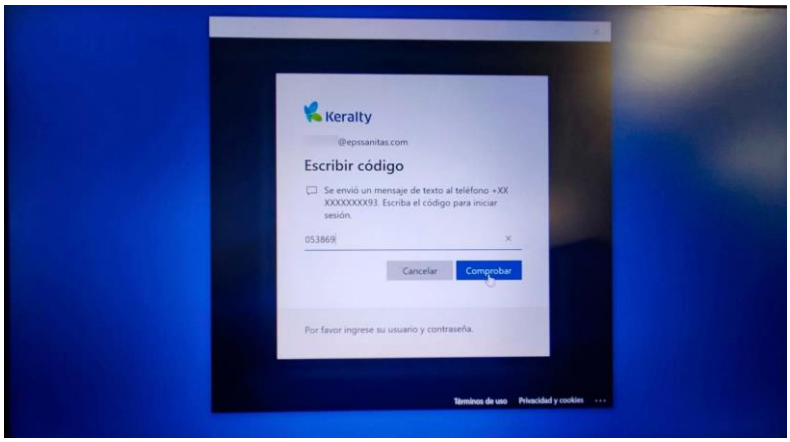
4.1.34. Ingresa el código de verificación en la página web y selecciona “Verificar” o “Enviar”.





4.1.35. Confirma la configuración de la autenticación en dos pasos o verificación en dos pasos en tu cuenta Microsoft o en tu organización asociada a Azure.

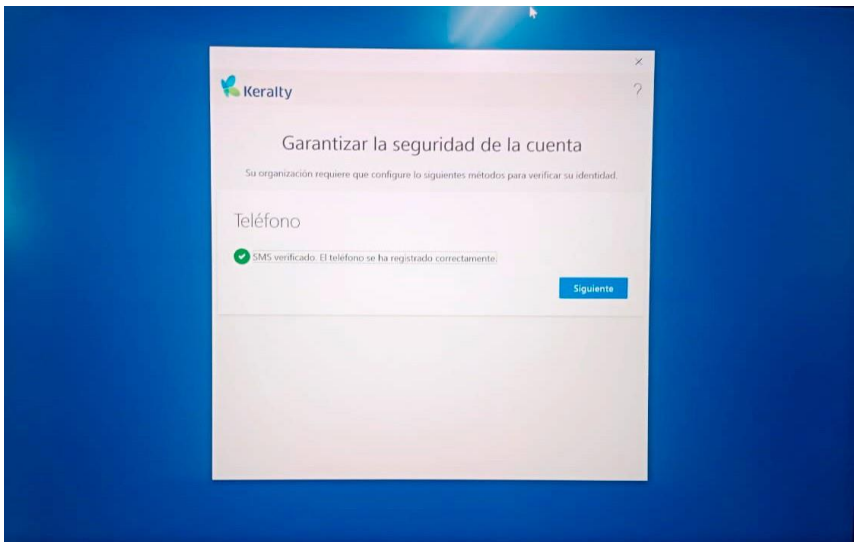




4.1.36. A partir de ahora, cuando intentes iniciar sesión en tu cuenta corporativa o en servicios asociados, recibirás un mensaje de texto con un código de verificación en el número de teléfono móvil que proporcionaste. Deberás ingresar ese código para completar el inicio de sesión.

4.1.37. Recuerda que este método requiere acceso a un teléfono móvil y una buena recepción de señal para recibir los mensajes de texto con los códigos de verificación. Además, ten en cuenta que los cargos de los mensajes de texto pueden aplicar según tu plan de telefonía móvil.

4.1.38. Es importante seguir las mejores prácticas de seguridad, como proteger tu número de teléfono y mantener tu dispositivo móvil seguro para evitar que alguien pueda acceder a tus mensajes de texto y comprometer tu autenticación.



4.1.39. A continuación, aparecerá una ventana emergente con instrucciones para configurar el reconocimiento facial. Sigue las instrucciones en pantalla, que generalmente implican mirar a la cámara y mover la cabeza ligeramente para capturar diferentes ángulos.

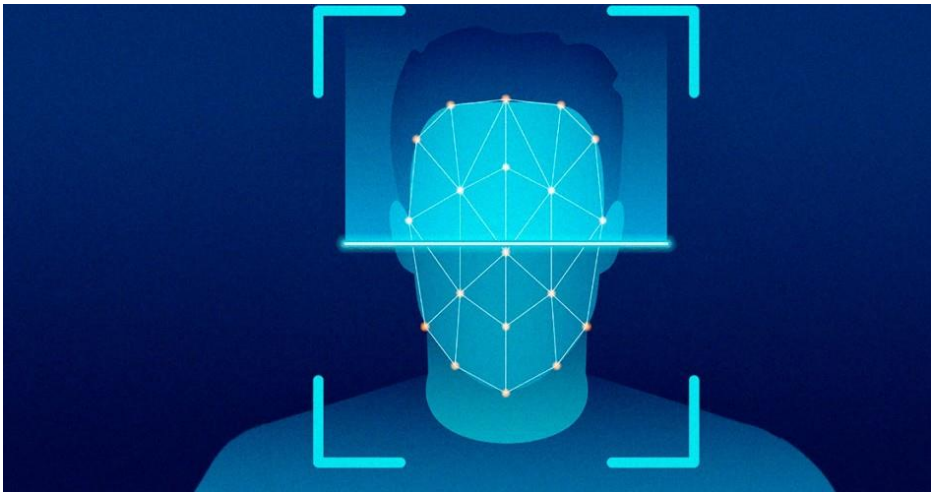
4.1.40. Una vez que se complete la configuración, se te mostrará un mensaje de éxito.

4.1.41. Ahora puedes reiniciar el equipo o bloquearlo para probar la función de inicio de sesión con reconocimiento facial.

4.1.42. Cuando llegues a la pantalla de inicio de sesión, el sistema utilizará la cámara para reconocer tu rostro. Si se reconoce correctamente, se iniciará sesión en tu cuenta de usuario.

4.1.43. Es importante tener en cuenta que no todos los dispositivos admiten Windows Hello y el reconocimiento facial. Asegúrate de verificar las especificaciones de tu dispositivo y que los controladores adecuados estén instalados para la cámara compatible con Windows Hello.

4.1.44. El reconocimiento facial ofrece una forma cómoda y segura de autenticación, pero es importante tener en cuenta que algunas situaciones, como cambios significativos en tu apariencia o condiciones de iluminación desfavorables, pueden afectar la precisión del reconocimiento facial. En tales casos, se te puede solicitar que utilices un método de autenticación alternativo, como una contraseña o un PIN

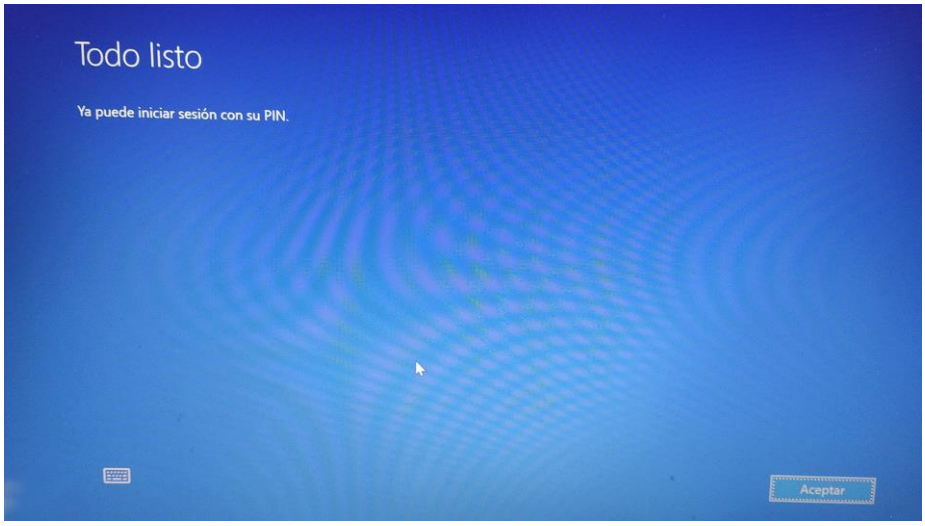


4.1.45. A continuación, se te pedirá que ingreses un nuevo PIN. El PIN debe tener al menos 6 dígitos, pero se recomienda utilizar un PIN más largo y más complejo para mayor seguridad. Ingresa el PIN deseado y haz clic en “Aceptar”. Confirma el PIN ingresándolo nuevamente y haz clic en “Aceptar”.

4.1.46. Una vez que se complete la configuración, se te mostrará un mensaje de éxito.

4.1.47. Ahora puedes reiniciar el equipo o bloquearlo para probar la función de inicio de sesión con PIN. Cuando llegues a la pantalla de inicio de sesión, selecciona “Iniciar sesión con un PIN” y luego ingresa el PIN que configuraste. Si el PIN es correcto, se iniciará sesión en tu cuenta de usuario.

4.1.48. Es importante recordar el PIN que configuraste, ya que será necesario cada vez que desees iniciar sesión en tu cuenta. Además, es recomendable establecer un PIN seguro y evitar el uso de información personal fácilmente identificable, como fechas de cumpleaños o números de teléfono.


Todo listo
Ya puede iniciar sesión con su PIN.
Aceptar

5. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
06/09/2024	Creación del documento.	1.0

Tabla 1 Control de cambios

6. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Fredy Páez Valencia Área/Proceso: Microinformática Fecha: 06/09/2024	Nombre: Jairo Enrique Robles Área/Proceso: Subgerencia de soporte Fecha: 06/09/2024	Nombre: Luisa Fernanda Trujillo Área/Proceso: Vicepresidencia de sistemas de información Fecha: 16/10/2024

Tabla 2 Flujo de aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.