



PORTAL DE GESTIÓN

FUNCIONALIDADES WIFI-NEGOCIO

TELMEX

CONTENIDO

Funcionalidades wifi-negocio	1
Historial de revisión	¡Error! Marcador no definido.
Identifica tus clientes	5
Branding inalámbrico	9
Radar de clientes	12
Personaliza tu wifi	14
Estrategias de marketing	19
Red temporal de eventos	20
Creación de estrategias wifi	21
Creación de privilegios wifi	24
Alarma equipo wifi	27
Bloqueo de intrusos	30
Control de ancho de banda	34
Creación de pagina comercial en facebook en una red de invitados	38
Generación automática de informes	45
Agrupación de equipos wifi contratados	52
Reloj wifi	64
Visualización por tipo de dispositivo	68
Crear mapas de calor en central aruba	69
Signos vitales wifi	76



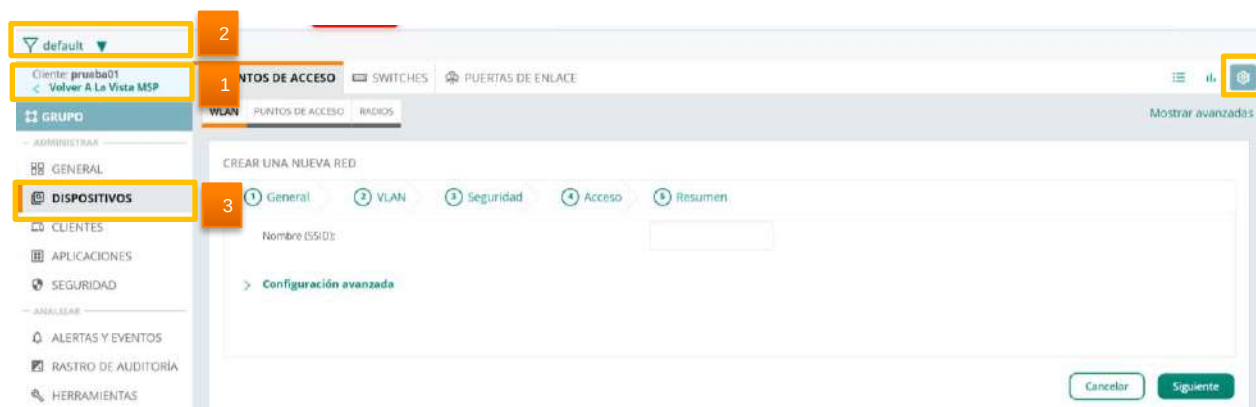
FUNCIONALIDADES DE WIFI-NEGOCIO

IDENTIFICA TUS CLIENTES

Primero debemos de crear nuestra Red que llamaremos **Invitados**

- 1- Ingresamos al cliente
- 2- Filtramos por el Grupo en este caso es **DEFAULT**

- 3- Damos click en la opción Dispositivos y seleccionamos el Icono 



- 4- Personalizamos el Nombre de nuestra Red (**Invitados**) y damos Siguiente



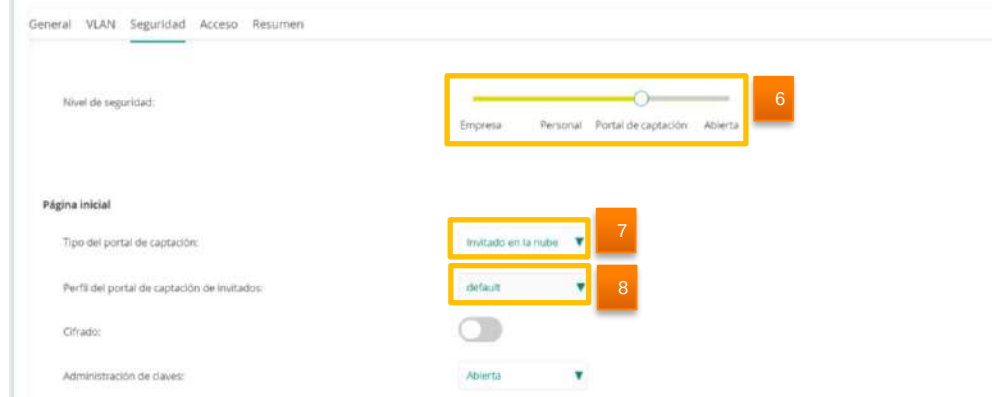
- 5- En la siguiente opción se determina quien estará brindando la IP a nuestro servicio, si será por DHCP o el Access Point, para continuar damos en siguiente.



6-Para que nuestros usuarios puedan acceder a un portal e ingresar sus datos se configura en la Opción **Portal de Captación**

7- Debemos de escoger la opción **Invitado en la nube**

8-Aquí escogemos la Página que ya tenemos configurada y damos clic en siguiente

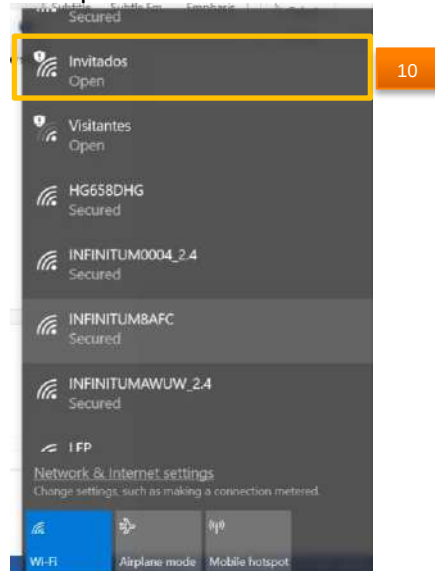


Nota: Podemos tomar como ejemplo el portal que esta como DEFAULT

9- En el menú siguiente vamos a escoger **Sin Restricción** si queremos que la navegación del cliente sea libre a cualquier sitio, damos **finalizar**



10- aquí mostramos como radiara la Red posterior a su creación



Proceso de registro de los clientes para posteriormente obtener sus datos (**Correo Electrónico / Teléfono**) para poder enviar las promociones o información de la Empresa

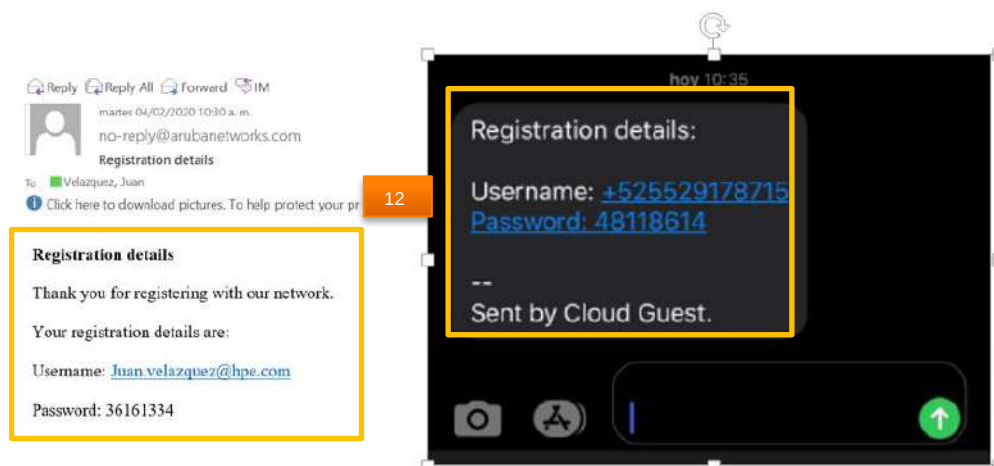
Al conectarse tus clientes a tu Red (**Invitados**), cuando accedan al portal puedes tener un control de tus accesos

11- En las siguientes imágenes mostramos el acceso a la página después de ingresar a la Red **Invitados** donde nos va solicitar nuestro teléfono o correo.

Nota: cuando accede por primera vez el cliente tiene que hacer registro desde la opción REGISTRAR en la cual le pedira el tipo de registro (correo electrónico o Teléfono)



12- Posteriormente nos llegara un mensaje dependiendo porque medio se registró **TELÉFONO/ CORREO** indicando el **Usuario y la contraseña**.



En esta opción marcamos los pasos para sacar la información de cada cliente registrado.

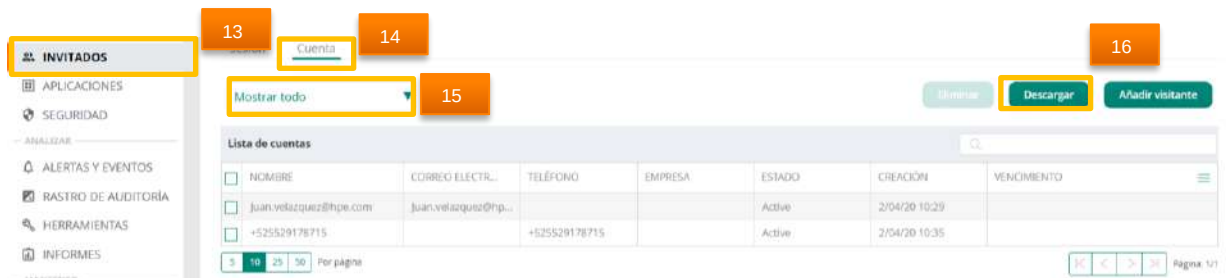
13-Para consultar los datos que tus clientes registraron “Teléfono – Correo electrónico”, y poder brindarle información sobre tu negocio debemos de acceder a la opción **INVITADOS**

14-Apartado **CUENTA**

15-Filtramos por **MOSTRAR TODO**

16-Bajaremos el reporte de los invitados desde la opción **DESCARGAR**

17- Abrir el archivo **EXCEL**



visitor (1).csv - Excel

	A	B	C	E	F	G	H	I
1	id	name	email	created_a	expire_at	is_enable	is_active	is_registered
2	b8af8500	5529178715		2019-08-13 15:54:06		TRUE	TRUE	TRUE
3	37dc4618	7772992086		2019-08-15 22:00:10		TRUE	TRUE	TRUE
4	6b6e3fce	avinajuan86@gmail.com	avinajuan86@gmail.com	2019-08-13 16:15:05		TRUE	TRUE	TRUE
5	1cecf417	daniel.altamirano@hpe.com	daniel.altamirano@hpe.com	2019-08-14 21:55:53		TRUE	TRUE	TRUE
6	12b24932	Troyano1985@live.com.mx	Troyano1985@live.com.mx	2019-08-15 22:00:12		TRUE	TRUE	TRUE
7	8591d923	usuario@gmail.com	usuario@gmail.com	2019-08-14 21:06:21		TRUE	TRUE	TRUE

Nota: Así después de que cada Invitado se registre podremos tener la información de su correo o teléfono para poder enviarle la información de nuestro producto o servicio como se muestra a continuación.

BRANDING INALAMBRICO

Vive una experiencia como la de las grandes compañías, muestra tu logo y tus promociones en la página de bienvenida.



- 1- Debemos de seleccionar en el icono  y escoger la opción **DEFAULT**
- 2- Ingresamos a la opción de **INVITADOS**
- 3- Después de escoger **DEFAULT** se nos habilitara la opción de agregar una nueva Página 

Nota: Crea tu página de bienvenida y da a conocer promociones a clientes

- 4- En este apartado se configura tu página personalizando el Nombre.
- 5- Tipo de autenticación pondremos para Acceso directo de los clientes (Anónima)
- 6- Por default debemos de dejar esta opción (securelogin.hpe.com)
- 7- En esta opción es el tiempo de espera de sesión.
- 8- En esta opción es el tiempo que dura la conexión diaria por usuario.

Nota: en 7 y 8 de preferencia deben de ser iguales para que no afecte en la sesión del Usuario

[Página inicial](#) > Promociones

✓ Configuración

Nombre:

Promociones

4

Tipo:

☐ Anónima ☐ Autenticados ☐ Wi-Fi de Facebook

5

Permitir Internet con fallo



Omitir nombre común



Nombre común securelogin.hpe.com

6

Clave de invitado



Comportamiento correcto de autenticación:

☐ Redirige a la URL original

☒ URL de redirección

http://www.telmex.com

Tiempo de espera de sesión:

0 día(s) 8 hora(s) 0 minuto(s)

7



Activar caché MAC

Compartir este perfil:



Límite de uso diario:

☒ Sin límite

☐ Por tiempo 8 hora(s) 0 minuto(s)

8

☐ Por datos

MB

☐ Por dispositivo

URL permitida:

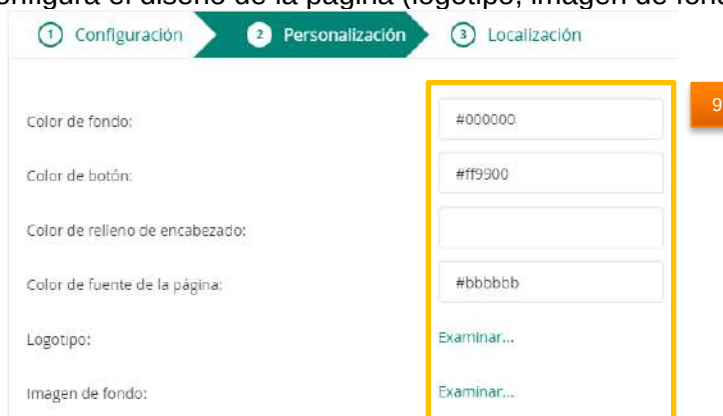


Añadir más direcciones URL

Cancelar

Siguiente

9- En esta opción se configura el diseño de la página (logotipo, imagen de fondo, color de letra)



1 Configuración 2 Personalización 3 Localización

Color de fondo: #000000

Color de botón: #ff9900

Color de relleno de encabezado:

Color de fuente de la página: #bbbbbb

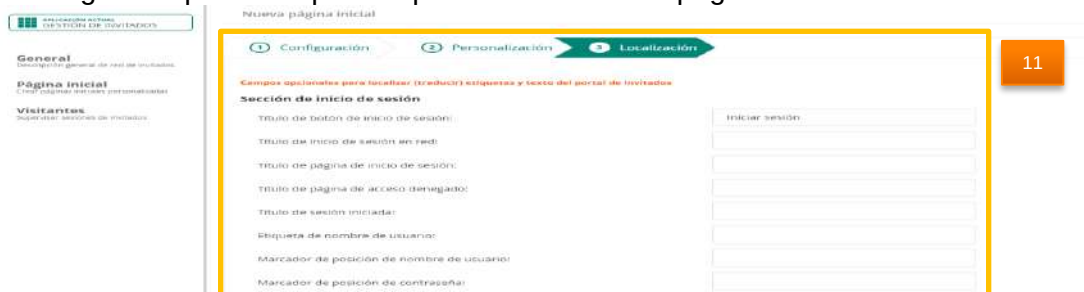
Logotipo: Examinar...

Imagen de fondo: Examinar...

10- Aquí podemos mostrar cómo queda la página para el acceso / puede ser personalizada a necesidad de su Negocio o área, al ingresar los invitados a la Red podrán ver la página de bienvenida



11- En el siguiente paso es opcional para el diseño de la página



1 Configuración 2 Personalización 3 Localización

Nueva página inicial

Campo opcional para localizar (traducir) etiquetas y texto del portal de invitados

Sección de inicio de sesión

Título de botón de inicio de sesión: Iniciar sesión

Título de inicio de sesión en red:

Título de página de inicio de sesión:

Título de página de acceso denegado:

Título de sesión iniciada:

Etiqueta de nombre de usuario:

Marcador de posición de nombre de usuario:

Marcador de posición de contraseña:

12- Al final clic en **Finalizar** configuración



Cancelar Atrás Vista previa Finalizar

RADAR DE CLIENTES

Mide que tan atractiva es tu promoción, podrás medir de una semana a otra como afectan las promociones que has creado revisando el número de transeúntes que se vuelven clientes en el tiempo que duró la promoción.

- 1- Ubica transeúntes y clientes dentro de negocio entrando a la opción **Presence Analytics** en el menú **INVITADOS**

Nota: se debe filtrar por todos los dispositivos para que nos muestre el Menú



- 2- Para validar los visitantes y transeúntes conectados a tu Red lo hacemos de la siguiente forma



Para el submenú de Presencia podemos ver las siguientes categorías:

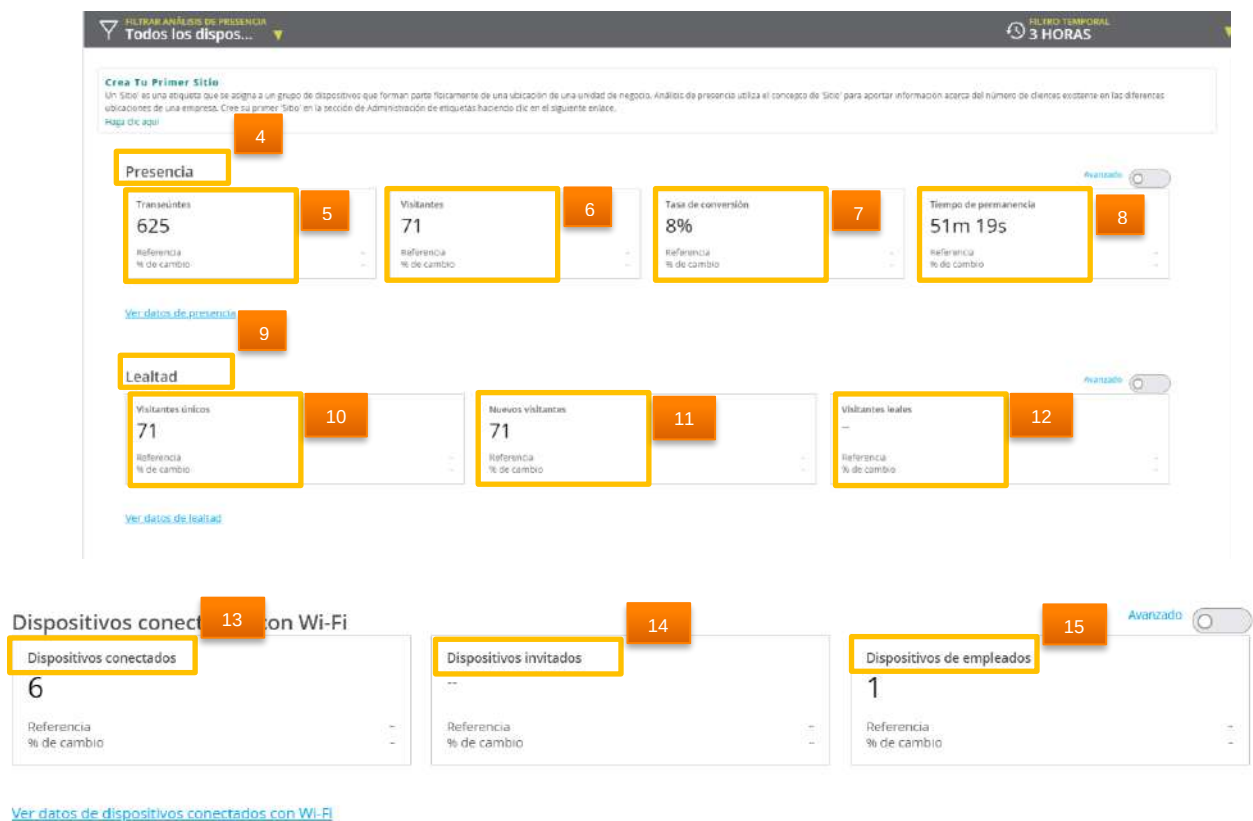
- 3- Presencia
- 4- La categoría **Transeúntes** indica el número de personas con un dispositivo inalámbrico que pasan cercanos a tu negocio, pero no entran a él.
- 5- La categoría de **Visitantes** indica el número de personas con un dispositivo inalámbrico que se encuentran dentro de tu negocio y que permanecen en él al menos 5 minutos.
- 6- El indicador **Tasa de abandono** indica el % de clientes **Transeúntes** que se convierten a la categoría **Visitantes**
- 7- **Tiempo de permanencia** es el tiempo de permanencia promedio en tu negocio de los clientes en la categoría **Visitantes**
- 8- Para el submenú de Lealtad podemos ver las siguientes categorías:
- 9- La categoría **Visitantes únicos** es la suma de **Visitantes Leales** y **Nuevos visitantes**

- 10- La categoría **Nuevos Visitantes** se refiere a los clientes que es la primera vez que están en tu negocio.
- 11- La categoría **Visitantes leales** se refiere a los clientes que han estado en tu negocio más de una ocasión en el pasado mes.

Para el submenú Dispositivos conectados con Wi-Fi.

- 12- La categoría **Dispositivos conectados** se refiere a los dispositivos que se han conectado mediante WI-FI.
- 13- La categoría **Dispositivos invitados** muestra la cantidad de dispositivos que se han conectado a la red de invitados.
- 14- La categoría **Dispositivos de empleados** muestra la cantidad de dispositivos que se han conectado a la red de empleados.

A continuación se presenta la pantalla principal con el resumen de los Analíticos de Presencia.

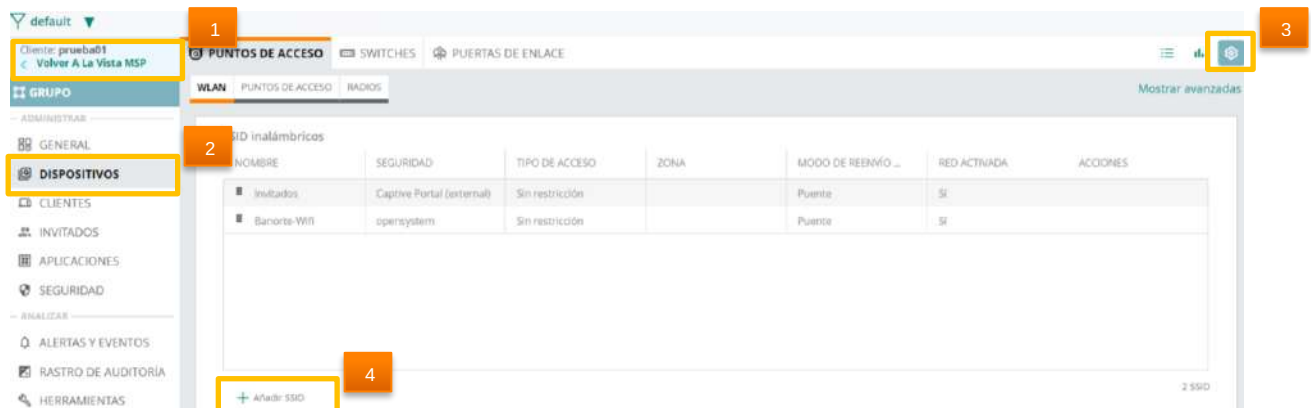


PERSONALIZA TU WIFI

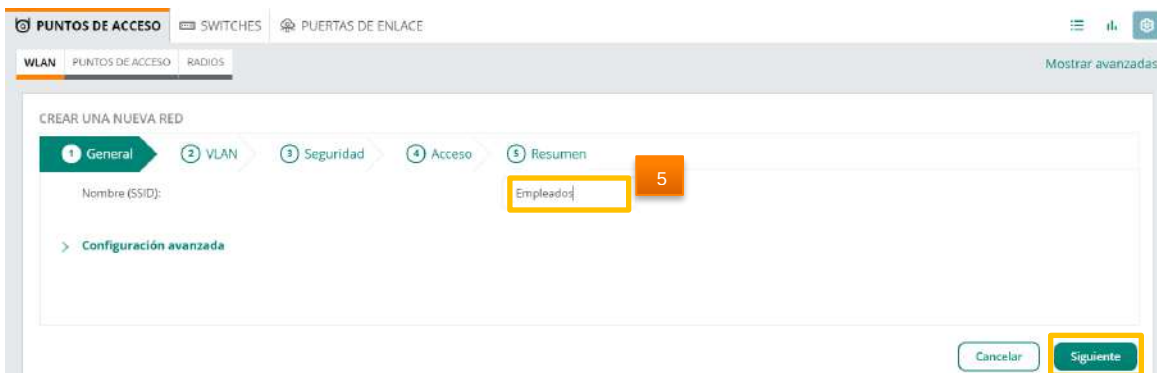
Creando redes inalámbricas de acuerdo a las necesidades de tu negocio puedes crear la experiencia de navegación adecuada a cada tipo de usuario y diferenciar tu negocio de otras redes con los nombres de tus redes personalizadas.

En esta opción puedes crear las redes de acuerdo a tu necesidad

- 1- Filtramos por **DEFAULT**
- 2- Ingresamos a la Opción **DISPOSITIVOS**
- 3- Seleccionamos el icono  para que nos muestre las SSID
- 4- Vamos a crear dos tipos de redes “Empleados-Invitados” y para esto damos clic en
+ Añadir SSID



- 5- Nombramos como Empleado nuestra SSID y Damos siguiente



- 6- Podemos tener nuestra red de empleados con seguridad WPA-2 con contraseña para su acceso, damos siguiente para continuar con la configuración
Nota: Por momento no se recomienda utilizar WPA3 Personal

- 7- Puede ser libre de acceso a navegar en cualquier página o tener limitaciones para los trabajadores en este paso damos en la opción Sin Restricciones y damos en Siguiete

- 8- En la siguiente ventana nos aparece como queda configurada Nuestra Red y damos Finalizar

General		Seguridad	
Nombre (SSID)	Empleados	Nivel de seguridad	Personal
ESSID	Empleados	Administración de claves	WPA-3 Personal
Modo de reenvío de tráfico	Puente	Autenticación MAC	No
Optimización de multidifusión	No	VLAN	
Banda	all	Asignación de IP de cliente	Servidor DHCP externo asignado
Intervalo de DTIM	1 ráos	Asignación VLAN de cliente	VLAN nativa
Uso principal	employee	VLAN	
Tiempo de espera de inactividad	1000 s	Acceso	
Opc. multidifusión dinámica	No	Asignaciones de roles para usuarios autenticados	No
Filtrado de contenido	No	FORZAR ROL EXCLUSIVO DE AUTENTICACIÓN MAC	No

- 9- En este paso Generaremos la Red de invitados como se Apprecia en la Siguiete Imagen, Nombramos la SSID como Invitados y damos Siguiete

CREAR UNA NUEVA RED

1 General 2 VLAN 3 Seguridad 4 Acceso 5 Resumen

Nombre (SSID): Invitados 9

> Configuración avanzada

Cancelar Siguiete

- 10- En este paso dejamos la misma configuración y damos siguiete.

CREAR UNA NUEVA RED

1 General 2 VLAN 3 Seguridad 4 Acceso 5 Resumen

Asignación de IP de cliente: Punto de acceso Instant asignado Servidor DHCP externo asignado 10

Asignación VLAN de cliente: Estática Dinámica VLAN nativa

Cancelar Atrás Siguiete

Nota: Aquí en este Paso, se determina quien Asigna la IP a los Dispositivos

- 11- Ingresamos el siguiente parámetro aunque se puede seleccionar que tenga una contraseña, un portal de bienvenida etc. en este caso se dejara abierta para los invitados.

CREAR UNA NUEVA RED

1 General 2 VLAN 3 Seguridad 4 Acceso 5 Resumen

Nivel de seguridad: Empresa Personal Portal de captación Abierta 11

Esta red no es segura. Los usuarios se conectarán a la red sin ninguna autenticación.

Administración de claves: Abierta

Cifrado: Ninguno/a

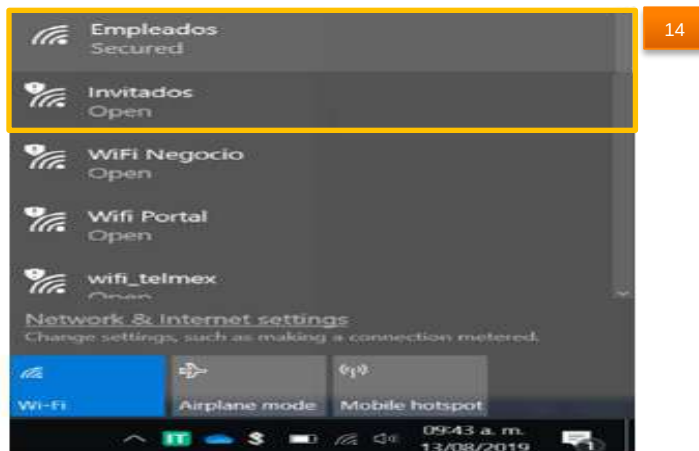
NOTA: En la Opción de Administración de claves se deja la opción ABIERTA

12- Podemos poner restricciones en el acceso de aplicaciones o dejar abierta la navegación, y damos Siguiente

13- Aquí en esta Opción nos muestra el Resumen de la Red de cómo queda configurada, por lo tanto damos Finalizar.

General		Seguridad	
Nombre (SSID)	Invitados	Nivel de seguridad	Abierta
ESSID	Invitados	Administración de claves	Abierta
Modo de reenvío de tráfico	Puente	Autenticación MAC	No
Optimización de multidifusión	No	VLAN	
Banda	all	Asignación de IP de cliente	Servidor DHCP externo asignado
Intervalo de DTIM	1 faros	Asignación VLAN de cliente	VLAN nativa
Uso principal	employee	Acceso	
Tiempo de espera de inactividad	1000 s	Asignaciones de roles para usuarios autenticados	No
Opc. multidifusión dinámica	No	FORZAR ROL EXCLUSIVO DE AUTENTICACIÓN MAC	No
Filtrado de contenido	No	ASIGNAR ROL DE PREAUTENTICACIÓN	No
Tiempo de transmisión	ilimitado	FORZAR AUTENTICACIÓN DE EQUIPO	No
Ocultar SSID	No		
Filtrado de difusión	arp		

- 14- Radiando de la siguiente Forma cada una con su respectiva configuración de acuerdo a las necesidades del negocio.



Nota: sugerimos tener una red de invitados y una de empleados, aunque se pueden crear de acuerdo a su necesidad o área.

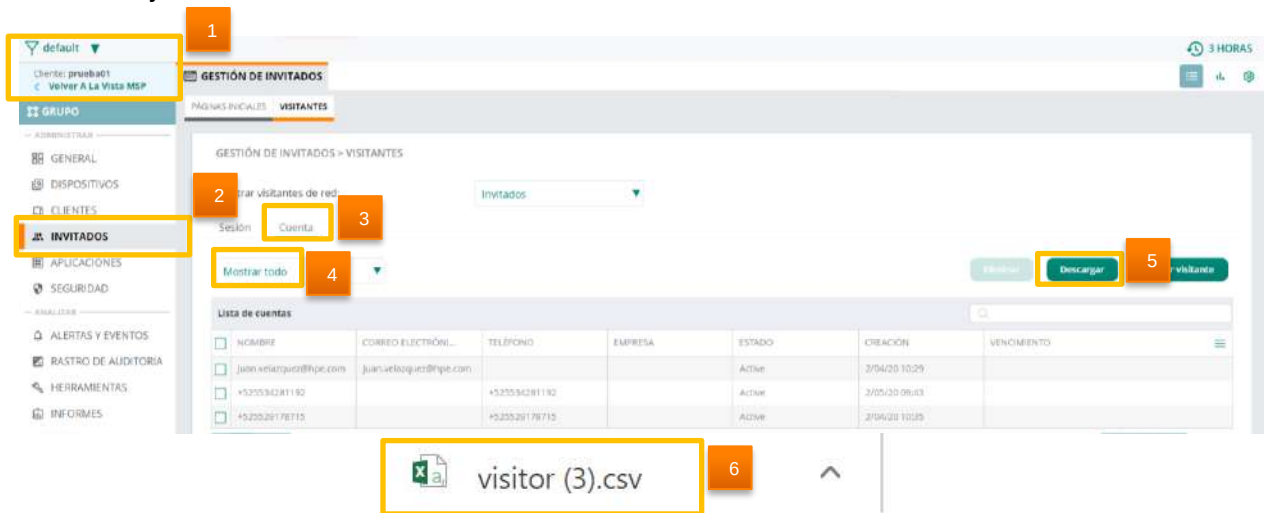
En la de empleado se tendrá cifrado y la de invitado se tendrá portal de bienvenida

ESTRATEGIAS DE MARKETING

Obtén la lista de correos y/o teléfonos de los usuarios que usaron tu red para enviarles información sobre tu negocio

Nota: SOLO SE MOSTRARA LA INFORMACIÓN DE LOS CLIENTES SIEMPRE Y CUANDO SE CONFIGURE UNA RED DE INVITADOS CON UN PORTAL DE AUTENTIFICACIÓN CON OPCIÓN AL REGISTRO POR CORREO ELECTRÓNICO / TELÉFONO

- 1- para consultar los datos que tus clientes registraron “Teléfono – Correo electrónico”, y poder brindarle información sobre tu negocio debemos Filtrar por Grupo **DEFAULT**
- 2- Seleccionamos la opción **INVITADOS**
- 3- Damos click en el apartado **CUENTA**
- 4- Seleccionamos **MOSTRAR TODO**
- 5- bajaremos el reporte de los invitados desde la opción **DESCARGAR**
- 6- nos baja archivo en **EXCEL**



Nota: Es necesario que la página se autentica por correo o teléfono

6-aquí podemos ver un listado de información y en la columna “name” podemos sacar la información del cliente para poder enviar nuestras promociones o servicios (teléfono o correo electrónico)

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW									
Clipboard Font Alignment Number Styles									
B4	✕ ✓ fx avinajuan86@gmail.com								
	A	B	C	E	F	G	H	I	
1	id	name	email	created_at	expire_at	is_enabled	is_active	is_registered	
2	b8af8500-	5529178715		2019-08-13 15:54:06	TRUE	TRUE	TRUE		
3	37dc4610-	7772992080		2019-08-15 22:00:10	TRUE	TRUE	TRUE		
4	6b6e3fce-	avinajuan86@gmail.com	avinajuan86@gmail.com	2019-08-13 16:15:05	TRUE	TRUE	TRUE		
5	1cec4117-f	daniel.altamirano@hpe.com	daniel.altamirano@hpe.com	2019-08-14 21:55:53	TRUE	TRUE	TRUE		
6	12b24912-	Trovano1985@live.com.mx	Trovano1985@live.com.mx	2019-08-15 22:00:12	TRUE	TRUE	TRUE		
7	8591d923-	usuario@gmail.com	usuario@gmail.com	2019-08-14 21:06:21	TRUE	TRUE	TRUE		

RED TEMPORAL DE EVENTOS.

Tu negocio puede activar una red específica con permisos, información, límites de ancho de banda y capacidades especiales para eventos especiales por el tiempo que tú determines.

- 1- De lado izquierdo de nuestra pantalla Filtraremos por Grupo **DEFAULT**, esto para realizar una configuración a nivel grupal de las Ap.
- 2- Seleccionamos **DISPOSITIVOS**,

- 3- Dar click en el Icono de Configuración  para que nos Muestre las SSID
- 4- Para desactivar temporalmente nuestra red inalámbrica solo debemos dar click en el icono 



The screenshot shows a web-based network management interface. On the left sidebar, there is a 'GRUPO' (Group) dropdown menu set to 'default' (callout 1) and a 'DISPOSITIVOS' (Devices) tab selected (callout 2). The main content area is titled 'PUNTOS DE ACCESO' (Access Points) and shows a table of wireless networks (SSID inalámbricas). The table has columns for 'NOMBRE' (Name), 'SEGURIDAD' (Security), 'TIPO DE ACCESO' (Access Type), 'ZONA' (Zone), 'MODO DE REENVÍO DE T...' (Forwarding Mode), 'RED ACTIVADA' (Network Activated), and 'ACCIONES' (Actions). The table lists two networks: 'Basorbi-Wifi' and 'Invitados'. The 'Invitados' network is highlighted in green, and its 'ACCIONES' column contains a Wi-Fi icon (callout 4) and a gear icon (callout 3).

SSID inalámbricas	NOMBRE	SEGURIDAD	TIPO DE ACCESO	ZONA	MODO DE REENVÍO DE T...	RED ACTIVADA	ACCIONES
Basorbi-Wifi	Basorbi-Wifi	open/system	sin restricción		Puente	Si	
Invitados	Invitados	Captive Portal (external)	Basado en red		Puente	No	 

CREACIÓN DE ESTRATEGIAS WIFI.

Asegura la experiencia de navegación que cada tipo de usuario en tu red debe tener limitando acceso a categorías o aplicaciones en cada red inalámbrica.

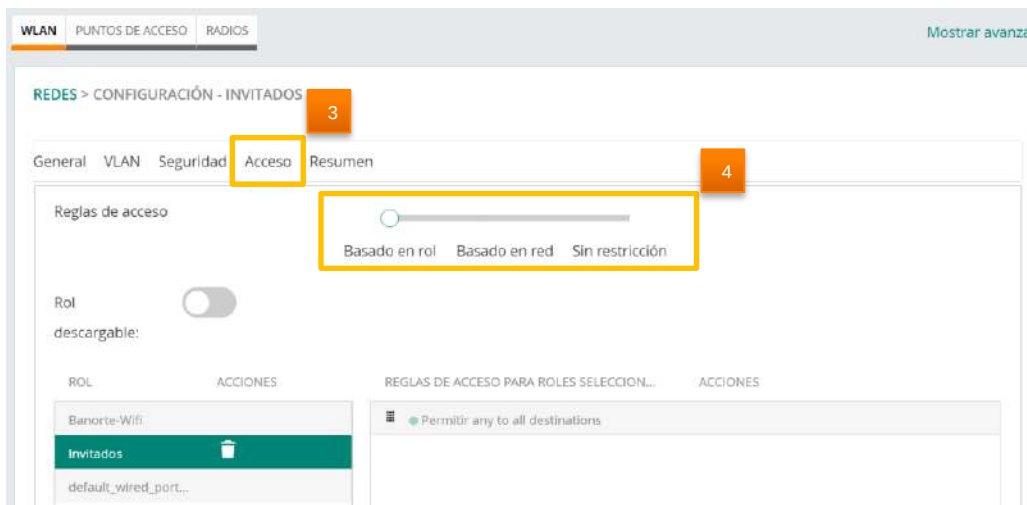
- 1- Dentro del submenú DISPOSITIVOS daremos click en la vista Configuración.



- 2- Editamos el SSID a configurar en el icono 

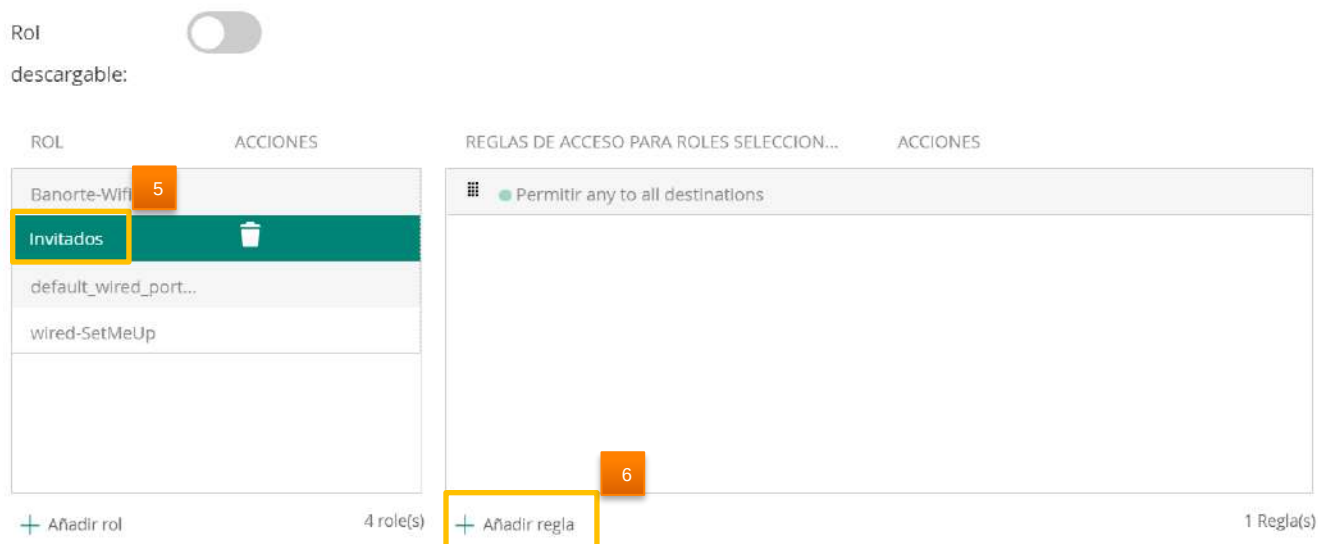


- 3- Dar click en Acceso para configurar la regla de acceso.
- 4- Posicionarnos en Basado en rol.



5- Para agregar una regla seleccionaremos el SSID donde estamos configurando

6- Daremos click en el icono de +



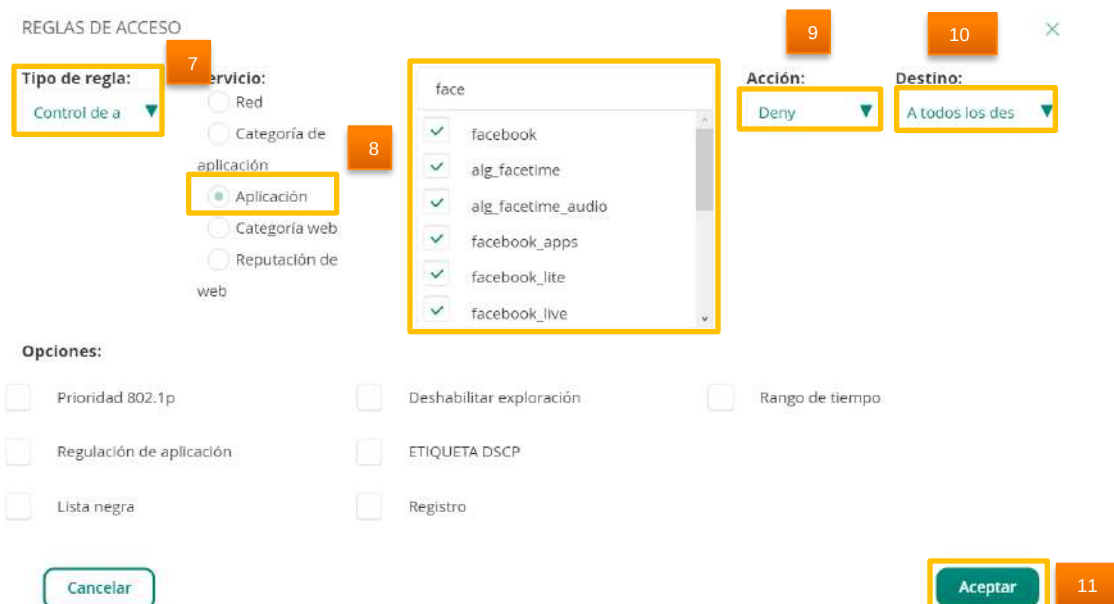
En la siguiente Pantalla es donde vamos a configurar el tipo de regla

7- **Tipo de regla:** Control de Acceso

8- **Servicio:** servicios desde aplicación(Facebook, whatsapp, Instagram, Netflix) categoría web (adultos, drogas, hacking, armas) reputación web (desde confiable hasta riesgo alto)

9- **Acción:** Permitir o Bloquear

10- **Destino:** Dejar a todos los destinos



11- Dar click en Aceptar, para guardar la regla creada.

En la siguiente pantalla se muestra la regla creada dentro del SSID Invitados:

Reglas de acceso

Basado en rol Basado en red Sin restricción

Rol ☐

descargable:

ROL	ACCIONES	REGLAS DE ACCESO PARA ROLES SELECCION...	ACCIONES
Invitados		- Denegar facebook to all destinations - Denegar alg_facetime to all destinations - Denegar alg_facetime_audio to all destin... - Denegar facebook_apps to all destinations - Denegar facebook_lite to all destinations - Denegar facebook_live to all destinations - Permitir any to all destinations	

+ Añadir rol 5 role(s) + Añadir regla 7 Regla(s)

CREACIÓN DE PRIVILEGIOS WIFI.

Nota: En esta opción podemos Generar el tipo de Navegación a internet “con restricciones”

- 1- Seleccionamos nuestra red que queremos configurar con algún rol basado en red, con su respectiva restricción sin seguridad de encriptación de contraseña (WPA2/WPA3)
- 2- Dar click en el icono de 

Empleados	wpa3-sae-aes	Sin restricción		Puente	Sí	1	2
Invitados	opensystem	Sin restricción		Puente	Sí		

- 3- Daremos click en Acceso para configurar los roles basados en red ya que por el momento tiene acceso a todas las aplicaciones y páginas web sin ninguna restricción (**puede acceder libremente a cualquier página**)
- 4- Click en Basado en red.
- 5- Click en Añadir regla

REDES > CONFIGURACIÓN - INVITADOS

3

General VLAN Seguridad Acceso Resumen

Reglas de acceso

4

Basado en rol Basado en red Sin restricción

Rol

descargable:

REGLAS DE ACCESO PARA ROLES SELECCIONADOS

ACCIONES

Permitir any to all destinations

5

+ Añadir regla

1 Regla(s)

Cancelar

Guardar configuración

- 6- **tipo de Regla:** Control de Acceso
- 7- **servicio:** Categoría web
- 8- Seleccionamos la categoría web, ejemplo: Adultos (**ADULT AND PORNOGRAPHY**) Aruba Central nos da una larga lista de categorías web para bloquear.
- 9- Para que restrinja el acceso debemos seleccionar **Deny**
- 10- Para guardar cambios en la configuración damos clic en **Aceptar**

REGLAS DE ACCESO

Tipo de regla:

Control de . ▼

Servicio:

☐ Red

☐ Categoría de aplicación

☐ Aplicación

☒ Categoría web

☐ Reputación de web

Acción:

Deny ▼

Opciones:

☐ Prioridad 802.1p

☐ Deshabilitar exploración

☐ Rango de tiempo

☐ Regulación de aplicación

☐ ETIQUETA DSCP

☐ Lista negra

☐ Registro

Cancelar

Aceptar

En la siguiente pantalla nos muestra las reglas no permitidas en la navegación de nuestra red inalámbrica.

REGLAS DE ACCESO PARA ROLES SELECCIONADOS	ACCIONES
☒ Denegar Adult and Pornography	
☒ Denegar Games	
☒ Denegar Hacking	
☒ Denegar Nudity	
☒ Denegar SPAM URLs	
☒ Denegar Spyware and Adware	
☒ Permitir any to all destinations	

Nota: la opción de **Permitir any to all destinations** siempre debe estar de bajo de todas las reglas para que puedan aplicarse, si usted modifica esta parte y pone en Accion **Deny** todo el tráfico de su red estará cerrada y no tendrá navegación.

REGLAS DE ACCESO

Tipo de regla: Control de acceso

Servicio: ☒ Red ☐ Categoría de aplicación ☐ Aplicación ☐ Categoría web ☐ Reputación de web

Cualquiera

Acción: **Allow** (highlighted in yellow box)

Destino: A todos los destinos

Opciones:

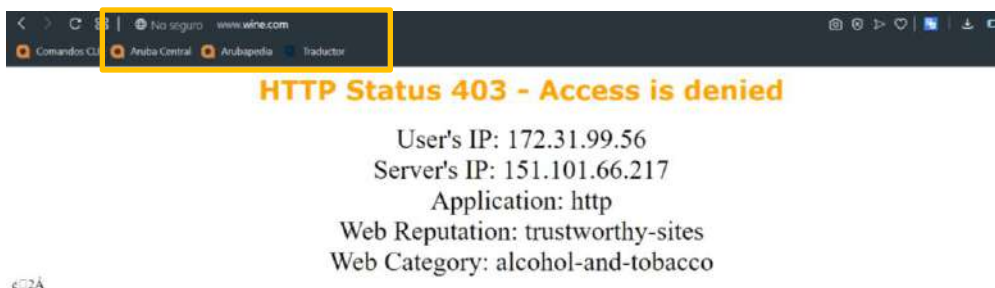
☐ Prioridad 802.1p ☐ Deshabilitar exploración ☐ Rango de tiempo

☐ Lista negra ☐ ETIQUETA DSCP

☐ Clasificar medios ☐ Registro

Cancelar Aceptar

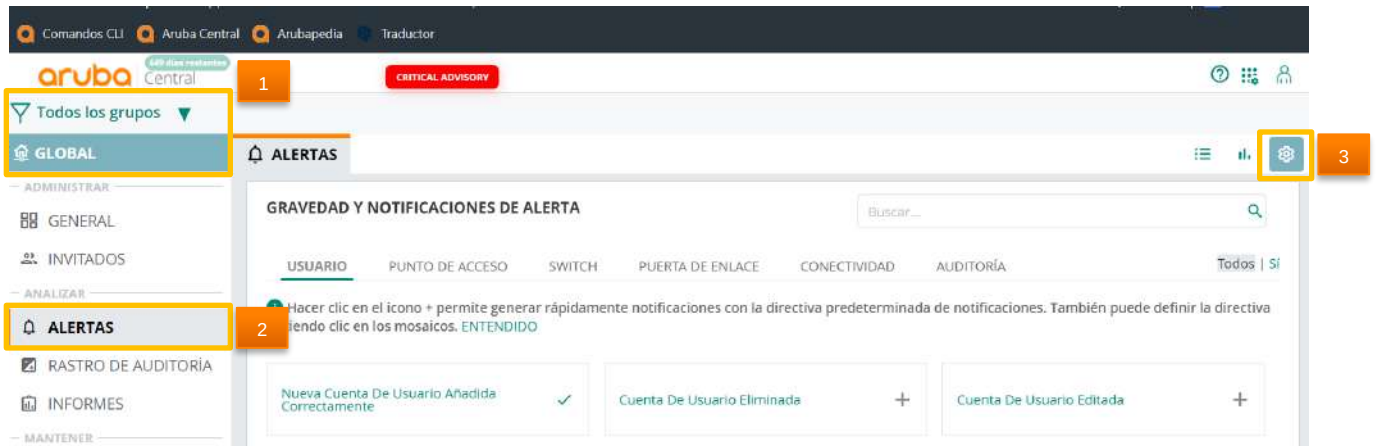
En la siguiente pantalla se muestra el bloqueo de alguna categoría:



ALARMA EQUIPO WIFI.

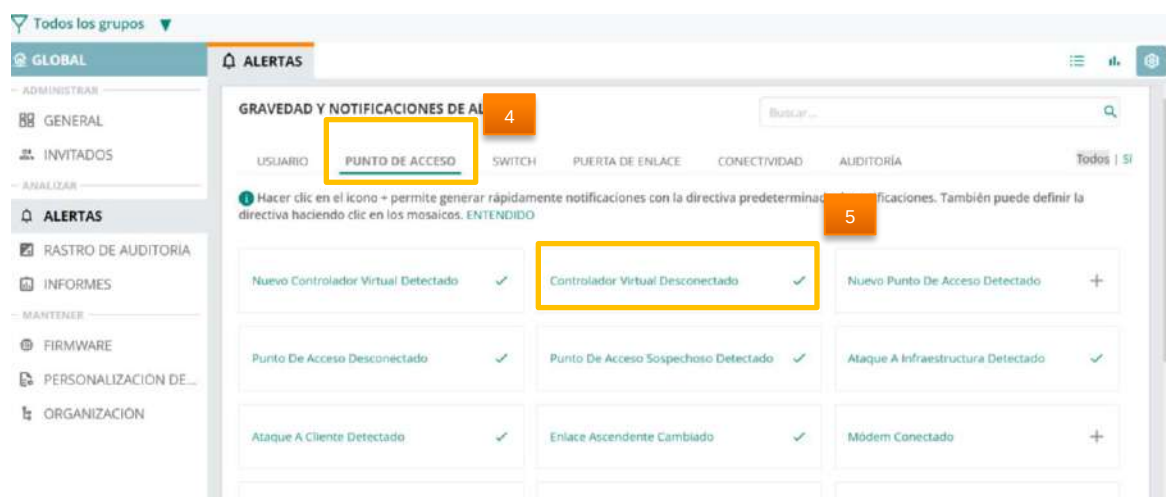
Recibe automáticamente a tu correo electrónico un aviso cuando tu equipo esté apagado para que puedas reaccionar de manera oportuna.

- 1- Seleccionar en el filtro Todos los grupos
- 2- Dar click en el submenú de Alertas
- 3- Dar click en vista Configuración



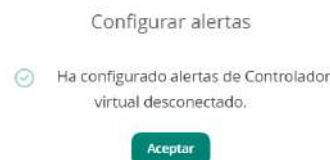
Aruba Central nos proporciona varias opciones de informes como Usuario, Puntos de Acceso, Swicht, Puerta de enlace, Conectividad, Auditoria.

- 4- Ahora procedemos a crear un informe dando click en PUNTO DE ACCESO
- 5- Después daremos click en Controlador Virtual Desconectado.

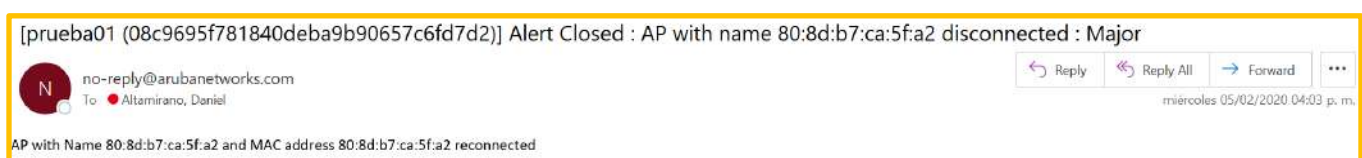


- 6- Seleccionar la gravedad de la Alerta, en este caso será Mayor
- 7- Colocar la duración en minutos desde 0 hasta 120.
- 8- Escoger el grupo donde esta asignado el Access Point
- 9- Escribir una etiqueta para nuestra alerta
- 10- Seleccionar nuestra Mac del Access Point
- 11- En Opciones de Notificación colocar un correo electrónico
- 12- Dar click en Guardar

- 13- Aruba Central mandara mensaje de que se ha configurado una alerta, dar click en Aceptar



Nota: Dentro de los primeros 5 minutos le estará llegando vía correo, una notificación de la alerta configurada.



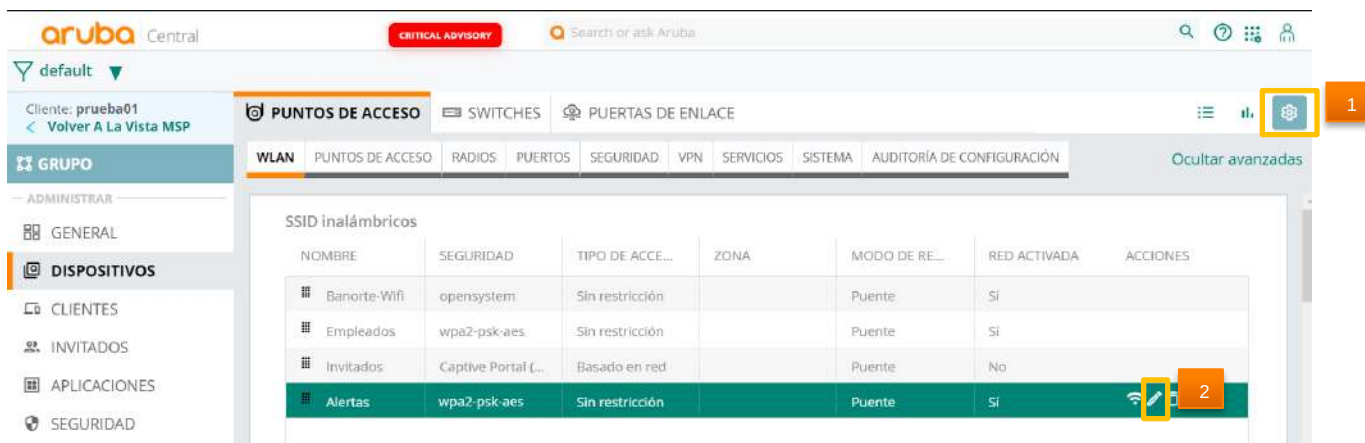
Como podemos observar Aruba Central nos da varias opciones de alertas en las que podemos configurar, como se muestra en la siguiente tabla:

IAP	Nuevo controlador virtual detectado: genera una alerta cuando hay un nuevo controlador virtual.
	Controlador virtual desconectado: genera una alerta cuando un controlador virtual está desconectado. Esta alerta está habilitada de manera predeterminada y la gravedad de la alerta es Mayor. En el campo Duración, ingrese la duración después de la cual se debe generar la alerta. El valor predeterminado es de 10 minutos.
	Nuevo AP detectado: genera una alerta cuando se detecta un nuevo AP instantáneo.
	AP desconectado: genera una alerta cuando se desconecta un AP instantáneo. En la duración campo, ingrese la duración después de la cual se debe generar la alerta. El valor predeterminado es de 15 minutos.
	AP no autorizado detectado: genera una alerta cuando se detecta un AP instantáneo no autorizado. Esta alerta es habilitada de forma predeterminada y la gravedad de la alerta es Mayor.
	Ataque de infraestructura detectado: genera una alerta cuando se produce un ataque de infraestructura.
	Ataque de cliente detectado: genera una alerta cuando se detecta un ataque de cliente.
	Enlace ascendente modificado: genera una alerta cuando un enlace ascendente ha cambiado.
	Módem conectado: genera una alerta cuando el módem está conectado.
	Módem desconectado: genera una alerta cuando el módem está desconectado.
	Utilización de CPU AP: genera una alerta cuando la utilización de CPU AP instantánea supera Valor umbral En el campo Duración, ingrese la duración después de la cual se debe generar la alerta. Puede agregar reglas adicionales para esta alerta.
	Utilización de memoria AP: genera una alerta cuando la utilización de la memoria AP instantánea excede el valor umbral. En el campo Duración, ingrese la duración después de la cual la alerta debe ser Generado. Puede agregar reglas adicionales para esta alerta.
	Utilización del canal de radio: genera una alerta cuando la utilización del canal de radio AP instantáneo excede el valor umbral. En el campo Duración, ingrese la duración después de la cual la alerta debe ser Generado. En el menú desplegable Banda, seleccione la banda del espectro: 2.4 GHz o 5 GHz. Puedes añadir Reglas adicionales para esta alerta.
	Radio Noise Floor: genera una alerta cuando el ruido de piso (dBm) excede el umbral valor. En el campo Duración, ingrese la duración después de la cual se debe generar la alerta. Desde la Banda desplegable, seleccione la banda del espectro: 2.4 GHz o 5 GHz. Puede agregar reglas adicionales para esta alerta.
	Cientes conectados: genera una alerta cuando el número de clientes conectados supera el valor umbral en el campo Duración, ingrese la duración después de la cual se debe generar la alerta. Puede agregar reglas adicionales para esta alerta.

BLOQUEO DE INTRUSOS.

Permite y bloquea dispositivos dentro de tu red asegurando que el uso de tu red sea el adecuado.

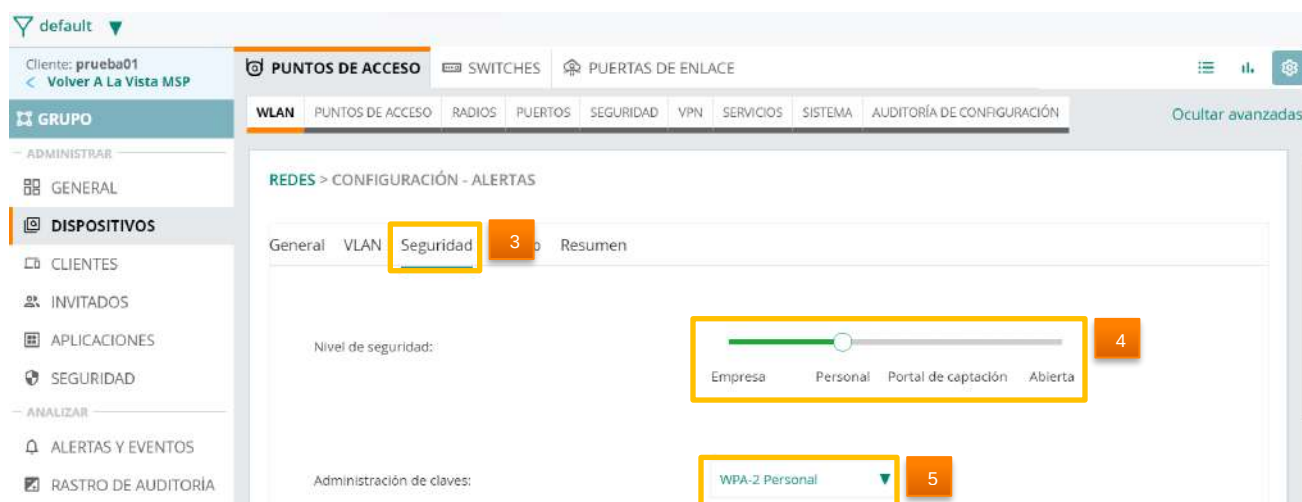
- 1- Dentro del submenú DISPOSITIVOS, dar click en la vista configuración
- 2- Seleccionar el SSID a configurar y dar click en el icono de 



Aruba Central interface showing the WLAN configuration page. The 'PUNTOS DE ACCESO' tab is selected. In the 'SSID inalámbricos' table, the 'Alertas' SSID is highlighted, and the edit icon (pencil) is clicked, indicated by a yellow box and an orange '2'.

NOMBRE	SEGURIDAD	TIPO DE ACCE...	ZONA	MODO DE RE...	RED ACTIVADA	ACCIONES
Banorte-Wifi	opensystem	Sin restricción		Puente	Si	
Empleados	wpa2-psk-aes	Sin restricción		Puente	Si	
Invitados	Captive Portal (...)	Basado en red		Puente	No	
Alertas	wpa2-psk-aes	Sin restricción		Puente	Si	

- 3- ir al apartado de Seguridad.
- 4- Dar click en Nivel de seguridad: Personal
- 5- Administración de claves: WPA-2 Personal



Aruba Central interface showing the 'Seguridad' configuration page for the 'Alertas' SSID. The 'Seguridad' tab is selected. The 'Nivel de seguridad' is set to 'Personal' and the 'Administración de claves' is set to 'WPA-2 Personal', both indicated by yellow boxes and orange numbers '4' and '5' respectively.

REDES > CONFIGURACIÓN - ALERTAS

General VLAN Seguridad Resumen

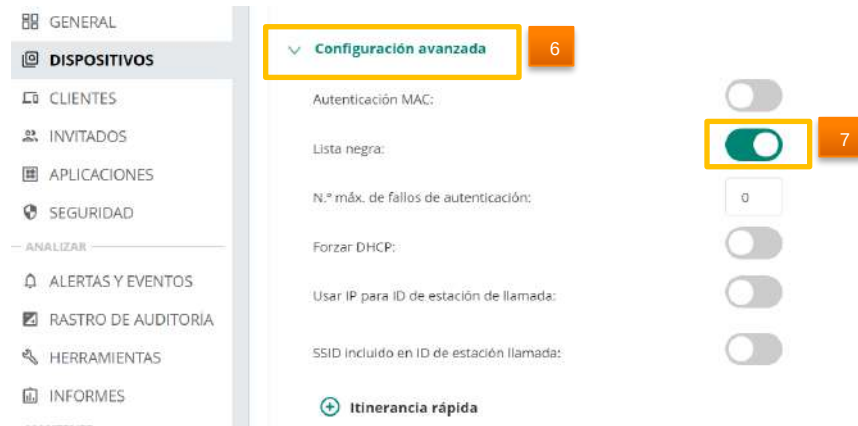
Nivel de seguridad:

Empresa Personal Portal de captación Abierta

Administración de claves:

WPA-2 Personal

- 6- Dar click en Configuración Avanzada
- 7- Activar la opción de Lista negra



Nota: para poder habilitar la opción de Lista negra es necesario que los ssid su nivel de seguridad sea **Empresa** o **Personal**, de lo contrario no se podrá bloquear por mac.

Para saber la dirección Mac de nuestros dispositivos daremos click en la siguiente pantalla:

- 8- Dar click en el submenú de CLIENTES
- 9- Copiar la dirección Mac del dispositivo



- 10- Una vez localizado la dirección Mac del dispositivo al que queremos bloquear, nos dirigimos al submenú de DISPOSITIVOS
- 11- Dar click en vista Configuracion
- 12- Dar click en Mostrar avanzadas



Cliente: prueba01
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

- GENERAL
- DISPOSITIVOS**
- CLIENTES
- INVITADOS
- APLICACIONES
- SEGURIDAD

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS

Mostrar avanzadas

10

Nombre	SEGURIDAD	TIPO DE ACCE...	ZONA	MODO DE RE...	RED ACTIVADA	ACCIONES
Banorte-Wifi	opensystem	Sin restricción		Puente	Si	
Empleados	wpa2-psk-aes	Sin restricción		Puente	Si	
Invitados	Captive Portal (...)	Basado en red		Puente	No	
Alertas	wpa2-psk-aes	Sin restricción		Puente	Si	

- 13- Dar click en el apartado de SEGURIDAD
- 14- Dar click Lista Negra



Cliente: prueba01
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

- GENERAL
- DISPOSITIVOS**
- CLIENTES
- INVITADOS
- APLICACIONES
- SEGURIDAD

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS PUERTOS **SEGURIDAD** VPN SERVICIOS SISTEMA AUDITORÍA DE CONFIGURACIÓN

Ocultar avanzadas

13

- > Usuario Para El Servidor Interno
- > Roles
- > Lista Negra**
- > IDS/IPS Inalámbrico

14

- 15- Ingresaremos las direcciones Mac, dando click en el icono de +



Cliente: prueba01
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

- GENERAL
- DISPOSITIVOS**
- CLIENTES
- INVITADOS
- APLICACIONES
- SEGURIDAD

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS PUERTOS **SEGURIDAD** VPN SERVICIOS SISTEMA AUDITORÍA DE CONFIGURACIÓN

Ocultar avanzadas

Lista negra manual

Lista negra manual

DIRECCIÓN MAC EN LA LISTA NEGR...

+

15

No hay datos para mostrar ahora mismo

16- En la siguiente pantalla ingresaremos la dirección Mac a bloquear

17- Para guardar cambios dar click en Aceptar

INTRODUZCA UNA DIRECCIÓN MAC

Dirección MAC: 78:88:6d:51:ca:e8

Cancelar Aceptar

18- Para eliminar esta dirección Mac dar click en 

19- Dar click en Guardar configuración

Cliente: prueba01
Volver A La Vista MSP

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ANALIZAR

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

HERRAMIENTAS

INFORMES

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS PUERTOS SEGURIDAD VPN SERVICIOS SISTEMA AUDITORIA DE CONFIGURACIÓN

Ocultar avanzadas

Lista Negra

Lista negra manual

Lista negra manual

DIRECCIÓN MAC	EN LA LISTA NEGR...
78:88:6d:51:ca:e8	6/2/2020 12:47:19

Lista negra dinámica

Cancelar Guardar configuración

Con esta configuración el dispositivo no tendrá acceso a la red inalámbrica del Access Point de Aruba.

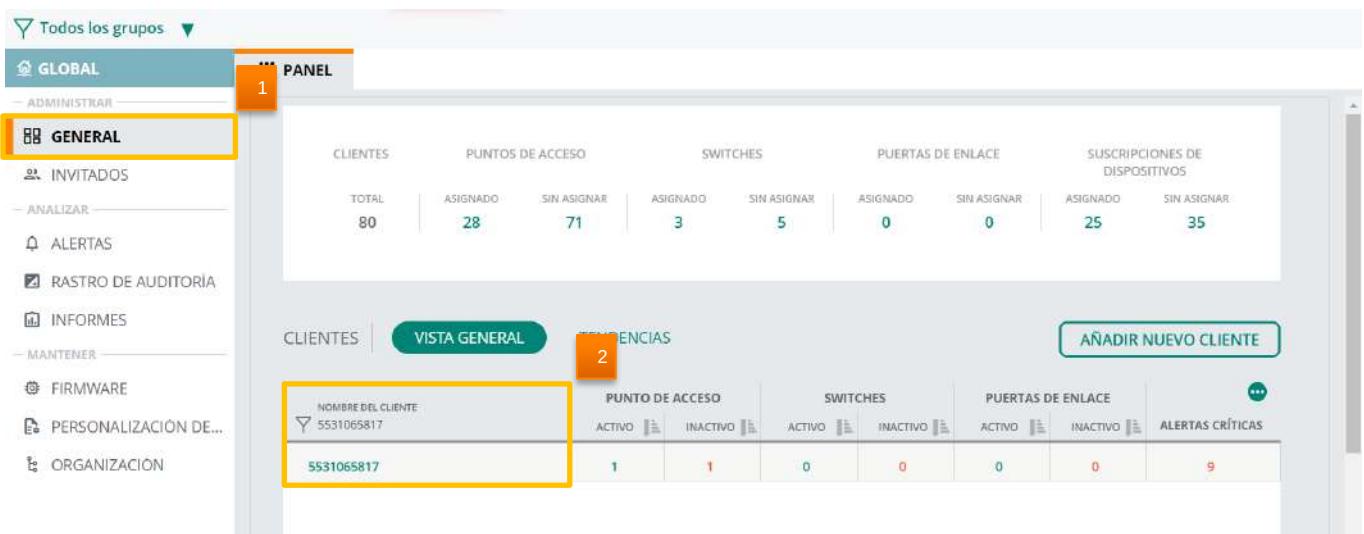
CONTROL DE ANCHO DE BANDA.

Aruba Central permite controlar el uso del ancho de banda en las redes inalámbricas, se puede poner un límite total por red o un límite por cada usuario que se conecte a esa red.

Para realizar la configuración de control de ancho de banda en un cliente es necesario primeramente seleccionar a dicho cliente.

Para ello realice lo siguiente:

1. Seleccionar **General** en el menú de contexto
2. Filtrar y seleccionar el **Nombre del cliente** para continuar con la configuración de control de ancho de banda

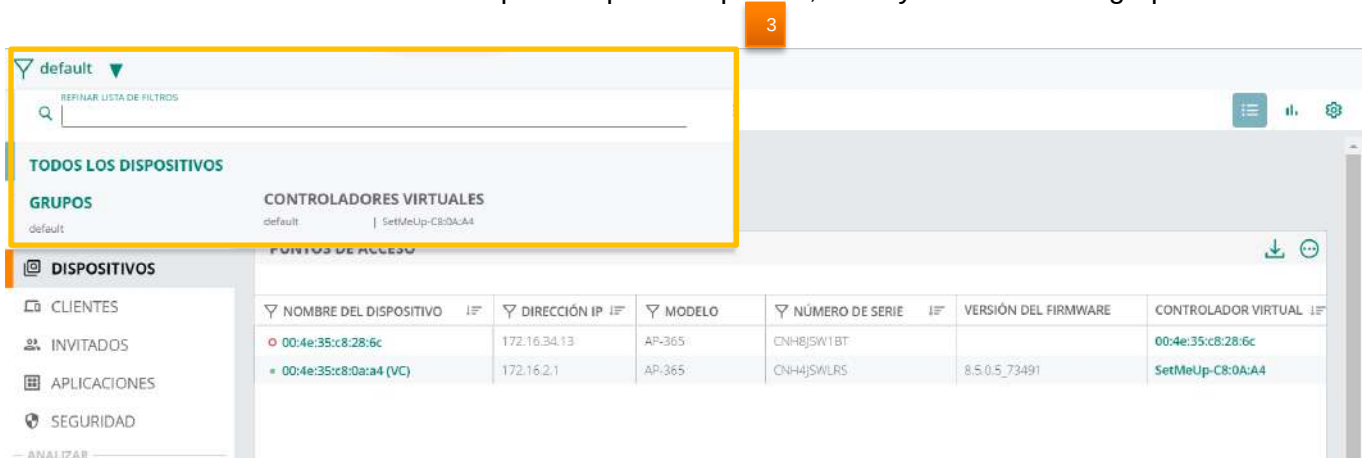


The screenshot shows the Aruba Central interface. On the left, the 'GENERAL' menu item is highlighted with an orange box and labeled with a red '1'. The main area displays a summary of network statistics. Below this, the 'CLIENTES' section is visible, with a red '2' pointing to the 'NOMBRE DEL CLIENTE' column in the table. The table has a red box around the first row, which contains the client ID '5531065817'.

CLIENTES	PUNTOS DE ACCESO		SWITCHES		PUERTAS DE ENLACE		SUSCRIPCIONES DE DISPOSITIVOS	
TOTAL	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR
80	28	71	3	5	0	0	25	35

NOMBRE DEL CLIENTE	PUNTO DE ACCESO		SWITCHES		PUERTAS DE ENLACE		ALERTAS CRÍTICAS
5531065817	ACTIVO	INACTIVO	ACTIVO	INACTIVO	ACTIVO	INACTIVO	
5531065817	1	1	0	0	0	0	9

3. En la lista de filtros ubicada en la parte superior izquierda, filtrar y seleccionar el grupo **default**



The screenshot shows the Aruba Central interface with the 'default' filter selected in the 'GRUPOS' section, highlighted with an orange box and labeled with a red '3'. The main area displays a table of network devices.

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CN-H8JSW1BT		00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CN-H4JSWLRS	8.5.0.5_73491	SetMeUp-C8:0A:A4

4. Seleccionar del menú contextual **Dispositivos**
5. Seleccionar el icono **configuración**

The screenshot shows the network management interface. On the left, the 'GRUPO' menu is expanded, and 'DISPOSITIVOS' is highlighted. On the right, the 'PUNTOS DE ACCESO' configuration page is displayed. The 'PUNTOS DE ACCESO' tab is selected, and the 'PUNTOS DE ACCESO' sub-tab is active. The 'PUNTOS DE ACCESO' table shows two entries: '00:4e:35:c8:28:6c' and '00:4e:35:c8:0a:a4 (VC)'. The 'PUNTOS DE ACCESO' table has columns: NOMBRE DEL DISPOSITIVO, DIRECCIÓN IP, MODELO, NÚMERO DE SERIE, VERSIÓN DEL FIRMWARE, and CONTROLADOR VIRTUAL. The 'PUNTOS DE ACCESO' table has a 'Configuración' icon in the top right corner.

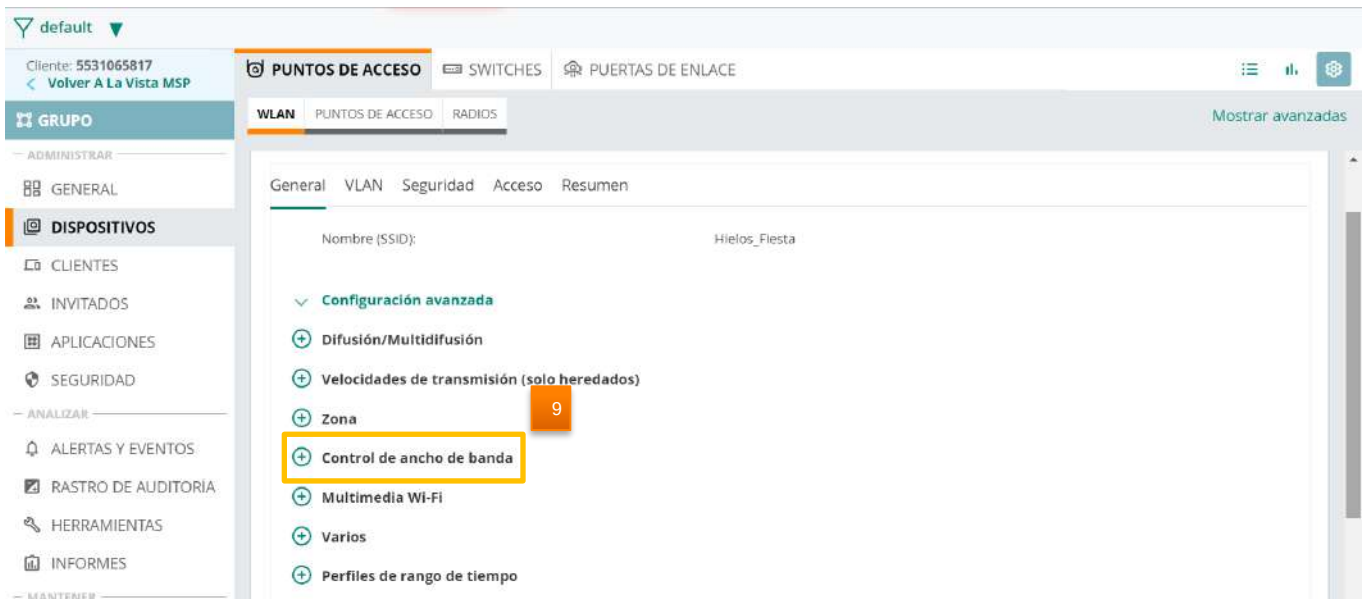
6. Seleccionar el menú **WLAN**
7. Posicionar el cursor sobre la red o SSID a configurar y selección el **icono lápiz**

The screenshot shows the network management interface. On the left, the 'GRUPO' menu is expanded, and 'DISPOSITIVOS' is highlighted. On the right, the 'WLAN' configuration page is displayed. The 'WLAN' tab is selected, and the 'SSID inalámbricos' sub-tab is active. The 'SSID inalámbricos' table shows several entries: 'WIFI Negocio', 'GIDAMO', 'wifi-soriana', 'hfiesta', 'infinitem_12...', and 'Hielos_Fiesta'. The 'Hielos_Fiesta' entry is highlighted. The 'Hielos_Fiesta' entry has a 'Configuración' icon in the top right corner.

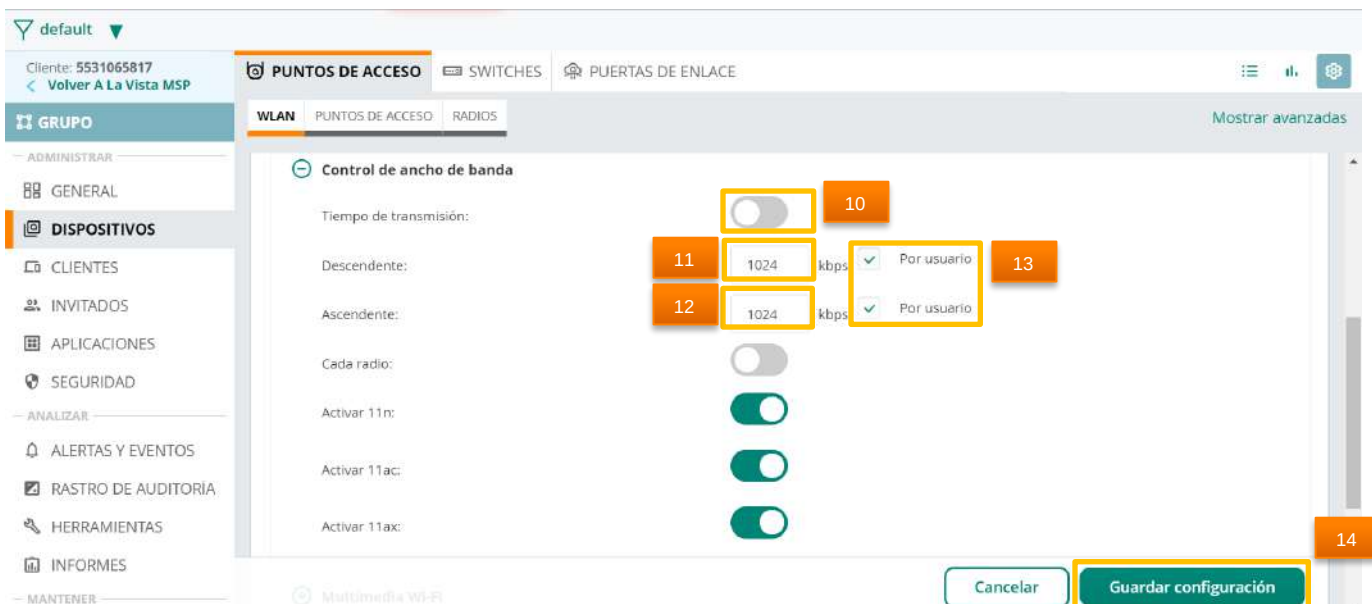
8. Seleccionar **Configuración avanzada**

The screenshot shows the network management interface. On the left, the 'GRUPO' menu is expanded, and 'DISPOSITIVOS' is highlighted. On the right, the 'Configuración avanzada' page for the 'Hielos_Fiesta' SSID is displayed. The 'Configuración avanzada' tab is selected, and the 'Configuración avanzada' sub-tab is active. The 'Configuración avanzada' page has a 'Configuración avanzada' button in the top right corner.

9. Seleccionar **Control de ancho de banda**



10. Seleccione **Tiempo de transmisión** para especificar una cantidad total de tiempo de transmisión que todos los clientes de esta red pueden usar. Se especifica en porcentaje
11. Establecer el valor **Descendente** en kbps. Ejemplo: 1024 kbps es el equivalente a 1 Mbps.
12. Establecer el valor **Ascendente** en kbps.
13. Si queremos limitar el ancho de banda descendente o ascendente por usuario solo seleccionamos **ambas casillas**.
14. Seleccionar el botón **Guardar configuración**.



Nota: si deseas que aplique por usuario lo definido para su ancho de banda Seleccionamos la casilla, pero si queremos que sea para toda la SSID lo dejamos en blanco

Para confirmar la configuración se puede realizar un test, en donde se puede verificar los Mbps descendentes y ascendentes



Para ello realice lo siguiente:

15. Seleccionar **General** en el menú de contexto
16. Filtrar y seleccionar el **Nombre del cliente** para continuar con la creación de página comercial en Facebook en una red de Invitados

Todos los grupos

GLOBAL

ADMINISTRAR

GENERAL

INVITADOS

ANALIZAR

ALERTAS

RASTRO DE AUDITORÍA

INFORMES

MANTENER

FIRMWARE

PERSONALIZACIÓN DE...

ORGANIZACIÓN

PANEL

1

CLIENTES

TOTAL	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR
80	28	71	3	5	0	0	25	35

CLIENTES

VISTA GENERAL

2

NOMBRE DEL CLIENTE

5531065817

PUNTO DE ACCESO	SWITCHES	PUERTAS DE ENLACE	ALERTAS CRÍTICAS
ACTIVO	INACTIVO	ACTIVO	INACTIVO
1	1	0	0
0	0	0	0
0	0	0	9

AÑADIR NUEVO CLIENTE

17. En la lista de filtros ubicada en la parte superior izquierda, filtrar y seleccionar el grupo **default**

default

REFINAR LISTA DE FILTROS

TODOS LOS DISPOSITIVOS

GRUPOS

default | SetMeUp-C8:0A:A4

DISPOSITIVOS

- CLIENTES
- INVITADOS
- APLICACIONES
- SEGURIDAD

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CN+HJ\$W1BT		00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CN+HJ\$WLRS	8.5.0.5_73491	SetMeUp-C8:0A:A4

18. Seleccionar del menú contextual **Invitados**
19. Seleccionar el icono **lista**
20. Seleccionar el icono **+ añadir perfil**

Dentro de esta página se configurará lo siguiente:

21. Nombre: Establecer un **nombre**, no se permiten caracteres especiales o acentos
 22. Tipo: Establecer **Wi-Fi de Facebook**
 23. Omitir nombre común: **Habilitar** esta opción para evitar problemas de certificado.
 24. Configuración de Wi-Fi avanzado de Facebook: Seleccionar **Editar ahora...**
- Al seleccionar esta opción mostrara otra ventana donde se configurarán los siguientes parámetros

25. Página de Facebook. **Seleccionar la página comercial** creada en el perfil de Facebook.
26. Modo de Omisión. Dar click en **Enlace para omitir registro**.
27. **Duración de la sesión**. Tiempo que darás a tus clientes de conexión a internet desde media hora hasta un día.
28. Seleccionar el botón **Guardar configuración**, para guardar los cambios



29. Al concluir saldrá el siguiente mensaje en la parte superior, proceda a cerrar la ventana



30. Seleccionar el botón



Vincular la red de invitados a un SSID.

En este apartado se realizara la vinculación de la red de invitados que se acaba de crear a un SSID

Para realizar la vinculación de la página comercial en Facebook a un SSID es necesario primeramente seleccionar a dicho cliente.

Para ello realice lo siguiente:

1. Seleccionar **General** en el menú de contexto
2. Filtrar y seleccionar el **Nombre del cliente** para continuar con la creación de página comercial en Facebook en una red de Invitados

1

2

CLIENTES	PUNTOS DE ACCESO		SWITCHES		PUERTAS DE ENLACE		SUSCRIPCIONES DE DISPOSITIVOS	
TOTAL	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR
80	28	71	3	5	0	0	25	35

NOMBRE DEL CLIENTE	PUNTO DE ACCESO	SWITCHES	PUERTAS DE ENLACE	ALERTAS CRÍTICAS
	ACTIVO	INACTIVO	ACTIVO	INACTIVO
5531065817	1	1	0	0

3. En la lista de filtros ubicada en la parte superior izquierda, filtrar y seleccionar el grupo **default**

3

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CN48JSW1BT	8.5.0.5_73491	00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CN44JSWLRS	8.5.0.5_73491	SetMeUp-C8:0A:A4

4. Seleccionar del menú contextual **Dispositivos**
5. Seleccionar el icono **configuración**

default ▾

Cliente: 5531065817
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

PUNTOS DE ACCESO + ACTIVO(S) 1 INACTIVO(S) 1 RADIOS 4

PUNTOS DE ACCESO

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CNH8JSW1BT		00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CNH4JSWLR5	8.5.0.5_73491	SetMeUp-C8-0A:A4

Configuración

6. Seleccionar el menú **WLAN**
7. Posicionar el cursor sobre la red o SSID a configurar y selección el icono lápiz

default ▾

Cliente: 5531065817
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ANALIZAR

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

HERRAMIENTAS

INFORMES

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN

Mostrar avanzadas

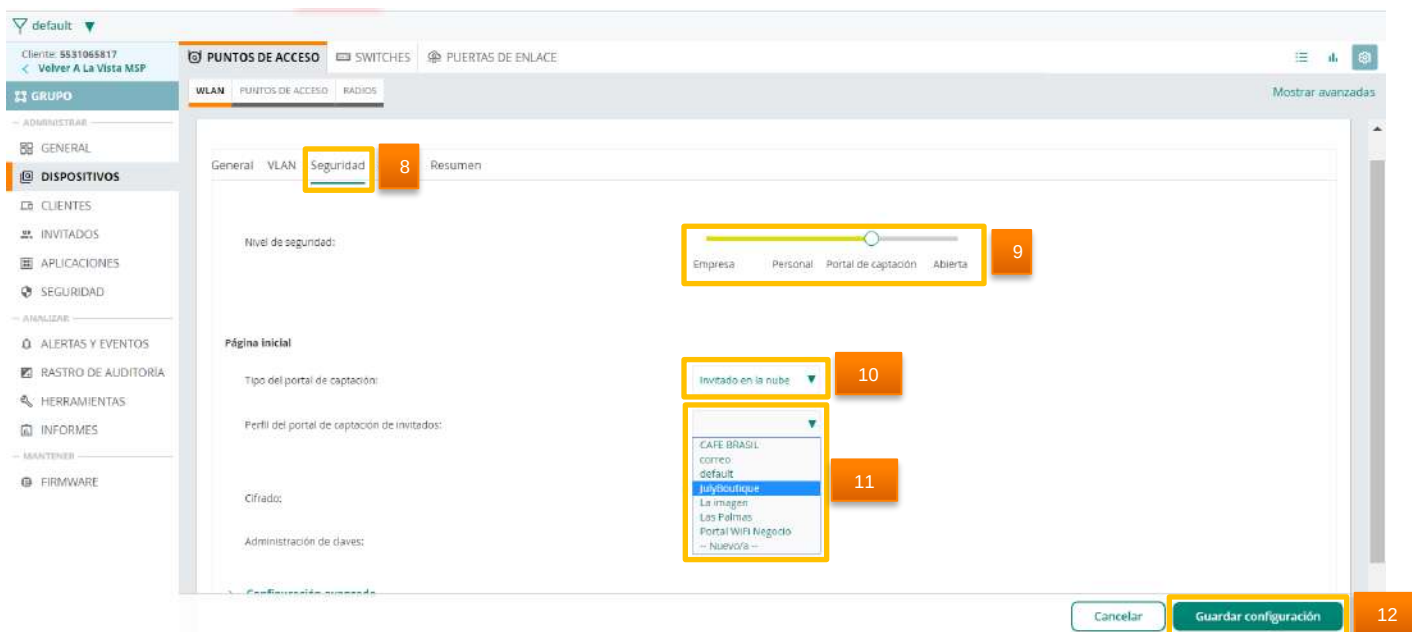
SSID inalámbricos

NOMBRE	SEGURIDAD	TIPO DE ACCESO	ZONA	MODULO DE REENVÍO ...	RED ACTIVADA	ACCIONES
WIFI Negocio	Captive Portal (external)	Sin restricción		Puente	No	
GIDAMO	wpa2-psk-aes	Basado en red		Puente	Si	
wifi-soniana	opensystem	Sin restricción		Puente	Si	
hfiesta	wpa2-psk-aes	Sin restricción		Puente	Si	
Infinitum_12345	wpa2-psk-aes	Sin restricción		Puente	Si	
Hielos_ fiesta	wpa2-psk-aes	Basado en red		Puente	Si	
JulyBoutique	Captive Portal (external)	Sin restricción		Puente	Si	[Edit Icon]

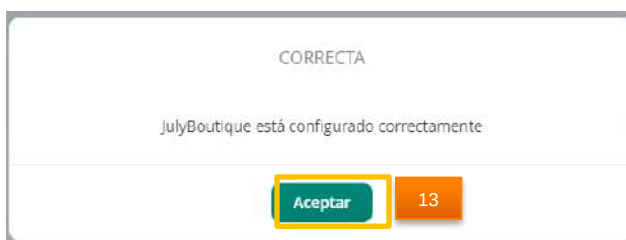
+ Añadir SSID

7 SSID

8. Seleccionar el apartado **Seguridad**
9. Cambiar Nivel de seguridad a: **Portal de captación**
10. Tipo de portal de captación: Seleccionar **invitado en la nube**
11. Perfil de portal de captación de invitado: **Seleccionar la red de invitados** que acabamos de crear en la primera sección de esta guía, en este caso JulyBoutique
12. Seleccionar el botón **Guardar configuración**



13. Seleccionar el botón aceptar para concluir la configuración



Nota: la landing page es administrada por Facebook, y los usuarios no son Administrados por nosotros.

14. Una vez conectado al SSID podremos ver que ya está configurada el wifi de Facebook de nuestro negocio para acceder a ella y poder navegar en internet.



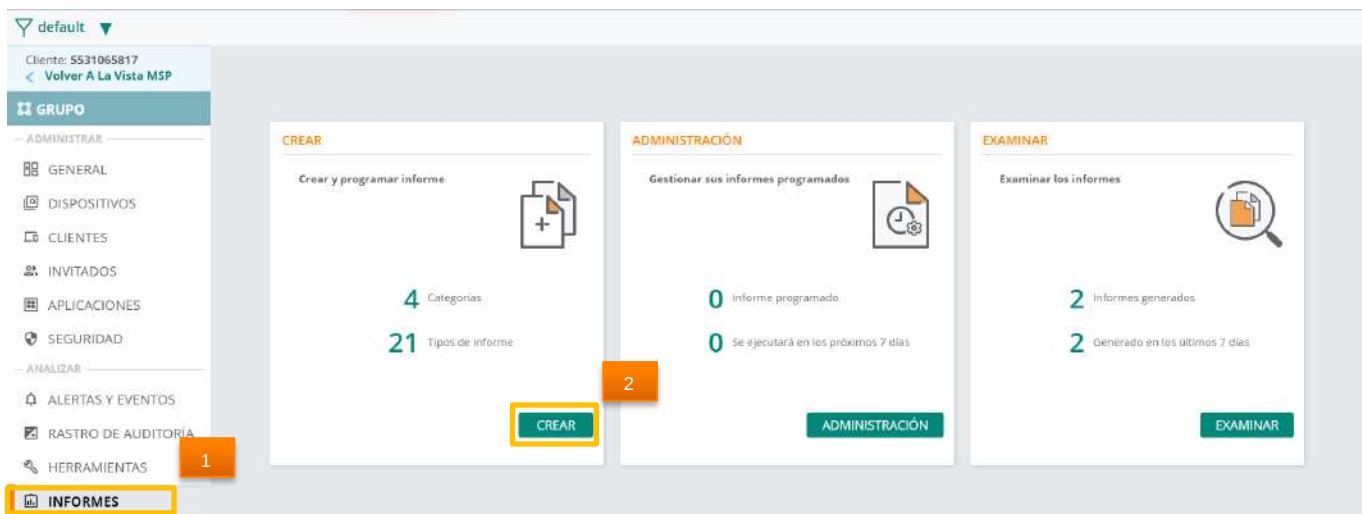
GENERACIÓN AUTOMÁTICA DE INFORMES.

El panel de control de Aruba Central le permite crear varios tipos de informes. Puede crear informes recurrentes o configurar los informes para que se ejecuten bajo demanda.

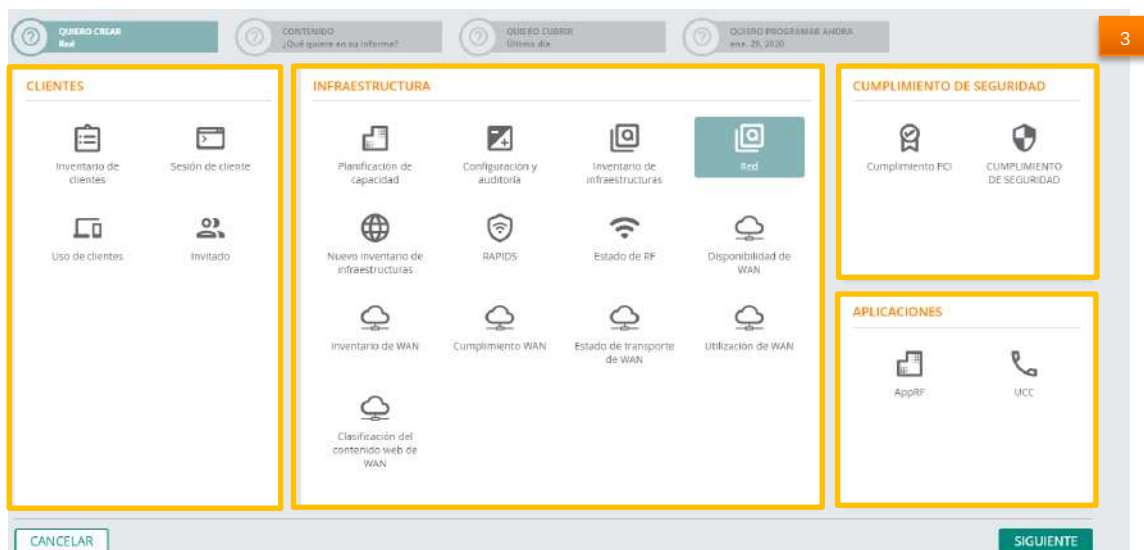
Nota: Para crear un informe, debe tener privilegios de lectura / escritura o derechos de administrador.

A continuación se describe el proceso para la generación automática de un informe

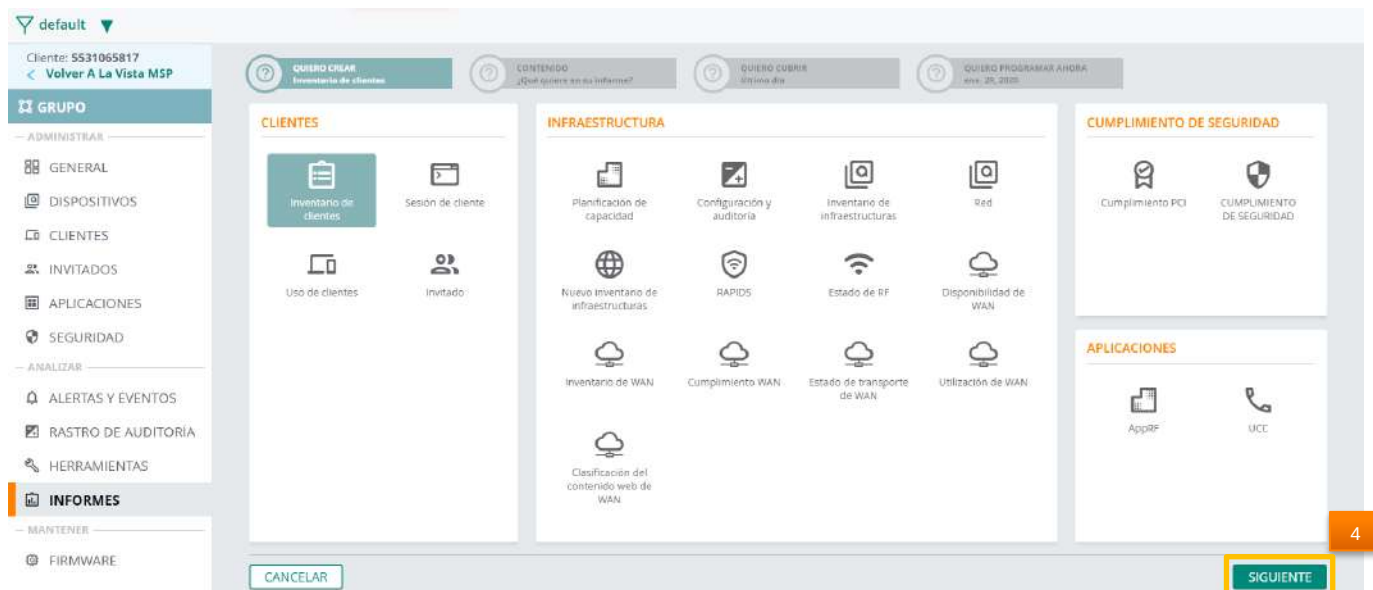
1. Seleccionar **Informes** del menú contextual
2. Seleccionar la Opción **Crear**



3. Seleccionar el **Tipo de informe** que se desea generar (La pantalla siguiente muestra todas las opciones disponibles de Informes organizadas en cuatro tipos). Clientes, Infraestructura, Cumplimiento de seguridad y Aplicaciones



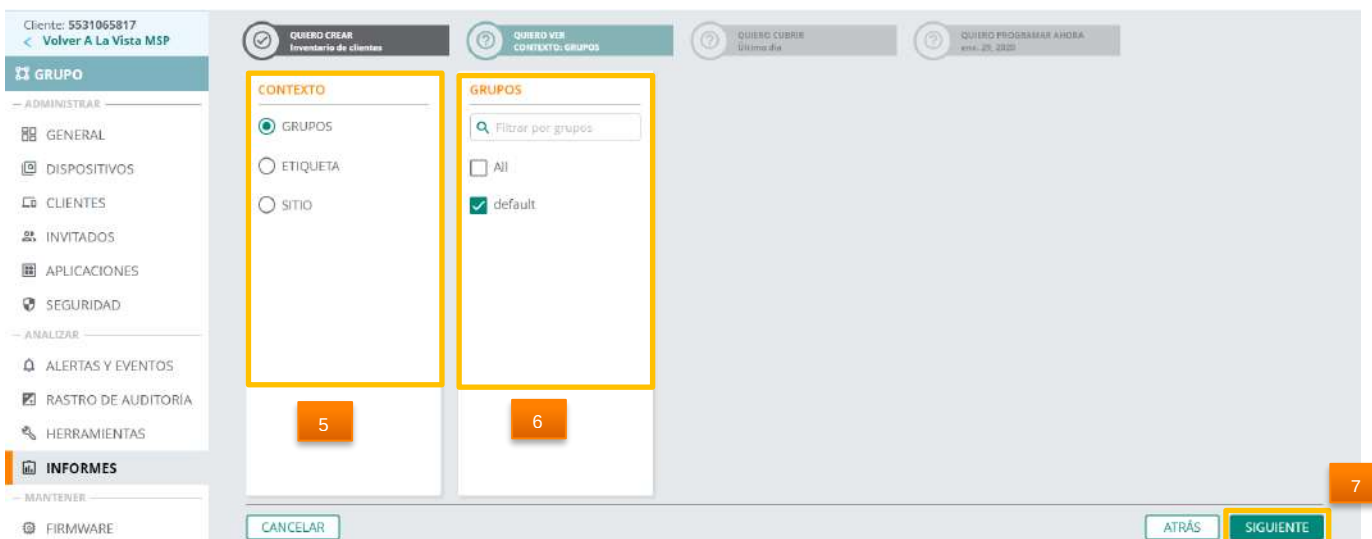
4. Una vez seleccionado el tipo de informe seleccionar el botón siguiente



5. En la Sección **Quiero crear** seleccionar el contexto; **Grupo, Etiqueta ó Sitio**, en base a lo requerido

6. Seleccionar el grupo **All, ó default** en base a lo requerido

7. Seleccionar el botón **Siguiente**



8. Seleccionar el Periodo del Informe

Elegir el **Rango personalizado** sobre el cual se quiere generar el informe

9. Seleccionar el botón **Siguiente**

10. Seleccionar la **periodicidad** del informe,

11. Seleccionar el **tiempo de ejecución**, moviendo el cursor sobre las manecillas del reloj

12. Establecer un **título del informe**

13. Establecer un **correo electrónico** al cual llegara el informe

14. Seleccionar el **formato** de salida

15. Seleccionar el botón **Generar**

Nota: La periodicidad del informe será establecida de acuerdo a las necesidades requeridas, para ser programado, a excepción de “Una vez (ahora)” derivado a que se ejecuta en ese instante y no puede ser programado. La programación se puede ver la parte superior

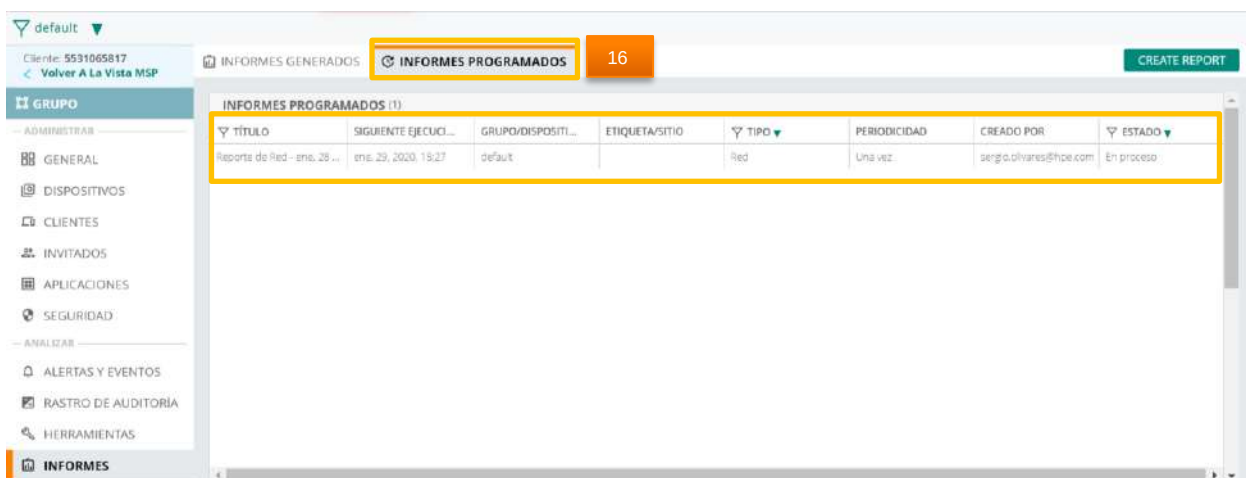


Al finalizar enviara el Mensaje **Informe creado correctamente.**

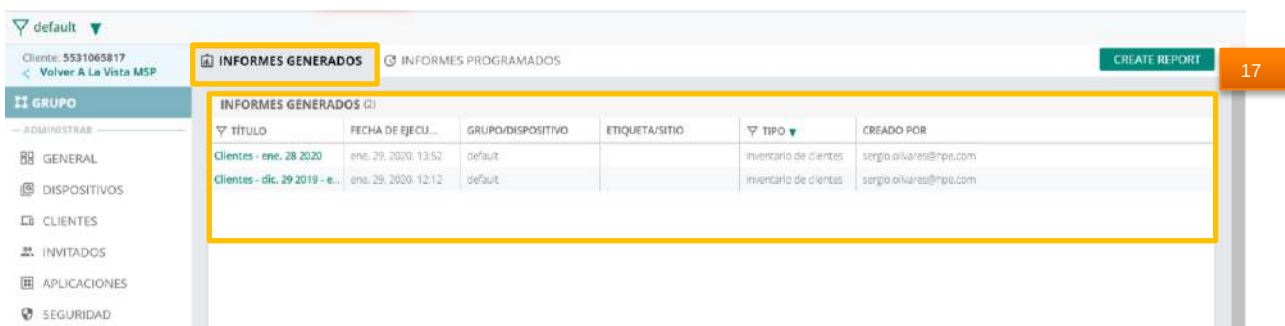
16. Seleccionar el botón **Aceptar**



17. Una vez generado el reporte se visualiza en la sección de **Informes programados**. Cabe hacer mención que el informe tarda aproximadamente 10 minutos en visualizarse en el correo establecido y en la parte Estado se muestra el estatus actual del informe



18. El informe queda registrado en la sección de **Informes Generados**.

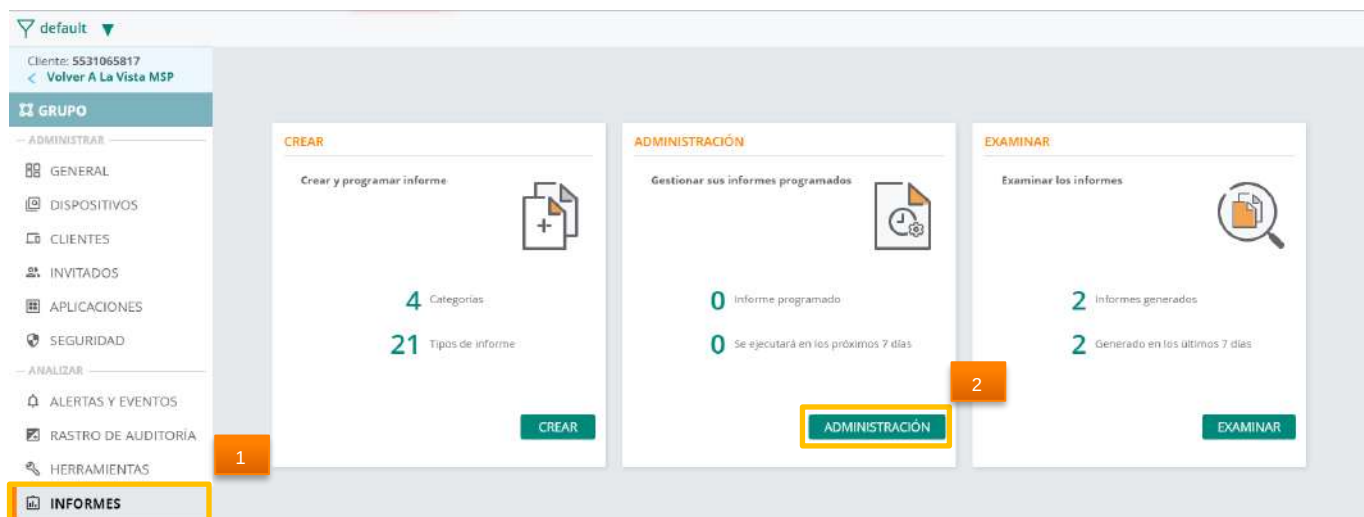


Administrar informes

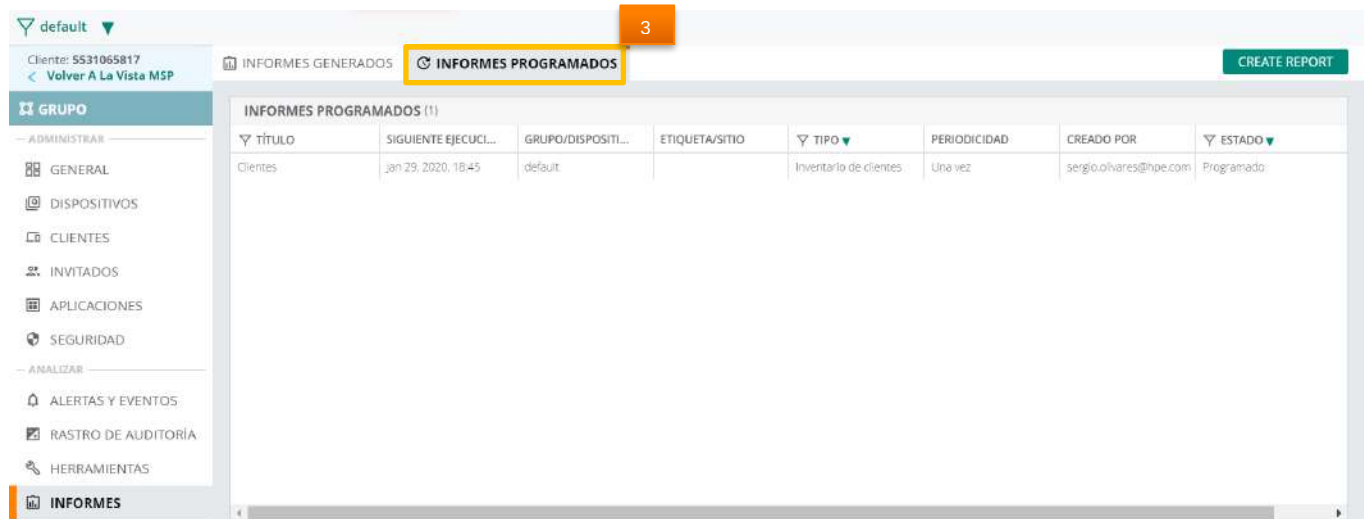
Una vez generado un informe se pueden administrar, editar o eliminar los informes programados.

Para la edición o eliminación de un informe seguir los siguientes pasos:

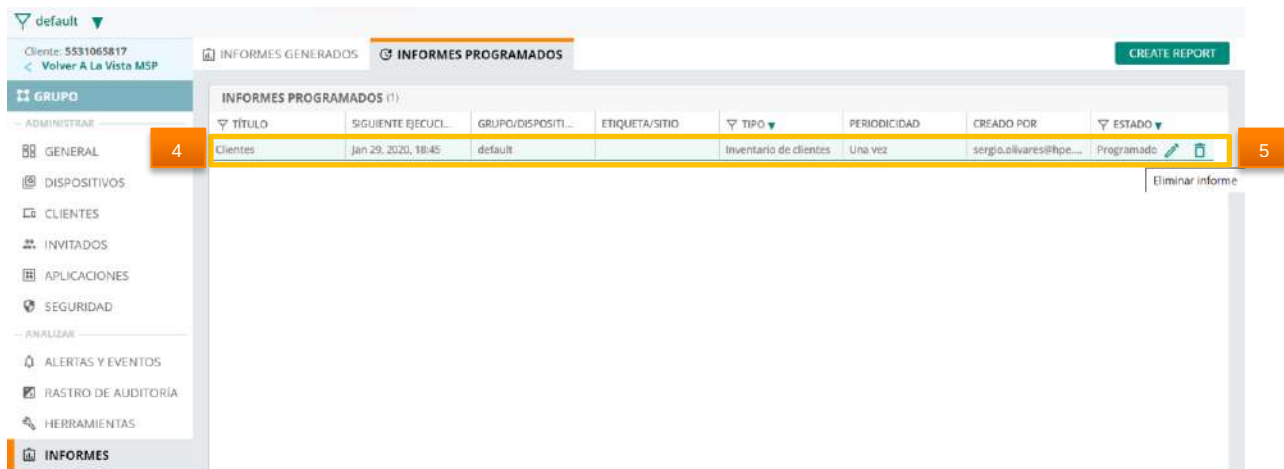
1. Seleccionar **Informes** del menú contextual ubicado en la parte inferior izquierda
2. Seleccionar **Administración** ubicada en la parte central



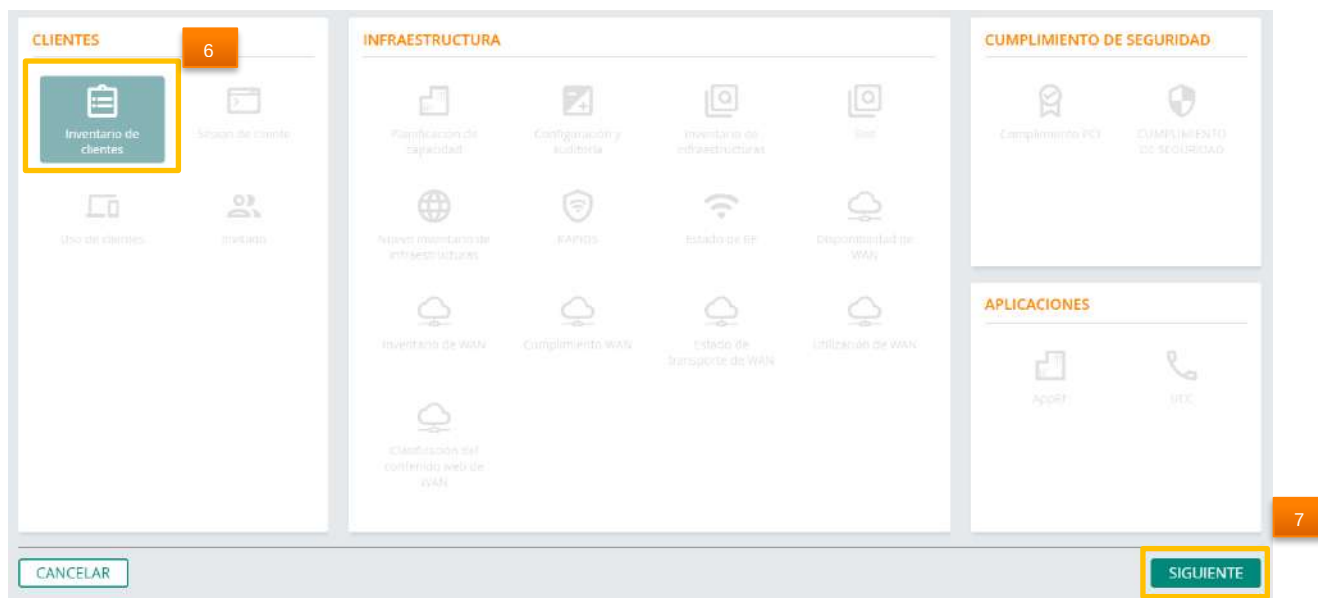
3. Seleccionar el menú **Informes Programados**



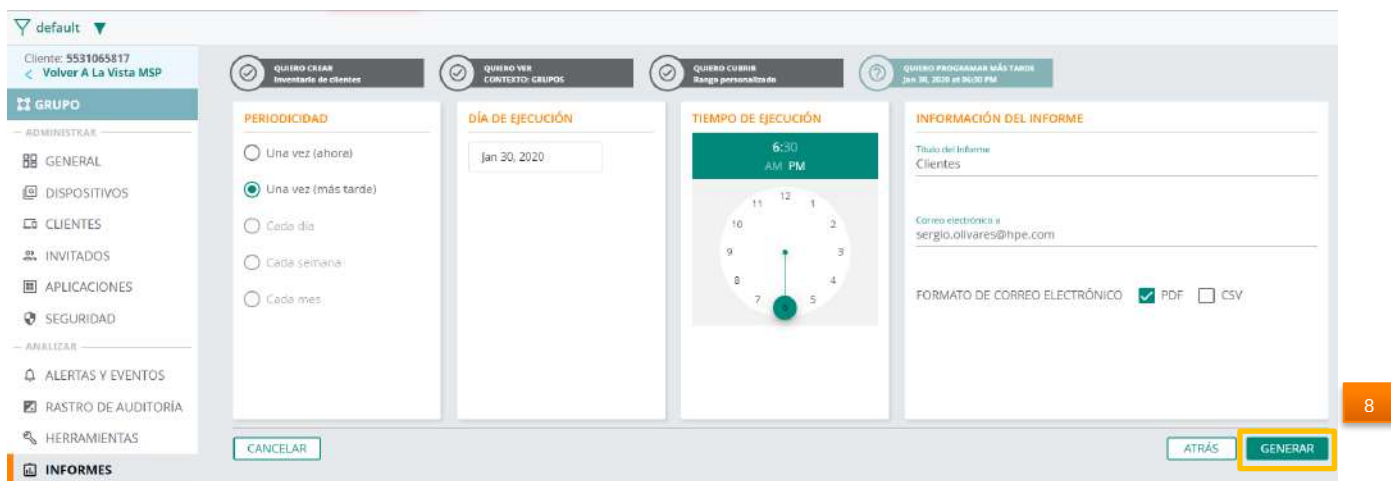
4. Posicionar el cursor sobre el informe a eliminar o editar, según sea el caso
5. Seleccionar el icono de lápiz para editar o el icono bote de basura para eliminar, según sea el caso



6. Si la acción a realizar es editar, se muestra la siguiente ventana, encontrándose marcado el informe creado anteriormente
7. Seleccionar el botón **siguiente** y continuar con la edición de los parámetros como se indica en los pasos anteriores “creación de informe”

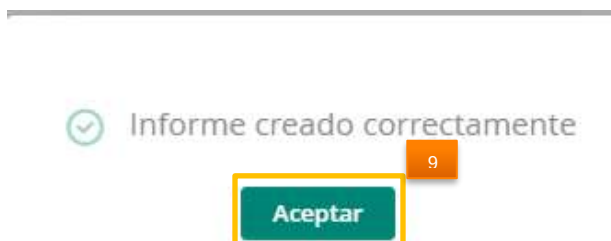


8. Al concluir los parámetros editados seleccionar el botón **Generar**



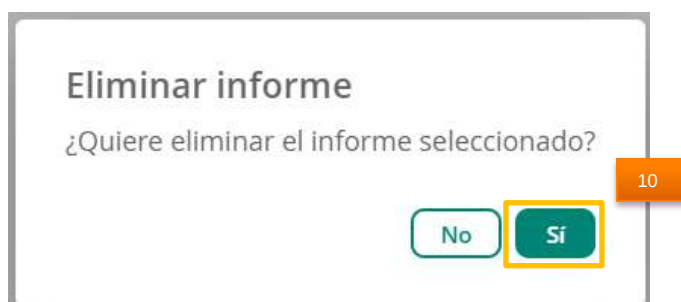
The screenshot shows a web application interface for generating reports. On the left is a sidebar menu with options like 'GRUPO', 'ADMINISTRAR', 'GENERAL', 'DISPOSITIVOS', 'CLIENTES', 'INVITADOS', 'APLICACIONES', 'SEGURIDAD', 'ANALIZAR', 'ALERTAS Y EVENTOS', 'RASTRO DE AUDITORIA', 'HERRAMIENTAS', and 'INFORMES'. The main area has four tabs: 'QUIERO CREAR', 'QUIERO VER', 'QUIERO CUBIR', and 'QUIERO PROGRAMAR MÁS TARDAR'. The 'QUIERO CREAR' tab is active, showing configuration options for 'PERIODICIDAD' (Frequency), 'DÍA DE EJECUCIÓN' (Execution Day), 'TIEMPO DE EJECUCIÓN' (Execution Time), and 'INFORMACIÓN DEL INFORME' (Report Information). The 'PERIODICIDAD' section has radio buttons for 'Una vez (ahora)', 'Una vez (más tarde)', 'Cada día', 'Cada semana', and 'Cada mes'. The 'DÍA DE EJECUCIÓN' section has a date input field showing 'Jan 30, 2020'. The 'TIEMPO DE EJECUCIÓN' section has a clock interface showing '6:30 AM'. The 'INFORMACIÓN DEL INFORME' section has fields for 'Título del Informe' (Report Title) and 'Correo electrónico a' (Email to), and a 'FORMATO DE CORREO ELECTRÓNICO' (Email Format) section with checkboxes for 'PDF' and 'CSV'. At the bottom right, there are three buttons: 'CANCELAR', 'ATRÁS', and 'GENERAR'. The 'GENERAR' button is highlighted with a yellow box and an orange callout bubble with the number '8'.

9. Seleccionar el botón **Aceptar**



The screenshot shows a confirmation dialog box with a green checkmark icon and the text 'Informe creado correctamente' (Report created successfully). Below the text is a green button labeled 'Aceptar' (Accept), which is highlighted with a yellow box and an orange callout bubble with the number '9'.

10. Si la acción a realizar es eliminar seleccione el icono bote de basura y presionar el botón **SI** para confirmar la acción



The screenshot shows a confirmation dialog box titled 'Eliminar informe' (Delete report) with the text '¿Quiere eliminar el informe seleccionado?' (Do you want to delete the selected report?). At the bottom, there are two buttons: 'No' and 'Sí' (Yes). The 'Sí' button is highlighted with a yellow box and an orange callout bubble with the number '10'.

AGRUPACIÓN DE EQUIPOS WIFI CONTRATADOS.

Sí desea hacer cambios muy seguidos para ir mostrando en su página nueva información de su negocio, Agrupando diferentes antenas puedes distribuir las redes, portales y configuraciones de manera rápida a todos los dispositivos sin tener que hacerlo de manera individual.

Esta guía se estará dividida en dos Módulos

- Creación de Grupos y Creación zonas

CREACIÓN DE GRUPOS

Para realizar este tipo de configuración es necesario primeramente generar un Grupo al cual ingresaremos todos nuestros APs y ellos tomaran la configuración de dicho grupo, sin necesidad de realizarla a cada AP. Para realizar la configuración es necesario primeramente seleccionar a dicho cliente.

Para ello realice lo siguiente:

31. Seleccionar **General** en el menú de contexto
32. Filtrar y seleccionar el **Nombre del cliente** para continuar con la configuración de control de ancho de banda

The screenshot shows the 'General' menu selected in the left sidebar. The main area displays a summary table and a detailed client table.

CLIENTES	PUNTOS DE ACCESO		SWITCHES		PUERTAS DE ENLACE		SUSCRIPCIONES DE DISPOSITIVOS	
TOTAL	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR
80	28	71	3	5	0	0	25	35

CLIENTES	PUNTO DE ACCESO		SWITCHES		PUERTAS DE ENLACE		ALERTAS CRÍTICAS
NOMBRE DEL CLIENTE	ACTIVO	INACTIVO	ACTIVO	INACTIVO	ACTIVO	INACTIVO	
5531065817	1	1	0	0	0	0	9

33. Seleccionar **Organización** del menú contextual

Cliente: 5531065817
Volver A La Vista MSP

ESTADO DE LA RED | RESUMEN | CONECTIVIDAD WI-FI | DETALLES Aruba Access | VISUALRF

GLOBAL

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

SERVICIOS DE RED

ANALIZAR

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

HERRAMIENTAS

INFORMES

MANTENER

FIRMWARE

ORGANIZACIÓN

NÚMERO DE DISPOSITIVOS

SIN ERRORES | PROBLEMAS POTENCIALES

NOMBRE DEL SITIO: ESTADO: ACTIVOS | INACTIVOS: USO INTENSIVO DE MEMORIA: USO INTENSIVO DE CPU: UTILIZACIÓN ALTA DE CH: 2.4 GHz | 5 GHz: RUIDO ALTO: 2.4 GHz | 5 GHz

MEXICO

CUBA

GUATEMALA

HONDURAS

Barbados

Jamaica

Dominican Republic

Puerto Rico

34. Seleccionar **+ Nuevo grupo** ubicado en la parte inferior

Cliente: 5531065817
Volver A La Vista MSP

GRUPOS | SITIOS Y ETIQUETAS | CERTIFICADOS | ADMINISTRADOR DE INSTALACIÓN

GLOBAL

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

SERVICIOS DE RED

ANALIZAR

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

HERRAMIENTAS

INFORMES

MANTENER

FIRMWARE

ORGANIZACIÓN

GRUPOS

Un grupo en Aruba Central actúa como contenedor de configuración principal de los dispositivos. Puede combinar dispositivos con requisitos de configuración comunes en un solo grupo y aplicar la misma configuración a todos los dispositivos del grupo.

ADMINISTRAR GRUPOS

ARRASTRE Y COLOQUE CLÚSTERES Y SWITCHES ENTRE GRUPOS

PARA SELECCIONAR VARIOS DISPOSITIVOS A LA VEZ, HAGA CLIC MANTENIENDO LA TECLA MAYÚS O CTRL PULSADA

NOMBRE DEL GRUPO	DISPOSITIVOS
TODOS LOS DISPOSITIVO...	1
DISPOSITIVOS SIN ASIGNAR	0
default	1

NOMBRE	UBICACIÓN	TIPO	N.º DE SERIE	DIRECCIÓN MAC
SetMetUp-CB.0A/A4	Mexico City,Mexico	IAP	CNH4JSWURS	00:4e:35:c8:0a:a4

+ Nuevo grupo

1 Grupo(s)

1 Dispositivo(s)

Nos va aparecerá una nueva ventana en la cual estableceremos los datos solicitados

35. Nombre del grupo: Establecer **nombre del grupo**

36. Utilizar el grupo como grupo de plantilla seleccionando el dispositivo: Seleccionar **Switch**

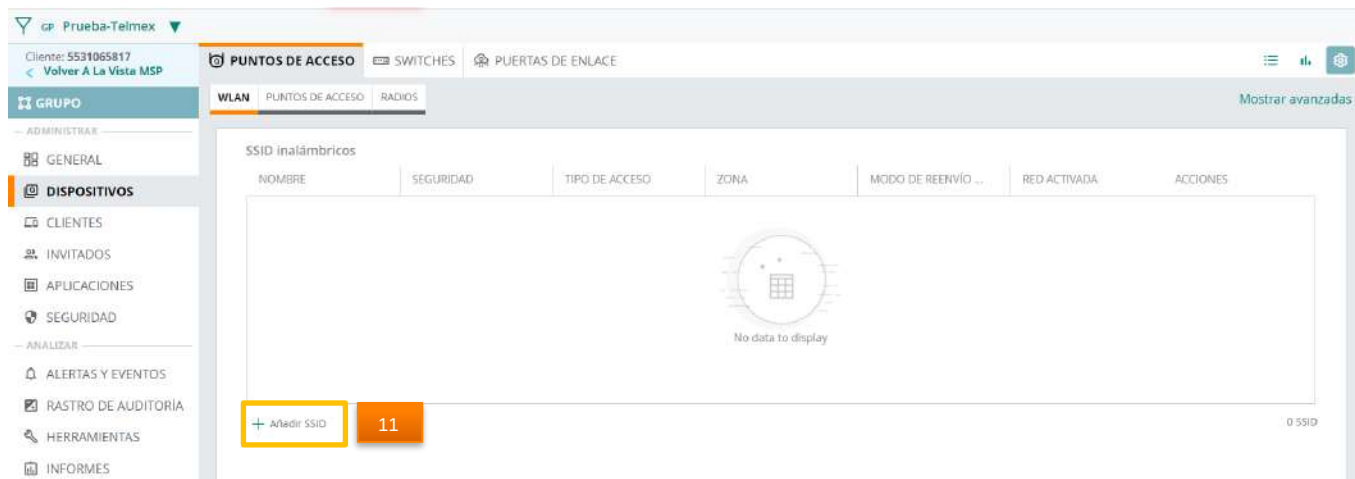
37. **Contraseña:** Establecer una contraseña para el grupo

38. **Confirmar contraseña:** Establecer la misma contraseña para corroborarla

39. Seleccionar el botón **Añadir grupo**

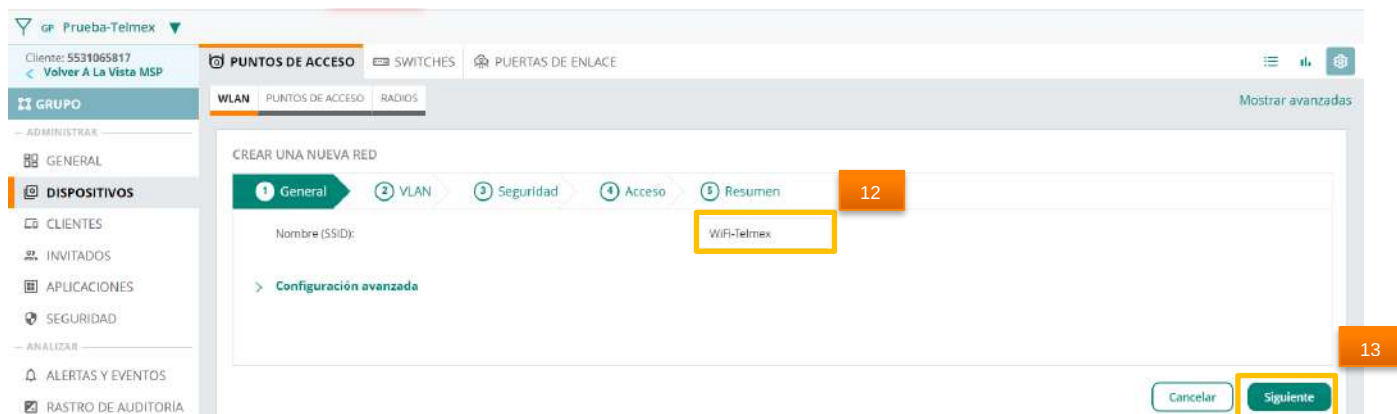
40. Posicionamos el cursos sobre le grupo creado y seleccionar **Config**

41. Seleccionar el signo de + para agregar una SSID



42. Establecer Un **nombre** al SSID

43. Seleccionar el botón **siguiente**



44. Asignación de IP de cliente: Seleccionar **Servidor DHCP externo asignado**

45. Asignación VLAN cliente: Seleccionar VLAN nativa

46. Seleccionar el botón **Siguiente**



47. Nivel de seguridad: Establecer **Personal**

48. Administración de claves: seleccionar la que se requiera, para este ejemplo WPA3-Personal

49. Frase de contraseña: Establecer una contraseña y confirmarla

50. Seleccionar el botón **siguiente**

Prueba-Telmex

Cliente: 5531065817
Volver A La Vista MSP

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS

Mostrar avanzadas

1 General 2 VLAN 3 Seguridad 4 Acceso 5 Resumen

Nivel de seguridad: Empresa Personal Portal de captación Abierta 17

Administración de claves: WPA3-Personal 18

Formato de frase de contraseña: 8-63 caracteres 19

Frase de contraseña:

Vuelva a escribirla:

Configuración avanzada

Cancelar Atrás Siguiente 20

51. Reglas de acceso: No modificar este parámetro, se establece como predeterminada.

52. Seleccionar el botón **siguiente**

Prueba-Telmex

Cliente: 5531065817
Volver A La Vista MSP

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN PUNTOS DE ACCESO RADIOS

Mostrar avanzadas

1 General 2 VLAN 3 Seguridad 4 Acceso 5 Resumen

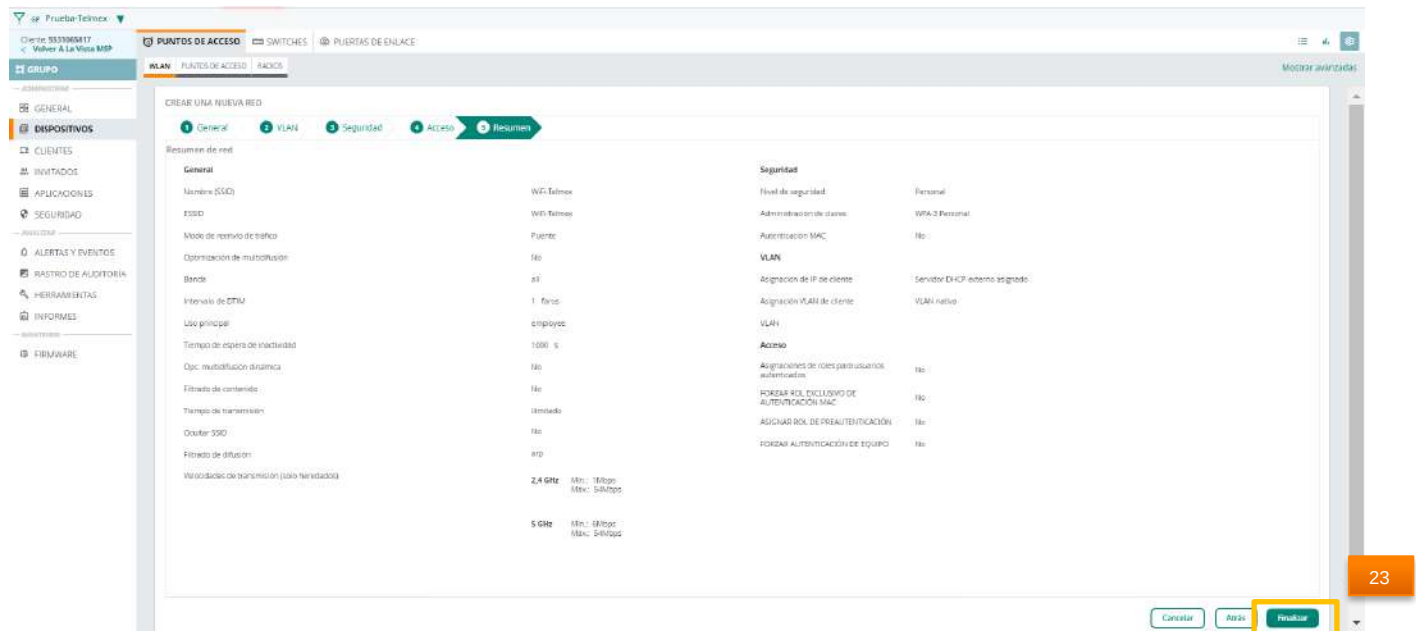
Reglas de acceso: Basado en rol Basado en red Sin restricción 21

⚠️ La opción Sin restricción permite acceso completo a la red. Esto puede generar problemas potenciales de seguridad.

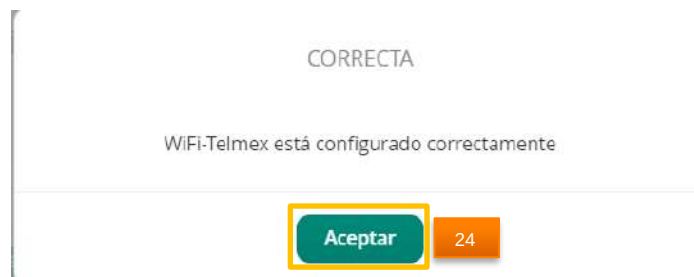
Rol descargable: ☐

Cancelar Atrás Siguiente 22

53. Seleccionar el botón **finalizar**



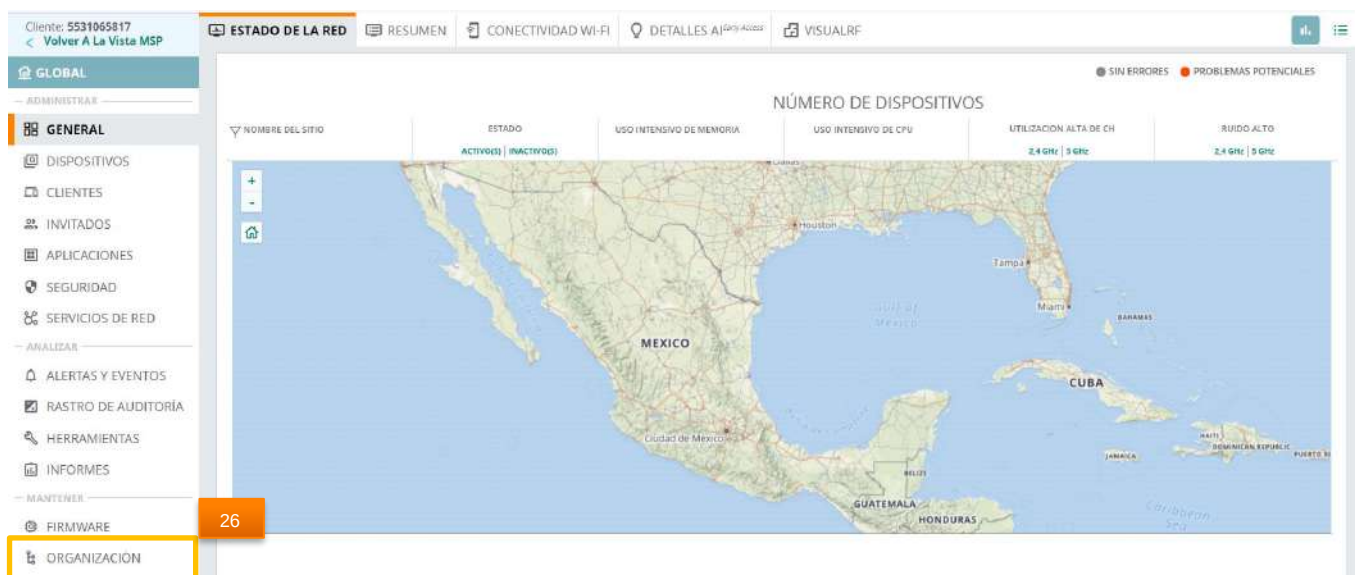
54. Seleccionar el botón **aceptar** para terminar la configuración



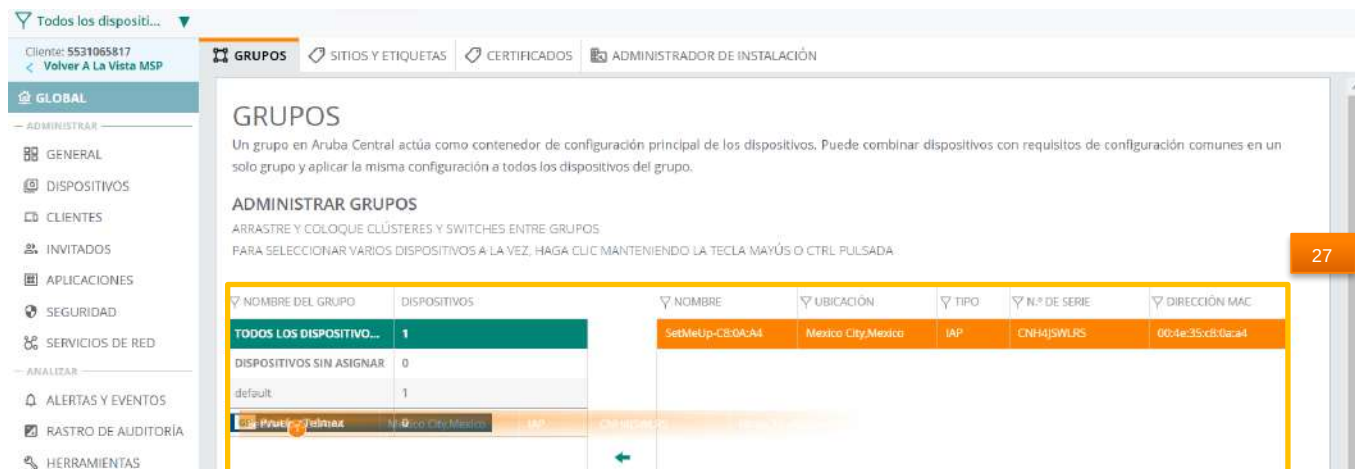
55. Filtrar por Todos los dispositivos



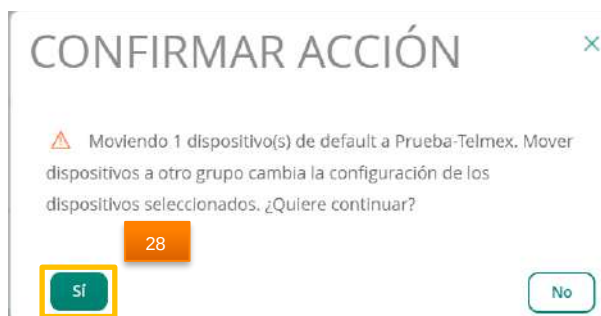
56. Seleccionar Organización del menú contextual



57. Seleccionar AP y lo arrastramos al grupo indicado, en este caso (Prueba-Telmex)



58. Seleccionar SI para confirmar la acción y terminar el proceso, quedando el AP asignado al nuevo Grupo Prueba Telmex.



CREACIÓN DE ZONAS

Para comenzar a configurar una zona se debe tener configurado previamente un SSID y seleccionar al Para ello realice lo siguiente:

1. Seleccionar **General** en el menú de contexto
2. Filtrar y seleccionar el **Nombre del cliente** para continuar con la configuración de control de ancho de banda

PANEL

Todos los grupos ▼

GLOBAL

ADMINISTRAR

GENERAL

INVITADOS

ANALIZAR

ALERTAS

RASTRO DE AUDITORÍA

INFORMES

MANTENER

FIRMWARE

PERSONALIZACIÓN DE...

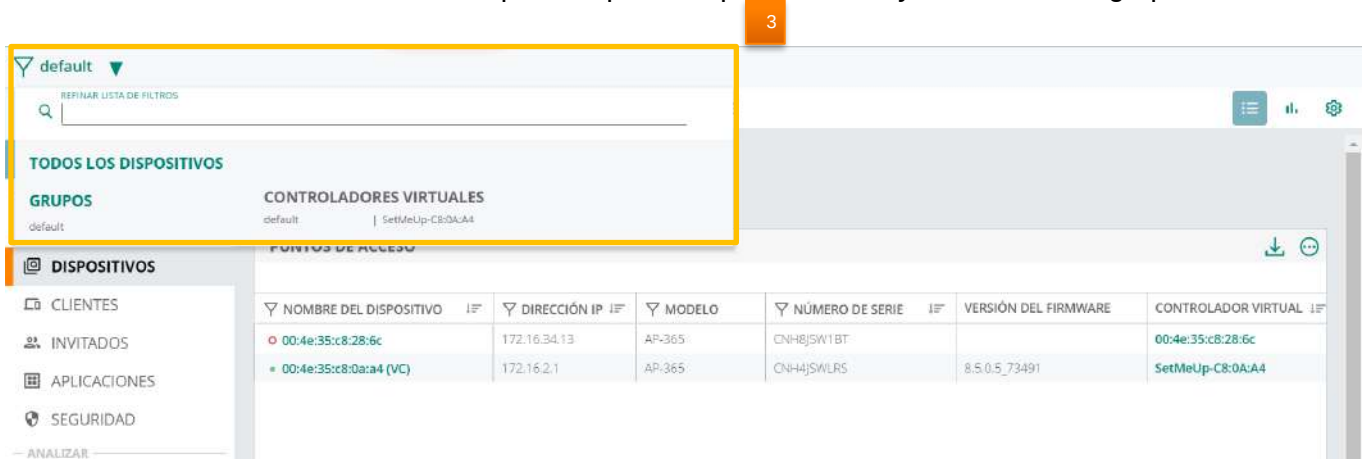
ORGANIZACIÓN

CLIENTES	PUNTOS DE ACCESO		SWITCHES		PUERTAS DE ENLACE		SUSCRIPCIONES DE DISPOSITIVOS	
TOTAL	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR	ASIGNADO	SIN ASIGNAR
80	28	71	3	5	0	0	25	35

CLIENTES | **VISTA GENERAL** | **INCIDENCIAS** | **AÑADIR NUEVO CLIENTE**

NOMBRE DEL CLIENTE	PUNTO DE ACCESO		SWITCHES		PUERTAS DE ENLACE		ALERTAS CRÍTICAS
5531065817	ACTIVO	INACTIVO	ACTIVO	INACTIVO	ACTIVO	INACTIVO	
5531065817	1	1	0	0	0	0	9

3. En la lista de filtros ubicada en la parte superior izquierda, filtrar y seleccionar el grupo **default**



default ▼

REFINAR LISTA DE FILTROS

TODOS LOS DISPOSITIVOS

GRUPOS

default

CONTROLADORES VIRTUALES

default | SetMeUp-C8:0A:A4

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ANALIZAR

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CNH8JSW1BT	8.5.0.5_73491	00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CNH4JSWLR5	8.5.0.5_73491	SetMeUp-C8:0A:A4

4. Seleccionar del menú contextual **Dispositivos**

5. Seleccionar el icono **configuración**



default ▼

Cliente: 5531065817

Volver A La Vista MSP

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

PUNTOS DE ACCESO

SWITCHES

PUERTAS DE ENLACE

PUNTOS DE ACCESO

ACTIVO(S) 2

INACTIVO(S) 1

RADIOS 4

NOMBRE DEL DISPOSITIVO	DIRECCIÓN IP	MODELO	NÚMERO DE SERIE	VERSIÓN DEL FIRMWARE	CONTROLADOR VIRTUAL
00:4e:35:c8:28:6c	172.16.34.13	AP-365	CNH8JSW1BT	8.5.0.5_73491	00:4e:35:c8:28:6c
00:4e:35:c8:0a:a4 (VC)	172.16.2.1	AP-365	CNH4JSWLR5	8.5.0.5_73491	SetMeUp-C8:0A:A4

Configuración

6. Seleccionar el menú **WLAN**

7. Posicionar el cursor sobre la red o SSID a configurar y selección el icono **lápiz**



default ▼

Cliente: 5531065817

Volver A La Vista MSP

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

PUNTOS DE ACCESO

SWITCHES

PUERTAS DE ENLACE

WLAN

PUNTOS DE ACCESO

RADIOS

Mostrar avanzadas

SSID inalámbricos

NOMBRE	SEGURIDAD	TIPO DE ACCESO	ZONA	MODULO DE REE...	RED ACTIVADA	ACCIONES
WIFI Negocio	Captive Portal (e...	Sin restricción		Puente	No	
GIDAMO	wpa2-psk-aes	Basado en red		Puente	Sí	
wifi-soriana	opensystem	Sin restricción		Puente	Sí	
hfiesta	wpa2-psk-aes	Sin restricción		Puente	Sí	
infinitum_12...	wpa2-psk-aes	Sin restricción		Puente	Sí	
Hielos_Fiesta	wpa2-psk-aes	Basado en red		Puente	Sí	

+ Añadir SSID

6 SSID

8. Ingresar a Configuración Avanzada
9. Dar clic en Zona
10. Asignar nombre en Apartado Zona

REDES > CONFIGURACIÓN - PASILLO

General VLAN Seguridad Acceso Resumen

Nombre (SSID): Pasillo

Configuración avanzada 8

Difusión/Multidifusión

Velocidades de transmisión (solo heredados)

Zona 9

Zona: Zona1 10

11. Dar clic en Guardar Configuración

Cancelar Guardar configuración 11

12. Validar que la zona se asignó correctamente en el SSID

NOMBRE	SEGURIDAD	TIPO DE ACCESO	ZONA	MODULO DE REENVÍO DET...	RED ACTIVADA	ACCIONES
Mesh	wpa2-psk-aes	sin restricción			SI	
Pasillo	wpa2-psk-aes	sin restricción	Zona1 12		SI	
Cancha	wpa2-psk-aes	sin restricción		Puerto	SI	
Comedor	wpa2-psk-aes	sin restricción		Puerto	SI	

Nota: Así se asignara un Nombre de zona a una SSID

En el punto siguiente se asigna el nombre de la zona, pero ahora en el Punto de Acceso (AP) para que Radie la Zona configurada en el paso anterior.

Nota: El Máximo de Zonas para configurar en un AP es de 6, estos campos deben ser separados por una "Coma"

13. Dar clic en el Submenú Puntos de Acceso
14. Ingresar al AP en el Icono  para Configurar la Zona

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

PUNTOS DE ACCESO 13

Mostrar avanzadas

Puntos de acceso

NOMBRE	NOMBRE DEL CO...	ESTADO	DIRECCIÓN IP	ASIGNACIÓN DE IP	MODULO	TIPO	3.4 GHz canal/ps...	5 GHz canal/ps...	
4448c10d0c0da	SetMcuP-CD-CD-DA	Online	192.168.1.21	DHCP	access	AP-207	Auto	Auto	 14
90948072ae8724	SetMcuP-CD-CD-DA	Online	192.168.1.124	DHCP	access	AP-207	Auto	Auto	
08234adcf8252	SetMcuP-CD-CD-DA	Online	192.168.1.23	DHCP	access	AP-207	Auto	Auto	

- Asignar el nombre de la Zona en el Apartado Zona De Punto de Acceso (debe ser el mismo nombre que se configuro en la SSID)



- Dar clic en Guardar Configuración



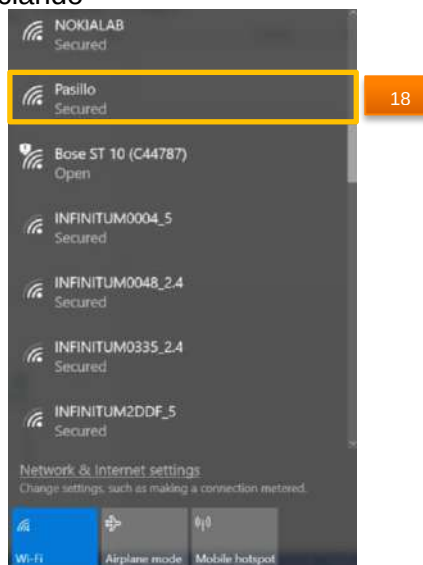
Nota: Si el SSID tiene Zona pero no Está configurada en el AP, esta no será Anunciada o Mostrada

- Mostrar cuales Zonas están configuradas en el AP's y son Anunciadas (en este caso solo la SSID Pasillo)

The screenshot shows a table of wireless SSIDs. The row for 'Pasillo' is highlighted with an orange box and labeled 17.

NOMBRE	SEGURIDAD	TIPO DE ACCESO	ZONA	MODOS DE REENVÍO DET...	RED ACTIVADA	ACCIONES
Mesh	wpa2-psk-aes	Sin restricción		Puente	SI	
Pasillo	wpa2-psk-aes	Sin restricción	Zona1	Puente	SI	
Cancha	wpa3-tae-aes	Sin restricción	Zona1	Puente	SI	
Corredor	wpa3-tae-aes	Sin restricción	Zona2	Puente	SI	

- Validar la SSID que está Anunciando



19. Asignar Zona a los siguientes AP's desde el Icono



19

20. Validar que después de configurar la Zona en el AP ya son Anunciadas las SSID (Zona1,Zona2)

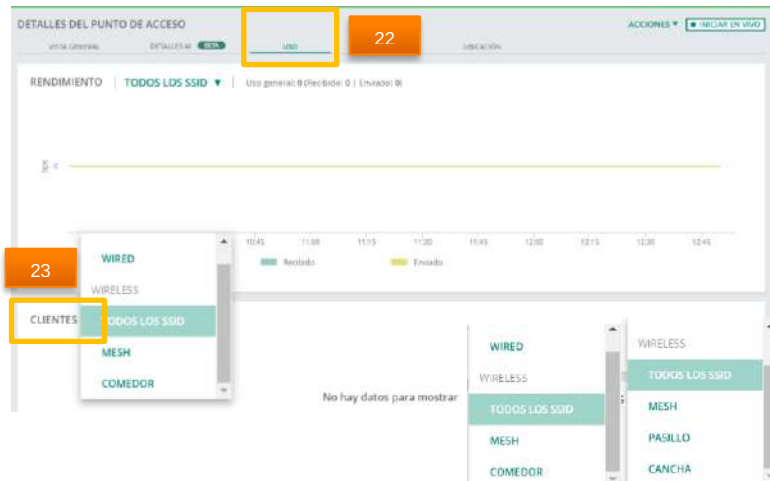


21. Ingresar al AP que se quiere validar que SSID está Anunciando

21

Nota: si tenemos configuradas diversas SSID con Zonas, estas solo se mostraran si están Configuradas en el AP, pero si la Zona no está configurada en la SSID y en el AP, estas se mostraran por Default en todas las AP que se encuentren en el Grupo Ejemplo el paso siguiente con la SSID (MESH)

22. Seleccionar la opción USO
23. Seleccionar Clientes, donde nos muestra que SSID está Radiando Este AP (Comedor y MESH)



Nota: se recomienda que para el uso de multizonas usen las versiones de Firmware posteriores a 6.5.4.7 y/o 8.3.0.0 o en su defecto por favor contacta a Cesar Barajas para que indique la versión homologada por Telmex.

RELOJ WIFI.

Controla el horario en que tus redes inalámbricas creadas estarán disponibles asegurando el uso de ellas en los horarios que tú consideres adecuados para tus usuarios

- 1- Entrar al ID de cliente, seleccionamos el grupo **Default** y
- 2- **DISPOSITIVOS**

- 3- Damos un click en el engrane



- 4- Desde la opción de WLAN
- 5- Debemos de seleccionar la SSID a la cual se le va configurar la denegación y damos un click en el lápiz 

Nota:Esta configuracion puede aplicar para una SSID tipo Empleado o Invitado.



default ▾

Cliente: prueba01
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ANALIZAR

ALERTAS Y EVENTOS

REPORTES DE AUDITORIA

PUNTOS DE ACCESO **4** ACCESO SWITCHES PUERTAS DE ENLACE

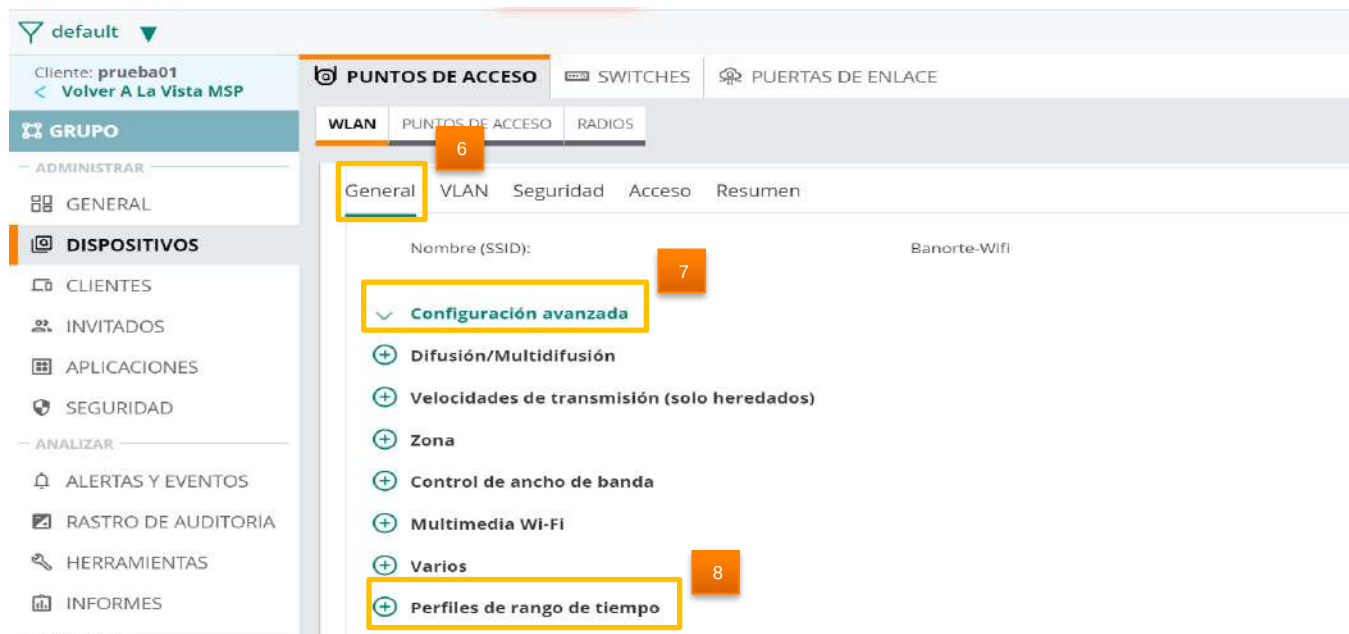
WLAN PUNTOS DE ACCESO RADIOS

Mostrar avanzadas

SSID inalámbricos

NOMBRE	SEGURIDAD	TIPO DE AC...	ZONA	MODO DE ...	RED ACTIVA...	ACCIONES 5
Banorte...	opensystem	Sin restricción		Puente	Si	
Emplead...	wpa2-psk-aes	Sin restricción		Puente	Si	
Invitados	Captive Porta...	Basado en red		Puente	No	
Alertas	wpa2-psk-aes	Sin restricción		Puente	Si	

- 6- una vez dentro, nos dirigimos a la pestaña de **General**.
- 7- Seleccionamos **Configuración avanzada**.
- 8- **Perfiles de rango de tiempo**.



default ▾

Cliente: prueba01
[Volver A La Vista MSP](#)

GRUPO

ADMINISTRAR

GENERAL

DISPOSITIVOS

CLIENTES

INVITADOS

APLICACIONES

SEGURIDAD

ANALIZAR

ALERTAS Y EVENTOS

RASTRO DE AUDITORIA

HERRAMIENTAS

INFORMES

REPORTES DE AUDITORIA

PUNTOS DE ACCESO SWITCHES PUERTAS DE ENLACE

WLAN **6** PUNTOS DE ACCESO RADIOS

General **6** VLAN Seguridad Acceso Resumen

Nombre (SSID): Banorte-Wifi

7 **Configuración avanzada**

- + Difusión/Multidifusión
- + Velocidades de transmisión (solo heredados)
- + Zona
- + Control de ancho de banda
- + Multimedia Wi-Fi
- + Varios
- 8** **+ Perfiles de rango de tiempo**

9- Colocamos el nombre al perfil

10- El siguiente paso se ingresa a la pantalla de configuración donde muestra dos opciones

Periódico y Absoluto

11- A continuación se genera la configuración de modo **Periódico** :

12- De **lunes a domingo**

13- **Horario inicial 8, Horario Final 19**

14- Le damos click en **Guardar**.

9

NUEVO PERFIL

Nombre:

Prueba

10

Tipo:

Periódico ▼

11

Repetir:

☒ Diario ☐ Semanal

Intervalo de fecha:

☒ Lunes - Domingo (todos los días) ☐ Lunes - Viernes (días laborables) ☐ Sábado - Domingo (fin de semana)

12

Hora Inicial:

Horas

8 ▼

13

Minutos

0 ▼

Hora Final:

Horas

19 ▼

Minutos

0 ▼

Nota: La visualización se aproxima a la hora.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																								
TUE																								
WED																								
THU																								
FRI																								
SAT																								
SUN																								

Duración de tiempo seleccionado

Cancelar

14

Guardar

15- Quedando de la siguiente manera

probando(Periodic Weekday 08:10 -

21:00)

Sí ▼

16- A continuación se describe el ejemplo donde se selecciona de forma **Absoluto**

17- con rango de fecha de **12/06/20 a 08/06/20**, y con horario de **8:00 am a 21:15 pm**, quedando de la siguiente manera la configuración.

18- Damos **Guardar** para que la Configuración quede establecida.

Nombre: 16

Tipo: Absoluto ▼

Intervalo de fecha: Día Inicial 02/06/2020  Día Final 08/06/2020  17

Hora Inicial: Horas 8 ▼ Minutos 0 ▼

Hora Final: Horas 21 ▼ Minutos 15 ▼

Cancelar Guardar 18

19- En la opción **Prueba de Tiempo/Absolute** seleccionamos **SI**

20- posteriormente **Guardar Configuración** como se muestra a continuación

PERFIL DE RANGO DE TIEMPO Estado

Prueba de Tiempo(Absolute Jun 19, 2019 08:00 - Jun 30, 2019 22:15) No se aplica ▼ 19

horario(Absolute Jun 19, 2019 11:00 - Jun 30, 2019 18:15) SI

+ Nuevo perfil de rango de tiempo

Nota: La visualización se aproxima a la hora.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MON																								
TUE																								
WED																								

Cancelar Guardar configuración 20

De esta forma es como se genera una configuración de tiempo para una SSID.

VISUALIZACIÓN POR TIPO DE DISPOSITIVO

Visualiza el tipo de dispositivo que está conectado a tu red.

1- Una vez que se ingresó al cliente nos vamos a la opción de **CLIENTES**.

Cliente: 5531065817
[Volver A La Vista MSP](#)

GLOBAL

ADMINISTRAR

- GENERAL
- DISPOSITIVOS
- CLIENTES**
- INVITADOS
- APLICACIONES
- SEGURIDAD
- SERVICIOS DE RED

ANALIZAR

- ALERTAS Y EVENTOS
- RASTRO DE AUDITORÍA

CLIENTES

CLIENTES | TODO ▾

5.05 GB (318.34 MB | 4.1)

INALÁMBRICO
 CONECTADO 30
 ERROR 0
 SIN CONEXIÓN 20
 CON CABLE
 CONECTADO 0
 ERROR 0
 SIN CONE 0

1	NOMBRE DE...	ESTADO ▾	DIREC...	VLAN	CONECTADO A	RO...	ROL DE ...
	JavierReyes-PC	Conectado	172.16.2.50	1	00:4e:35:c8:0a:a4	wifi-soriana	
	0c:cb:85:e3:57:23	Conectado	172.16.2.226	1	00:4e:35:c8:0a:a4	hfiesta	
	DUCESCLERICAH	Conectado	172.16.2.13	1	00:4e:35:c8:0a:a4	wifi-soriana	
	iPhoneDeSergio	Conectado	172.16.2.246	1	00:4e:35:c8:0a:a4	wifi-soriana	
	DUCIEMPLEREZ...	Conectado	172.16.2.4	1	00:4e:35:c8:0a:a4	hfiesta	
	android-d74ed...	Conectado	172.16.2.232	1	00:4e:35:c8:0a:a4	hfiesta	
	HUAWEI_P20_lit...	Conectado	172.16.2.229	1	00:4e:35:c8:0a:a4	Hielos_Fiesta	

2.- En esta pantalla nos aparecerán el total de clientes conectados y el tipo de dispositivos (iPhone, Android, Huawei etc.)

Cliente: 5531065817
[Volver A La Vista MSP](#)

GLOBAL

ADMINISTRAR

- GENERAL
- DISPOSITIVOS
- CLIENTES**
- INVITADOS
- APLICACIONES
- SEGURIDAD
- SERVICIOS DE RED

ANALIZAR

- ALERTAS Y EVENTOS
- RASTRO DE AUDITORÍA

CLIENTES

CLIENTES | TODO ▾

5.05 GB (318.34 MB | 4.1)

INALÁMBRICO
 CONECTADO 30
 ERROR 0
 SIN CONEXIÓN 20
 CON CABLE
 CONECTADO 0
 ERROR 0
 SIN CONE 0

2	NOMBRE DE...	ESTADO ▾	DIREC...	VLAN	CONECTADO A	RO...	ROL DE ...
	JavierReyes-PC	Conectado	172.16.2.50	1	00:4e:35:c8:0a:a4	wifi-soriana	
	0c:cb:85:e3:57:23	Conectado	172.16.2.226	1	00:4e:35:c8:0a:a4	hfiesta	
	DUCESCLERICAH	Conectado	172.16.2.13	1	00:4e:35:c8:0a:a4	wifi-soriana	
	iPhoneDeSergio	Conectado	172.16.2.246	1	00:4e:35:c8:0a:a4	wifi-soriana	
	DUCIEMPLEREZ...	Conectado	172.16.2.4	1	00:4e:35:c8:0a:a4	hfiesta	
	android-d74ed...	Conectado	172.16.2.232	1	00:4e:35:c8:0a:a4	hfiesta	
	HUAWEI_P20_lit...	Conectado	172.16.2.229	1	00:4e:35:c8:0a:a4	Hielos_Fiesta	

CREAR MAPAS DE CALOR EN CENTRAL ARUBA

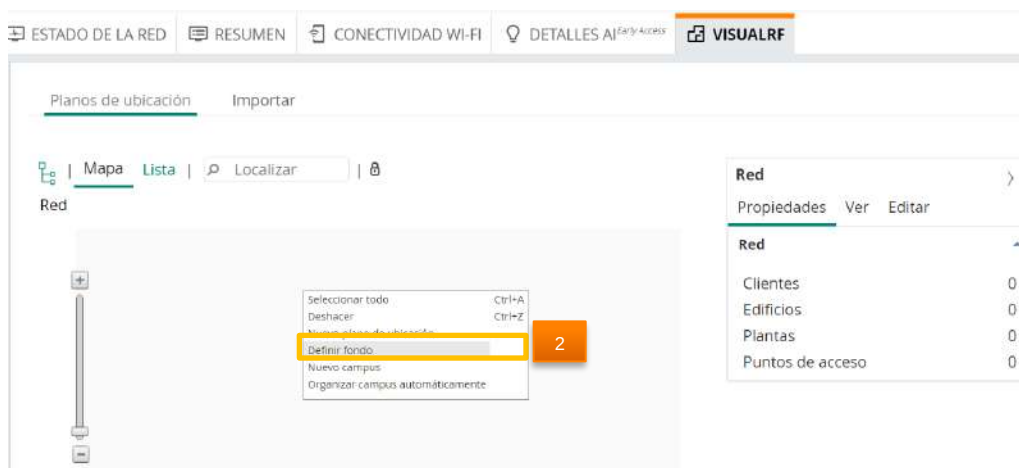
1- En el submenú GENERAL seleccionaremos VISUALRF.



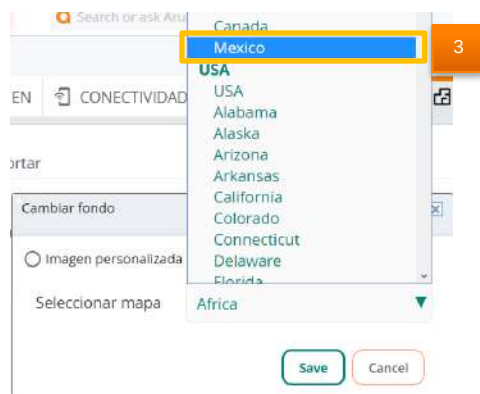
En esta pantalla importaremos un mapa para ubicar nuestro Access Point.

Dar click derecho sobre la pantalla en blanco.

2- Dar click en Definir fondo.



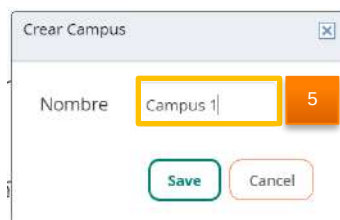
3- Dar click en seleccionar mapa, escoger México.



4- Una vez cargado el mapa, dar click derecho y escoger Nuevo campus.



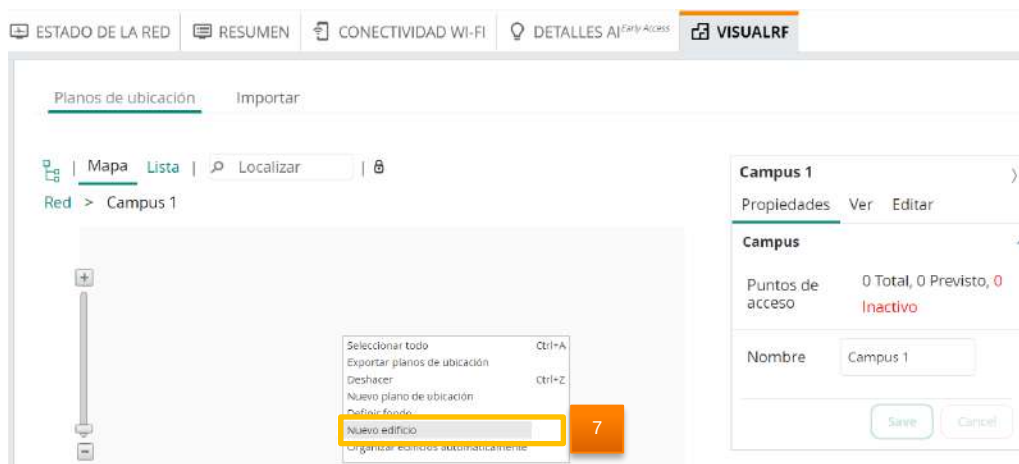
5- Poner el nombre a nuestro campus.



6- Nos posicionamos en el icono y daremos doble click.



7- Ahora daremos click derecho sobre la zona gris y escogeremos Nuevo edificio.



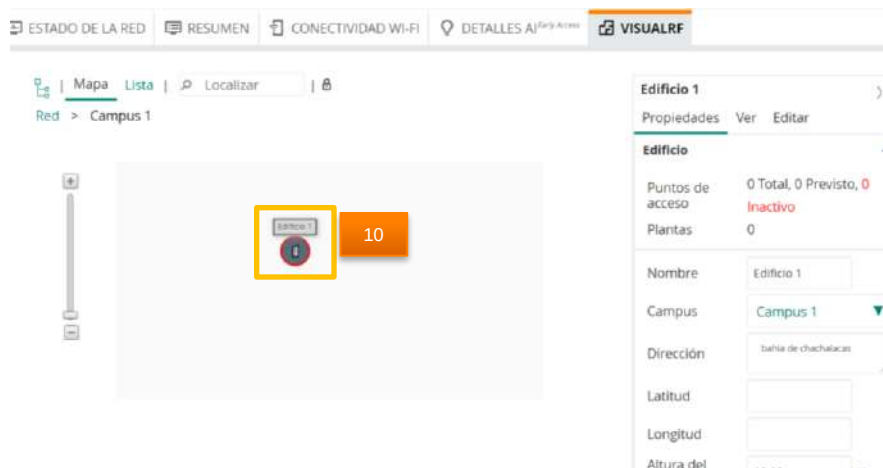
8- Completar los campos de Nombre y Dirección.

9- Dar click en Save.



De esta manera quedara creado el nuevo edificio.

10- Dar doble click sobre el icono.



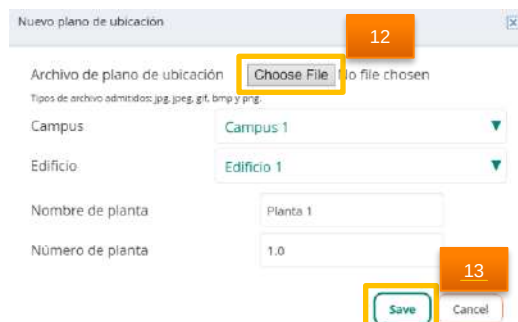
Dar click derecho sobre la zona gris.

11- Dar click en Nuevo plano de ubicación

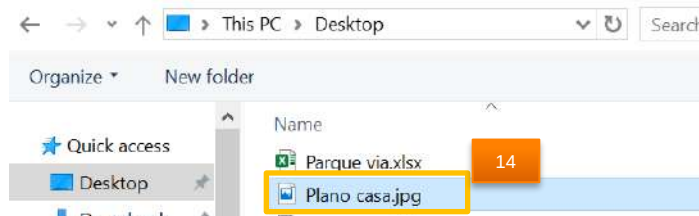


12- Click en Choose File, para cargar nuestro plano, en los formatos admitidos.

13- Click en Save.



14- Seleccionar nuestro archivo en el Explorer.



15- Dar click en Save.

Nuevo plano de ubicación

Archivo de plano de ubicación: Plano casa.jpg

Tipos de archivo admitidos: jpg, jpeg, gif, bmp y png.

Campus:

Edificio:

Nombre de planta:

Número de planta:

Ahora comenzaremos a configurar VisualRF.

16- Con el mouse arrastrar la zona sombreada hasta los bordes del plano.



17- Dar click en el icono de  Medir

18- Dibujar una línea sobre la parte sombreada, nos aparecerá un mensaje de que se está excediendo el límite del área (poner metros reales del plano).

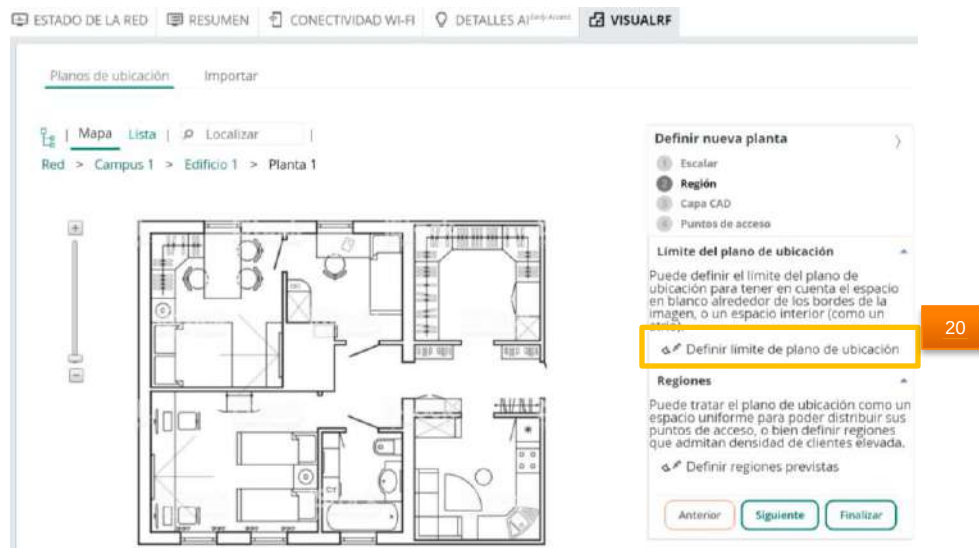


19- Dar click en Siguiente.

20- Ahora daremos click en el icono de  Definir límite de plano de ubicación

21- Ahora dibujaremos la limitación de nuestro plano.

22- Click en Siguiente.



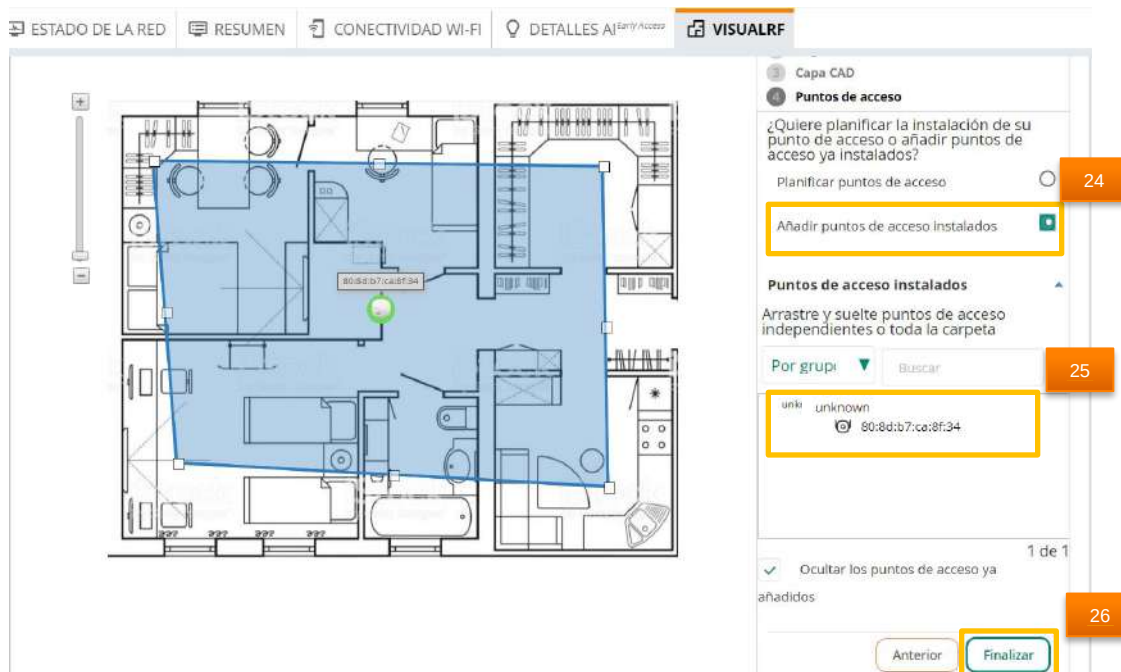
23- Click en Siguiente.



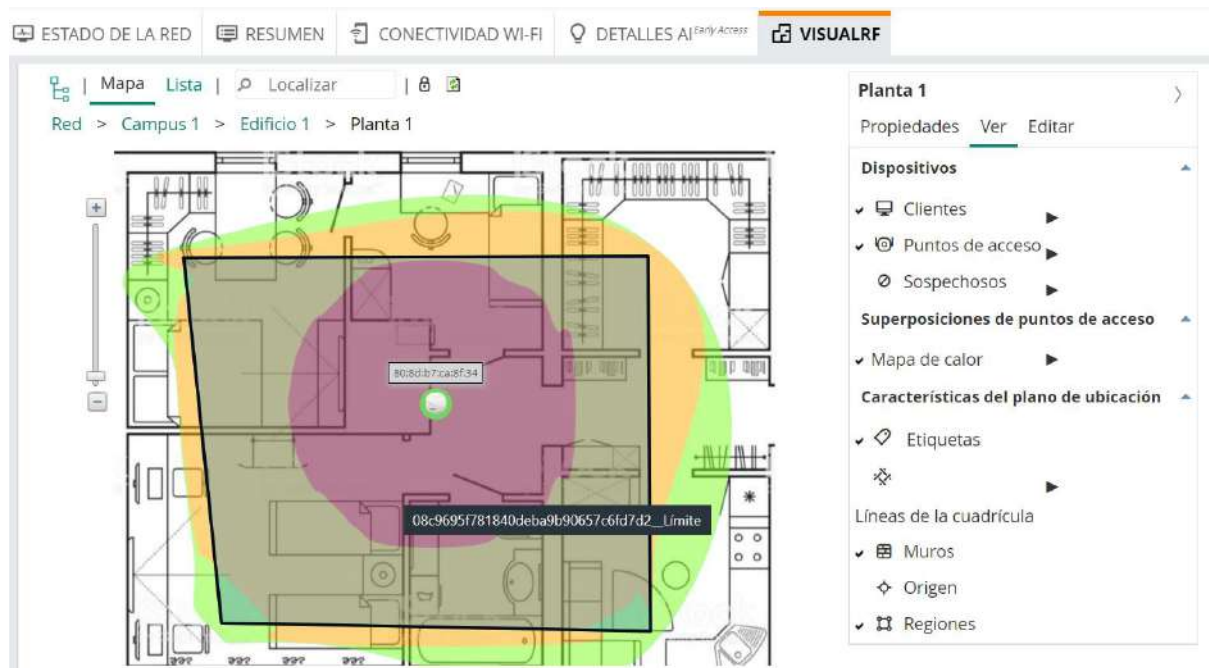
24- Dar click en Añadir puntos de accesos instalados.

25- Arrastrar el siguiente icono  el cual sería nuestro Ap, al plano de lado derecho.

26- Click en Finalizar.



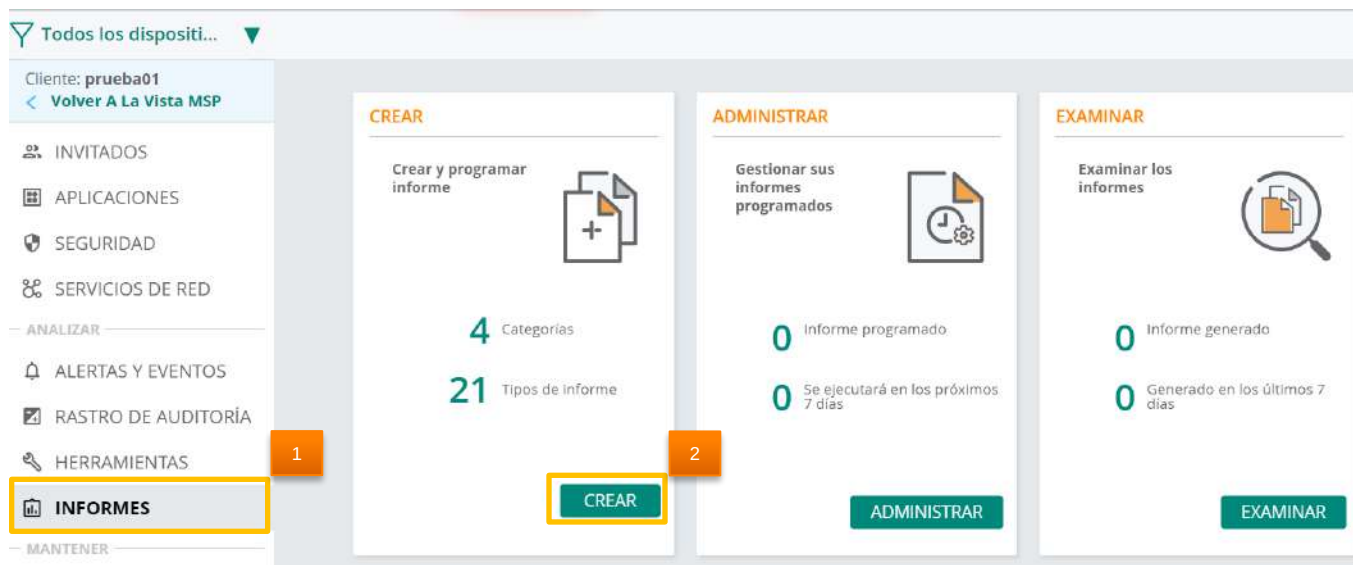
Al finalizar nos muestra el mapa de calor configurado en Aruba de los radios 2.4 y 5.



SIGNOS VITALES WIFI

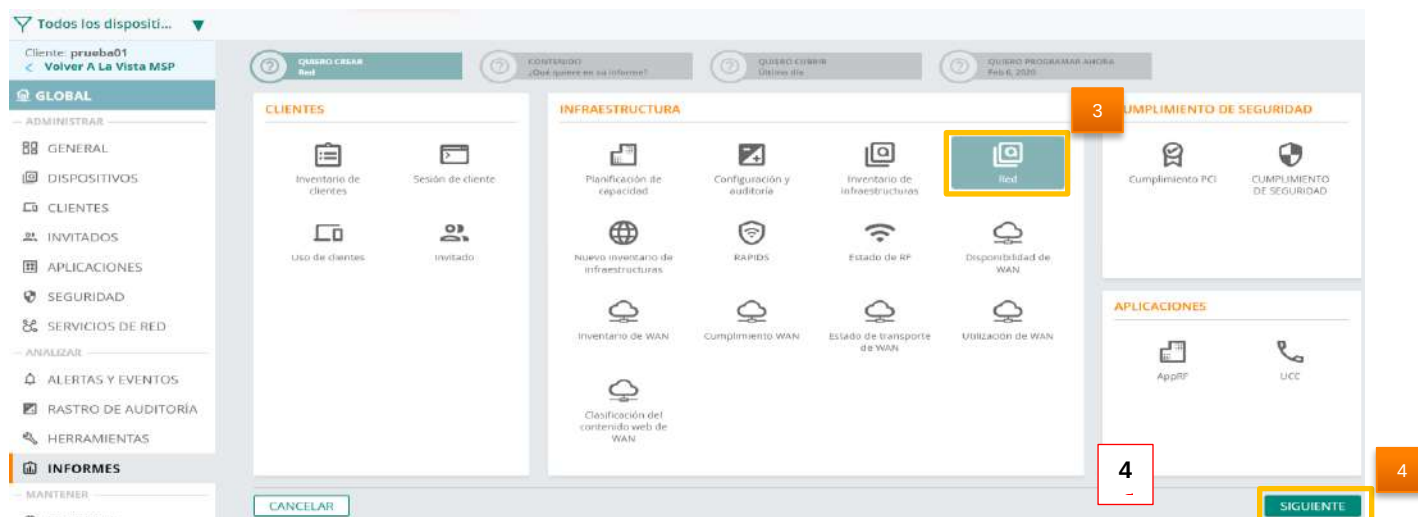
Revisa la información de los reportes preestablecidos desde el portal para conocer el estado de salud de tu red inalámbrica.

- 1- Desde la opción de INFORMES
- 2- nos vamos al botón CREAR



En Tipo de Informes nos aparecerán varias opciones a seleccionar CLIENTES, INFRAESTRUCTURA, CUMPLIMIENTO DE SEGURIDAD Y APLICACIONES

3. Para el ejemplo vamos a seleccionar **RED**
4. Daremos un click en **SIGUIENTE**



Los tipos de informes que se pueden seleccionar son:

- **CLIENTES**
 - Inventario de clientes- reporte sobre detalle de los clientes conectados
 - Sesión de cliente- reporte sobre detalle de las sesiones de cliente
 - Uso de clientes- reporte del detalle de utilización de clientes
 - Invitado
- **INFRAESTRUCTURA**
 - Planificación de capacidad- reporte sobre rendimiento y densidad de usuarios
 - Configuración y auditoría
 - Inventario de infraestructura- reporte sobre las antenas y licencias
 - Red- reporte general de las redes inalámbricas (SSIDs, clientes, APs, etc.)
 - Nuevo Inventario de infraestructura- reporte sobre antenas y licencias agregadas a la herramienta de gestión
 - Rapids
 - Estado de RF
 - Disponibilidad de VLAN
 - Inventarios de WAN
 - Estado de transporte WAN
 - Utilización de WAN
 - Clasificación del contenido WEB de WAN
- **CUMPLIMIENTO DE SEGURIDAD**
 - Cumplimiento PCI- reporte sobre cumplimiento PCI
 - Cumplimiento de Seguridad
- **APLICACIONES**
 - AppRF
 - UCC
 - Reporte sobre utilización de categorías de aplicaciones
 - Estado de Auditoría de Configuración
 - Inventario de infraestructura- reporte sobre las antenas y licencias
 - Seguridad- reporte sobre intrusiones y antenas no autorizadas detectadas
 - Unified Communications-

5. Crear informe a partir de: **Grupos**
6. Grupo de dispositivos: Lo asignaremos al grupo **DEFAULT**
7. Le damos un click en **SIGUIENTE**

8. Periodo: Tendremos 4 opciones último día, Última semana, Último mes y Rango personalizado. Para el ejemplo vamos a seleccionar **Último día**
9. Damos un click en **SIGUIENTE**

10. Para el ejemplo vamos a seleccionar Una vez (ahora)
11. colocamos el nombre a nuestro informe
12. una dirección de correo
13. el formato para nuestro documento
14. damos en **GENERAR**

▼ Todos los dispositi... ▼

Cliente: prueba01
[Volver A La Vista MSP](#)

GLOBAL

— ADMINISTRAR —

- GENERAL
- DISPOSITIVOS
- CLIENTES
- INVITADOS
- APLICACIONES
- SEGURIDAD
- SERVICIOS DE RED

— ANALIZAR —

- ALERTAS Y EVENTOS
- RASTRO DE AUDITORÍA

QUIERO CREAR *Applet*

QUIERO VER CONTEXTO: GRUPOS

QUIERO CURSAR Último día

QUIERO PROGRAMAR AHORA Feb 8, 2020

PERIODICIDAD 10

☒ Una vez (ahora)

☐ Una vez (más tarde)

☐ Cada día

☐ Cada semana

☐ Cada mes

INFORMACIÓN DEL INFORME

Título del informe: Prueba-Informes 11

Correo electrónico a: csilvahe@gmail.com 12

FORMATO DE CORREO ELECTRÓNICO ☒ PDF ☐ CSV 13

CANCELAR

ATRÁS

GENERAR 14