

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## 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.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

TABLA DE CONTENIDO

1. OBJETIVO ..... 3

2. ALCANCE ..... 3

3. DEFINICIONES..... 3

4. CONTENIDO..... 5

4.1 SSID ..... 6

5. FLUJO DEL PROCEDIMIENTO ..... 7

6. DETALLE DEL PROCEDIMIENTO.....14

7. CONTROL DE CAMBIOS. ....15

8. FLUJO DE APROBACIÓN. ....16

Versión: 2.1	PROCEDIMIENTO ACCESO REDES WIFI	
Fecha: 30-05-2024		
Código: SIG-TIRC-CKE-PR01		

## 1. OBJETIVO.


El presente documento pretende dar a conocer el proceso de conexión de los usuarios cuando se intentan conectar a los diferentes SSID que se tienen implementados en la solución Wifi de Keralty.

## 2. ALCANCE

Permitir a través de un proceso de conexión segura poder tener acceso a las diferentes redes inalámbricas corporativas que se encuentran en las diferentes sedes kealty que cuentan con dicho servicio

## 3. DEFINICIONES

- **Confiabilidad:** Está determinada por el posible daño, como resultado de una operación del sistema de información realizada en forma incorrecta, incompleta, impropia o inoportuna.
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control de Acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria, es una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.
- **Contraseña o Clave:** Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

recurso. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.

- **Mejor Práctica (Buena Practica):** Corresponde a un modelo completamente definido, cuyos buenos resultados operacionales están comprobados y que está disponible para ser utilizada.
- **Política:** Actividad(es) orientada(s) en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como una manera de ejercer el poder con la intención de resolver o minimizar el choque entre los intereses encontrados que se producen dentro de una sociedad.
- **Política de Seguridad Informática (PSI):** Una política de seguridad informática es una forma de comunicarse con los usuarios. Las políticas de seguridad informática (PSI) establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el porqué de ello. Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la organización.
- **Portal Cautivo:** Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.
- **Procedimiento:** Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.
- **PSK:** En criptografía, una clave previamente compartida, clave pre compartida o PSK (en inglés pre-shared key) es una clave secreta compartida con anterioridad entre las dos partes usando algún canal seguro antes de que se utilice.

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

- **Red LAN:** Red de Área Local (Local Área Network).
- **Red WAN:** Red de Área Ancha (Wide Área Network).
- **Seguridad Informática:** La seguridad informática, también conocida como ciberseguridad,<sup>1</sup> es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.<sup>2</sup> Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y/o a la propia información.
- **802.1X:** La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802. Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla.

## 4. CONTENIDO

Keralty cuenta con controladoras locales distribuidas en las sedes principales (Calle 100, CRS, CUC, Sebastián Belalcázar, Iberoamérica, Central urgencias) las cuales se encargan de gestionar los Access point que se encuentran instalados a lo largo de las sedes. Adicional se cuenta con una controladora virtual, que se encarga de gestionar los Access point instalados en las sedes que no cuentan con una controladora local (SML, Calle 96, Cali CJ, ...)

También se cuenta con servidores Cisco ISE, los cuales se encargan de realizar la autenticación a la red corporativa y a la red de invitados, estos servidores están

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

sincronizados contra el directorio activo para hacer las validaciones de los usuarios corporativos.

Se tienen configurados diferentes SSID con diferentes tipos de seguridad, esto se resumirá en el punto 4 de este documento.

#### 4.1 SSID

A continuación, se presentan los distintos SSID, tipos de políticas, encriptación y llave de autenticación que utilizan cada uno. Las demás redes que no son nombradas cuentan con el tipo de seguridad WPA2-PSK con inscripción AES.

<b>SSID</b>	<b>Policy</b>	<b>Encryption</b>	<b>Authentication Key</b>
<i>Keralty_Corporativa</i>	<i>WPA2</i>	<i>AES</i>	<i>802.1x</i>
<i>Keralty_Intranet</i>	<i>WPA2</i>	<i>AES</i>	<i>PSK</i>
<i>Keralty_VIP</i>	<i>WPA2</i>	<i>AES</i>	<i>PSK</i>
<i>Keralty_Invitados</i>	<i>MAC filtering</i>		<i>CWA</i>

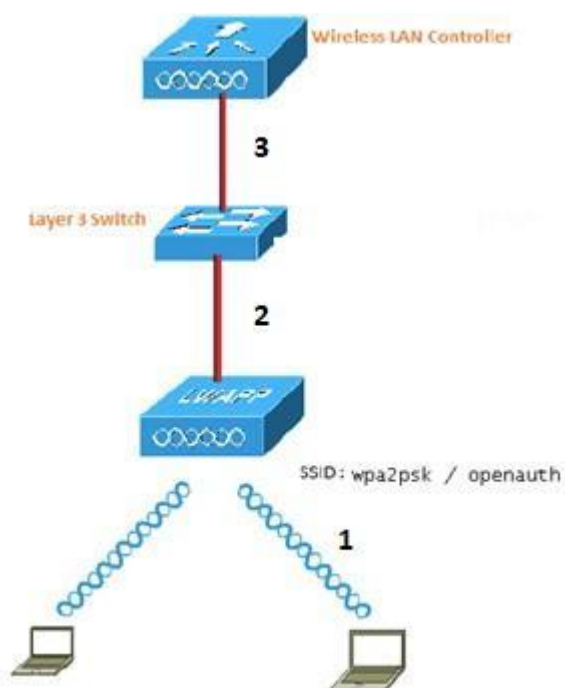
<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## 5. FLUJO DEL PROCEDIMIENTO



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

Diagrama conexión a SSID con WPA2-PSK (Keralty\_Intranet, Keralty\_VIP, CPE\_Intranet, Hospira, ...)



- Conexión del dispositivo al SSID con tipo de seguridad WPA2-PSK, ingreso de contraseña
- AP redirige tráfico hacia la WLC
- WLC realiza validación del PSK, si es correcto, acepta la conexión del dispositivo.

Diagrama conexión SSID con WPA2-802.1x (Keralty\_Corporativa)

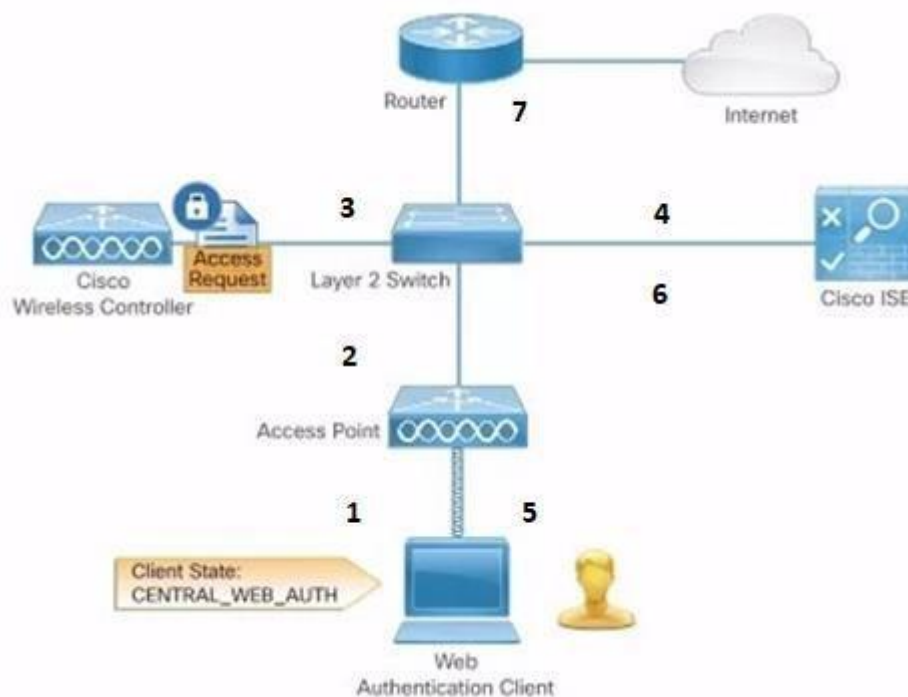


<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		



- Conexión del dispositivo al SSID con tipo de seguridad WPA2-802.1x, ingreso de credenciales
- AP redirige tráfico hacia la WLC, la WLC redirige la petición hacia el servidor de autenticación (Cisco ISE).
- ISE realiza validación de las credenciales en el directorio activo.
- Si las credenciales son correctas, acepta la conexión del dispositivo.

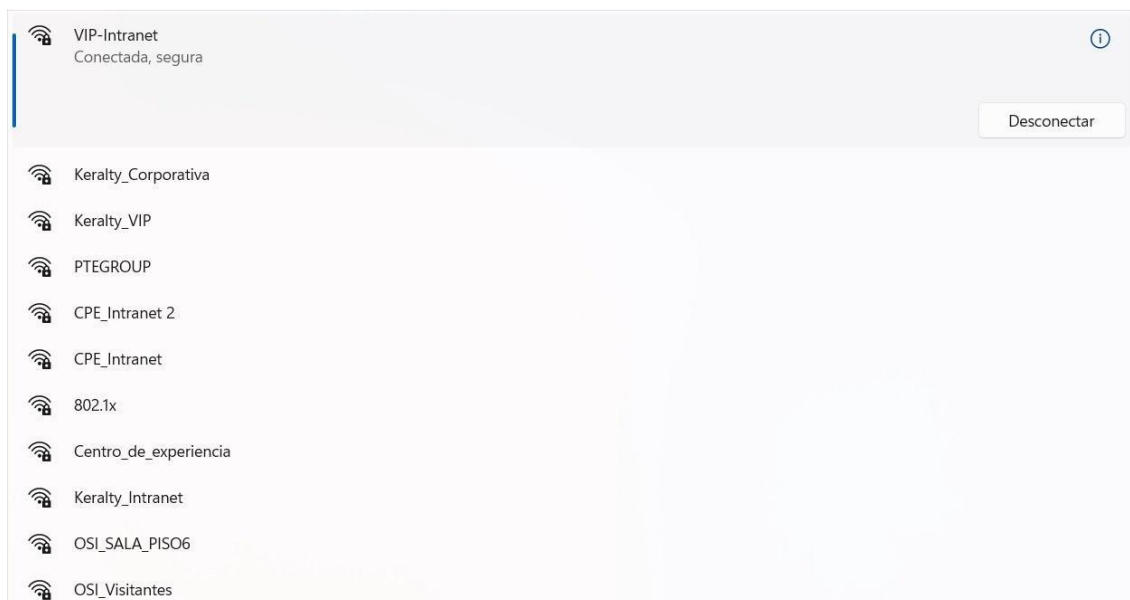
Diagrama conexión SSID con CWA (Keralty\_Invitados)



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

- Conexión del dispositivo al SSID con CWA (Autenticación a través del servidor ISE).
- AP redirige tráfico hacia la WLC.
- WLC redirige la petición hacia el servidor de autenticación (Cisco ISE).
- ISE reenvía formulario para conexión de usuario
- Usuario diligencia el formulario y realiza el login.
- ISE crea usuario y acepta la conexión del usuario.
- Salida a internet del dispositivo.

Para la conexión a los SSID de Keralty, desde el dispositivo desplegamos las redes wifi-disponibles y elegimos a la que deseamos conectarnos.



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## Conexión VIP

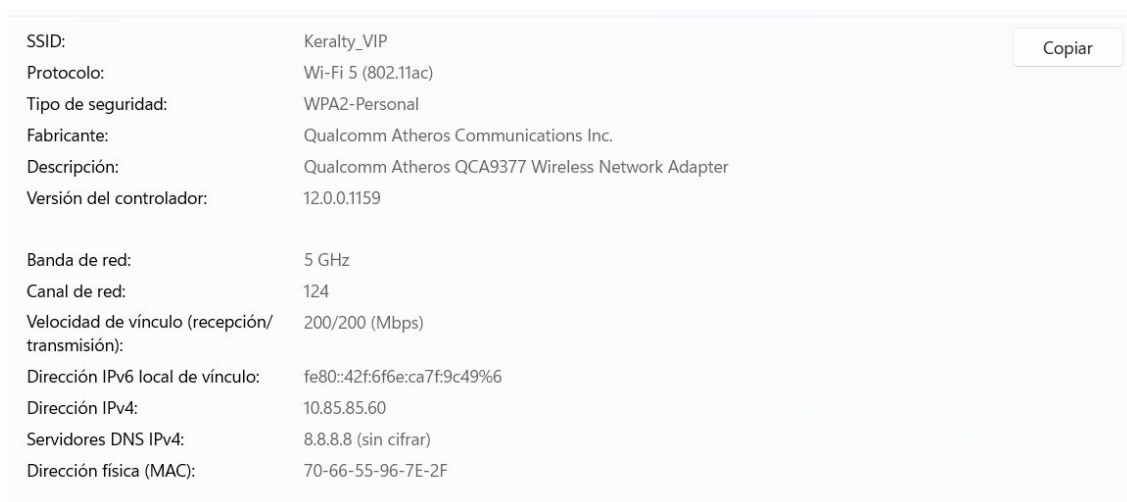
Para la conexión a esta red se debe ingresar la contraseña de seguridad (PSK)



VIP-Intranet  
Segura  
Escribir la clave de seguridad de red

.....

Siguiente Cancelar



SSID: Keralty\_VIP Copiar

Protocolo: Wi-Fi 5 (802.11ac)

Tipo de seguridad: WPA2-Personal

Fabricante: Qualcomm Atheros Communications Inc.

Descripción: Qualcomm Atheros QCA9377 Wireless Network Adapter

Versión del controlador: 12.0.0.1159

Banda de red: 5 GHz

Canal de red: 124

Velocidad de vínculo (recepción/transmisión): 200/200 (Mbps)

Dirección IPv6 local de vínculo: fe80::42f:6f6e:ca7f:9c49%6

Dirección IPv4: 10.85.85.60

Servidores DNS IPv4: 8.8.8.8 (sin cifrar)

Dirección física (MAC): 70-66-55-96-7E-2F

## Conexión Keralty\_Corporativa

Para la conexión a esta red se debe ingresar usuario y contraseña corporativos (Se debe cumplir alguna de las siguientes condiciones

- 1. Equipo registrado al Dominio corporativo
- 2. Usuarios registrado en el Dominio Corporativo.



<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## Conexión Keralty\_Invitados

Para la conexión a esta red se debe diligenciar el portal cautivo y realizar el auto login



**Bienvenido a la red Invitados de Keralty**

Si usted no cuenta con un usuario y contraseña por favor dar clic en la opción **REGÍSTRESE PARA ACCEDER COMO INVITADO**

Nombre de usuario:

Contraseña:

**Iniciar sesión**

[¿Regístrese para acceder como invitado?](#)



**Registro**

Rellene el siguiente formulario de registro:

Nombre

Apellidos

Dirección de correo electrónico\*

**Registrar** **Cancelar**

SSID:	Keralty_Invitados	<b>Copiar</b>
Protocolo:	Wi-Fi 5 (802.11ac)	
Tipo de seguridad:	Abierto	
Fabricante:	Qualcomm Atheros Communications Inc.	
Descripción:	Qualcomm Atheros QCA9377 Wireless Network Adapter	
Versión del controlador:	12.0.0.1159	
Banda de red:	5 GHz	
Canal de red:	124	
Velocidad de vínculo (recepción/transmisión):	200/200 (Mbps)	
Dirección IPv6 local de vínculo:	fe80::42f6f6eca7f9c49%6	
Dirección IPv4:	192.168.50.162	
Servidores DNS IPv4:	8.8.8.8 (sin cifrar)	
Dirección física (MAC):	70-66-55-96-7E-2F	

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## 6. DETALLE DEL PROCEDIMIENTO

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Conexión del computador a la red inalámbrica corporativa	Conexión del dispositivo al SSID con tipo de seguridad WPA2-802.1x, ingreso de credenciales	Usuario	NA
2	Proceso de doble factor de autenticación	AP redirige tráfico hacia la WLC, la WLC redirige la petición hacia el servidor de autenticación (Cisco ISE).	Usuario	NA
3	Autenticación exitosa - navegación	ISE realiza validación de las credenciales en el directorio activo. Si las credenciales son correctas, acepta la conexión del dispositivo.	Usuario	NA

*Tabla 1 Detalle del procedimiento*

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## 7. CONTROL DE CAMBIOS.

<b>FECHA</b>	<b>CAMBIO</b>	<b>VERSIÓN</b>
03/10/2022	Creación del Documento	1
06/10/2023	Actualización formato	2
30/05/2024	Se realiza inclusión de la tabla correspondiente al detalle del procedimiento, el documento se revisa en el marco de la actualización del SGSI año 2024, se realiza inclusión de la sigla del país y la compañía en el código del documento.	2.1

*Tabla 2 Control de cambios*

<b>Versión: 2.1</b>	<b>PROCEDIMIENTO ACCESO REDES WIFI</b>	
<b>Fecha: 30-05-2024</b>		
<b>Código: SIG-TIRC-CKE-PR01</b>		

## 8. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Miguel A. Pinilla S. Área/Proceso: Terasys Fecha: 30/09/2022. 	Nombre: Miguel Ángel León García Área/Proceso: Redes y comunicaciones Fecha: 30/05/2024 	Nombre: Javier Alonso Galván Castañeda Área/Proceso: Gerencia corporativa de tecnología Fecha: 09/06/2024 

*Tabla 3 Flujo de aprobación*

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