



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

CARRERA DE REDES Y COMUNICACIÓN DE DATOS

**TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO
DE INGENIERÍA EN REDES Y COMUNICACIÓN DE DATOS**

**TEMA: “ANÁLISIS DE DESEMPEÑO Y COBERTURA DE LA NUEVA
RED INALÁMBRICA DE LA UNIVERSIDAD DE LAS FUERZAS
ARMADAS ESPE - CAMPUS SANGOLQUÍ PROVISTA POR UN
PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES”**

AUTOR: YÁNEZ VERA, JORGE DAVID

DIRECTOR: ING. VEGA MUÑOZ, CHRISTIAN NÉSTOR

SANGOLQUÍ

2019



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES

CARRERA DE DE REDES Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "ANÁLISIS DE DESEMPEÑO Y COBERTURA DE LA NUEVA RED INALÁMBRICA DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE - CAMPUS SANGOLQUÍ PROVISTA POR UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES" fue realizado por el señor Yánez Vera, Jorge David el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 11 de abril de 2019

Firma:

Ing. Christian Vega Muñoz.

C. C. 1709328353



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

CARRERA DE DE REDES Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

Yo, Yáñez Vera, Jorge David declaro que el contenido, ideas y criterios del trabajo de titulación: **ANÁLISIS DE DESEMPEÑO Y COBERTURA DE LA NUEVA RED INALÁMBRICA DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE - CAMPUS SANGOLQUÍ PROVISTA POR UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 11 de abril de 2019

Firma:

Jorge David Yáñez Vera.

C. C. 1721408118



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y
TELECOMUNICACIONES**

CARRERA DE DE REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, Yánez Vera, Jorge David autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **ANÁLISIS DE DESEMPEÑO Y COBERTURA DE LA NUEVA RED INALÁMBRICA DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE - CAMPUS SANGOLQUÍ PROVISTA POR UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 11 de abril de 2019

Firma:

Jorge David Yánez Vera.

C. C. 1721408118

DEDICATORIA

Los logros más importantes de mi vida han sido y son gracias a las personas que me dieron aliento para seguir adelante. Dedico el presente, a mis padres Jorge y Catalina, a mi hermana Lorena y a mi esposo Carlos.

AGRADECIMIENTO

A Carlos, que, con perseverancia y tiempo me ayudó a alcanzar este escalón.

A todos los profesores de mi carrera en la Universidad de las Fuerzas Armadas - ESPE por brindarme sus conocimientos, en particular al Ing. Christian Vega y al Dr. Nikolai Espinosa, por su aporte y seguimiento durante el desarrollo de mi tesis.

A Edwin Vera y José Moromenacho por haber confiado en mí.

De manera especial a mis abuelos Anita, Blanquita, Etelvina y Efraín, por las palabras de constancia que hasta el día de hoy me empujan para seguir adelante y cumplir mis propósitos.

A mis compañeras y amigas Tania, Andrea, Diana y Anabel por interminables jornadas de estudio compartidas.

A Century Link Ecuador S. A. e Integraldata S. A., empresas que me ha ofrecido toda la ayuda necesaria para el desarrollo de mi tesis.

ÍNDICE DE CONTENIDOS

DEDICATORIA	iv
AGRADECIMIENTO	v
ÍNDICE DE CONTENIDOS.....	vi
RESUMEN.....	xii
ABSTRACT	xiii
INTRODUCCIÓN.....	1
1. Capítulo I: Redes inalámbricas	3
1.1. Tipos de redes inalámbricas	3
1.1.1. Redes Punto a Punto	3
1.1.2. Redes Punto a Multipunto	4
1.1.3. Redes Multipunto a Multipunto.....	4
1.2. Elementos de una red inalámbrica 802.11	6
1.2.1. Antenas	6
1.2.2. Dispositivos	7
1.2.3. Identificador de red inalámbrica	9
1.3. Estándar IEEE 802.11	9
1.3.1. Estándar IEEE 802.11a.....	11
1.3.2. Estándar IEEE 802.11b.....	12
1.3.3. Estándar IEEE 802.11g.....	12
1.3.4. Estándar IEEE 802.11n.....	13
1.3.5. Estándar IEEE 802.11ac.....	14
1.4. Técnicas de modulación en 802.11	17
1.4.1. Espectro Ensanchado por Secuencia Directa	17
1.4.2. Espectro Ensanchando por Salto de Frecuencia	17
1.5. Movilidad e itinerancia en 802.11	18
1.6. Escaneo de redes.....	18
1.7. Seguridad	18
2. Capítulo II: Descripción general de la WLAN.....	22

2.1.	Equipamiento	22
2.1.1.	Controladora	22
2.1.2.	Puntos de acceso para interiores	23
2.1.3.	Puntos de acceso para exteriores	27
2.2.	Tiempo de servicio	28
2.3.	Características generales	29
2.4.	Gestión de red	29
2.5.	Expansibilidad	30
2.6.	Conectividad	31
2.7.	Propagación de SSID	31
2.8.	Solapamiento	32
2.9.	Estándares soportados	32
2.10.	Movilidad	33
2.11.	Seguridad	33
2.12.	Monitoreo	34
2.13.	Diagnóstico y alertas	34
2.14.	Soporte técnico	35
2.15.	Administración y configuración	35
2.16.	Roles de usuarios de la plataforma	36
2.17.	Localización	36
2.18.	Reportes	36
2.19.	Otros	36
3.	Capítulo III: Medición de la WLAN	38
3.1.	Descripción del escenario de pruebas	38
3.2.	Descarga y configuración de aplicaciones para móviles y portátiles	38
3.3.	Ejecución del ambiente de pruebas	40
3.4.	Registro en la red inalámbrica con SSID ESPE	43
3.5.	Toma de muestras	48
4.	Capítulo IV: Tabulación de muestras (resultados)	59
4.1.	Representación gráfica de resultados (mapa)	65
4.2.	Muestras complementarias	74
4.3.	Encuesta de uso de servicios de la red inalámbrica	82
5.	Capítulo V: Conclusiones y recomendaciones	99

5.1. Conclusiones	99
5.2. Recomendaciones	100
BIBLIOGRAFÍA.....	102

ÍNDICE DE TABLAS

Tabla 1. <i>Áreas de estudio IEEE 802.X</i>	10
Tabla 2. <i>Subdivisión del estándar 802.11</i>	11
Tabla 3. <i>Nivel de señal</i>	29
Tabla 4. <i>Requerimientos mínimos para VMWare</i>	30
Tabla 5. <i>Tabulación de datos</i>	60
Tabla 6. <i>Resumen de puntos aledaños</i>	63
Tabla 7. <i>Representación gráfica de puntos</i>	65
Tabla 8. <i>Clientes por SSID y por estándar</i>	82
Tabla 9. <i>División de población entrevistada</i>	83

ÍNDICE DE FIGURAS

Figura 1. Red inalámbrica punto a punto.....	3
Figura 2. Red inalámbrica punto a multipunto.	4
Figura 3. Red inalámbrica multipunto a multipunto.....	5
Figura 4. Antena omnidireccional versus antena direccional.....	6
Figura 5. Propagación omnidireccional vs beamforming.....	15
Figura 6. MU-MIMO con varios clientes.....	16
Figura 7. Logo de certificación de WiFi Alliance.....	20
Figura 8. Cisco 5520 Wireless Controller.....	23
Figura 9. Punto de acceso para interior Cisco Aironet serie 2800.....	23
Figura 10. Modelo de propagación punto de acceso interiores.....	26
Figura 11. Punto de acceso para exterior Cisco Aironet serie 1560.....	27
Figura 12. Switch LAN dedicado para red inalámbrica.....	37
Figura 13. Network Analyzer en AppStore.....	39
Figura 14. Speedtest en AppStore.....	39
Figura 15. NetSpot para MacOS.....	40
Figura 16. WiFi Analyzer en Play Store.....	40
Figura 17. Dispositivo portátil.....	41
Figura 18. Selección de WLAN mediante SSID.....	43
Figura 19. Portal cautivo WLAN ESPE.....	44
Figura 20. Página de bienvenida.....	45
Figura 21. Estado de conexión inalámbrica.....	46
Figura 22. Advertencia de certificado.....	47
Figura 23. Advertencia máximo de dispositivos.....	48
Figura 24. Nivel de señal de ESPE.....	50
Figura 25. Desempeño de canales de ESPE.....	50
Figura 26. Escaneo de redes en 2.4GHz.....	51
Figura 27. Escaneo de redes en 5GHz.....	51
Figura 28. Escaneo de redes en 5GHz.....	52
Figura 29. Escaneo de redes con Netspot.....	52
Figura 30. Archivo prueba descarga.....	53
Figura 31. Prueba velocidad.....	54
Figura 32. Prueba de streaming en vivo.....	55
Figura 33. Punto de acceso interior.....	56
Figura 34. Punto de red para punto de acceso interior.....	56
Figura 35. Punto de acceso exterior.....	58
Figura 36. Armario y fuente de poder.....	58
Figura 37. Construcción de mapa de calor - Capa Idóneo.....	66
Figura 38. Construcción de mapa de calor - Capa Bueno.....	66
Figura 39. Construcción de mapa de calor - Capa Bajo.....	67
Figura 40. Construcción de mapa de calor - Capa Sin Señal.....	67
Figura 41. Construcción de mapa de calor - Todas las capas.....	68
Figura 42. Resultado sobre un mapa 3D sobre Google Earth.....	69
Figura 43. Resultado capa Idóneo sobre Google Earth.....	70

Figura 44. Resultado capa Bueno sobre Google Earth	71
Figura 45. Resultado capa Bajo sobre Google Earth.....	72
Figura 46. Resultado capa Sin Señal sobre Google Earth.....	73
Figura 47. Resultado todas las capas sobre Google Earth - CAFDER.....	74
Figura 48. Plano base sector canchas.....	75
Figura 49. Mapa de calor con Ekahau - canchas.....	75
Figura 50. Mapa de calor con NetSpot - canchas.....	76
Figura 51. Plano base edificio Central PB	77
Figura 52. Mapa de calor con Ekahau - bloque A.....	78
Figura 53. Mapa de calor con Ekahau - bloque B.....	78
Figura 54. Mapa de calor con Ekahau - UTIC.....	79
Figura 55. Mapa de calor con Netspot bloques A y B.....	80
Figura 56. Plano base bloques G y H P2.....	80
Figura 57. Mapa de calor con Netspot bloques G y H	81
Figura 58. Código QR encuesta	84
Figura 59. Resultados pregunta 1 de encuesta	85
Figura 60. Resultados pregunta 2 de encuesta	86
Figura 61. Combinación redes de invitados.....	87
Figura 62. Resultados pregunta 3 de encuesta	88
Figura 63. Filtrado por usuarios de ESPE.....	89
Figura 64. Resultados pregunta 4 de encuesta	90
Figura 65. Resultados pregunta 5 de encuesta	91
Figura 66. Resultados pregunta 6 de encuesta	92
Figura 67. Resultados pregunta 7 de encuesta	93
Figura 68. Resultados pregunta 8 de encuesta	94
Figura 69. Resultados pregunta 9 de encuesta	95
Figura 70. Pregunta 9 filtrado por profesores	96
Figura 71. Pregunta 10 filtrado por estudiantes	96
Figura 72. Resultados pregunta 10 de encuesta	97

RESUMEN

Con el desarrollo de este proyecto de investigación se busca evaluar la experiencia del usuario sobre los servicios de conectividad de la nueva red inalámbrica de la Universidad de las Fuerzas Armadas - ESPE, campus matriz, realizando mediciones en cuanto al desempeño y cobertura de la nueva solución implementada, con la utilización de herramientas de hardware y software que se encuentren al alcance de los diferentes grupos de usuarios del campus y con el fin de poder identificar las ventajas pero también las falencias de la misma, en base a los requerimientos de un contrato de prestación de servicios. Las pruebas se realizan mediante la toma de muestras en puntos de sectores estratégicos destinados al desarrollo de actividades académicas, con la ayuda de software sobre varias plataformas: Android, iOS, Windows, MacOS, como, por ejemplo, WiFi Analyzer, NetSpot y las herramientas de gestión y monitoreo propias de Cisco. Estas son aplicaciones especializadas para escanear, estudiar y analizar el espectro en zonas definidas del campus, con el fin de obtener datos de la nueva red en cuanto a su rendimiento, y en un futuro poder brindar mejoras que reflejen una mejor apreciación por parte de los usuarios. Los nombres de las empresas públicas y privadas han sido omitidos, cumpliendo con el compromiso de confidencialidad.

PALABRAS CLAVE:

- **Red inalámbrica**
- **WIFI**
- **Proveedor de servicios**

ABSTRACT

The target of the development of this research project is to evaluate the user experience on connectivity services of the Universidad de las Fuerzas Armadas – ESPE headquarters' new wireless network, performing measurements regarding the performance and coverage of the new solution implemented, with the use of hardware and software tools that are available to different groups of users present on campus and in order to identify the advantages but also the shortcomings of it, based on the requirements of a service contract. The tests are made by taking samples at strategic points related to development of academic activities, using software on different platforms: Android, iOS, Windows, MacOS, such as WiFi Analyzer, NetSpot and Cisco management and monitoring tools. These are specialized applications to scan, study and analyze the spectrum in defined areas of the campus, in order to obtain data from the new network regarding its performance, and in the future can provide improvements that reflect a better appreciation by the users. The names of public and private companies have been omitted, fulfilling the commitment of confidentiality.

KEYWORDS:

- **WLAN**
- **WIFI**
- **Service provider**

INTRODUCCIÓN

En la actualidad, la explotación del espectro electromagnético es una herramienta muy utilizada para el despliegue de comunicaciones inalámbricas, que prometen entregar servicios de calidad, a los usuarios, compitiendo con las que aun utilizan cables, en cuanto a costos, limpieza, estética, movilidad, seguridad, alcance, accesibilidad.

Es por esto, por lo que el desarrollo de tecnologías inalámbricas ha tenido un importante aporte en los últimos años, permitiendo que la misma, sea accesible para diferentes tipos de usuarios, como por ejemplo en el sector doméstico, industrial, empresarial, gobierno, académico, entre otros.

Dentro de las instituciones educativas, contar una red inalámbrica, que permita a los usuarios acceder a servicios de navegación y consulta, acceso a servicios ofertados dentro de la misma LAN (Local Area Network) como servidores, servicios en la nube y otros, es de suma importancia, dándole a la educación un valor agregado al contar con todos los beneficios mencionados anteriormente, sobre una red inalámbrica.

Es por esto, que la Universidad de las Fuerzas Armadas – ESPE, por medio de su Unidad de Tecnologías de la Información y Comunicaciones, en la búsqueda de cumplir su objetivo en cuanto a servicios de red, ha actualizado su red inalámbrica, por medio de un proveedor de servicios de telecomunicaciones, buscando permitir el acceso a la comunicación inalámbrica a los diferentes tipos de usuarios dentro de sus sedes educativas.

Con la aplicación de este proyecto, se busca medir la red inalámbrica del campus Sangolquí, por medio de la evaluación de la experiencia del usuario, con la ayuda de diferentes aplicaciones que corran sobre dispositivos móviles y portátiles.

Adicionalmente se podrá contrastar ciertos datos proporcionados por el proveedor de servicios, según los documentos de contratación de servicios.

1. Capítulo I: Redes inalámbricas

1.1. Tipos de redes inalámbricas

1.1.1. Redes Punto a Punto

Se refiere a una conexión *uno a uno* y se las utiliza para enlazar dos nodos o estaciones diferentes de una misma o de diferentes organizaciones, y puede tener varios usos, basado en transmisión y recepción de datos.

Al otro lado del nodo remoto, en el nodo principal, se contará con equipamiento de acceso a la intranet o a Internet, permitiendo el acceso a la información.

El contenido que se transmite es indiferente, pues el mismo puede sostener una gran cantidad de datos como audio y video, sin ningún inconveniente, y el enlace puede alcanzar suficiente distancia como para, por ejemplo, cubrir un campo de deportes o un área de comedor, dependiendo de las características propias del enlace.



Figura 1. Red inalámbrica punto a punto

Fuente: (Netkrom Group, s/a)

1.1.2. Redes Punto a Multipunto

Se refiere a una conexión *varios a uno* y se las utiliza para permitir varias conexiones hacia un concentrador.

También se las utiliza en la transmisión de datos, que puede tener acceso a Internet, y que al mismo tiempo permita compartir recursos e información entre dispositivos (que no tengan una conexión *ad hoc*) de una misma red. Sin embargo, dependiendo de su implementación y despliegue, la misma puede causar conflictos, por lo que conlleva un grado más alto de complejidad.



Figura 2. Red inalámbrica punto a multipunto.

Fuente: (Netkrom Group, s/a)

1.1.3. Redes Multipunto a Multipunto

También conocidos como *Ad Hoc*, *Mesh* o malla, son redes que permiten la comunicación entre varios nodos o dispositivos, sin contar con un nodo central o concentrador.

Además, este tipo de configuración permite escalabilidad al aumentar los dispositivos o nodos, auto reparación en inconvenientes de enrutamiento, compartir recursos al tener una salida a Internet, entre otras.

Por otro lado, también presenta desventajas como complejidad, disminución de rendimiento, intrusiones de seguridad, soporte complejo en cuanto al uso del espectro y alta carga en la administración de la red.

Los diferentes tipos de redes pueden utilizarse dentro de una misma organización de forma convergente para proveer acceso a los usuarios, teniendo en cuenta que, a mayor número de dispositivos y configuraciones, se eleva el grado de complejidad del manejo de la red.



Figura 3. Red inalámbrica multipunto a multipunto

Fuente: (Netkrom Group, s/a)

1.2. Elementos de una red inalámbrica 802.11

Dentro de los principales elementos podemos citar:

1.2.1. Antenas

Se pueden clasificar en dos categorías:

Omnidireccional: Son de fácil uso ya que no requieren de alineamiento, y se utilizan en la mayoría de los puntos de acceso y tarjetas de red inalámbricas. Ideal para entornos interiores, con alcances de hasta 45 metros. Como desventaja se tiene que no alcanzan una distancia considerable, a menos que se utilicen amplificadores. En muchos de los casos, su uso puede ser considerado como ilegal.

Punto a punto: También conocidas como direccionales. Requieren alineamiento y son utilizadas en exteriores. El alcance depende de regulaciones locales o de la línea de vista.

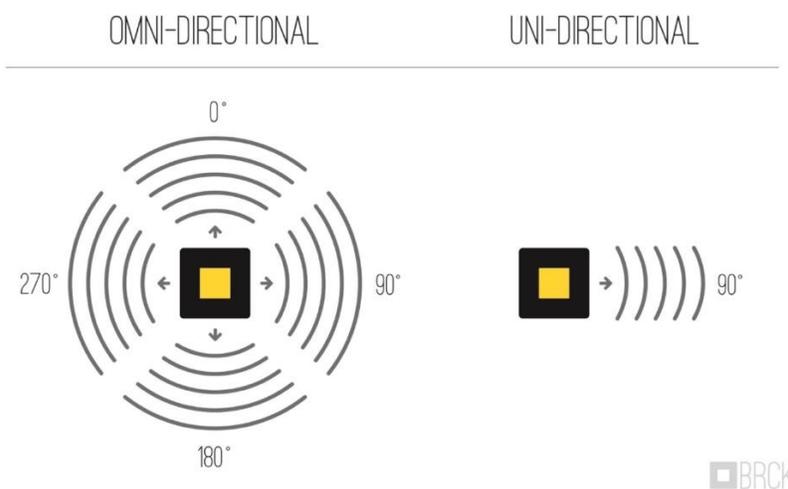


Figura 4. Antena omnidireccional versus antena direccional

Fuente: (Hersman, 2014)

1.2.2. Dispositivos

Dentro del estándar 802.11 se puede clasificar a los dispositivos en 2 grandes grupos: puntos de acceso y clientes.

Punto de acceso

Dispositivo transmisor/receptor que funge como concentrador de una red o puerta de acceso entre una red inalámbrica y una red cableada. También conocido como estación base.

Punto de acceso inteligente o maestro

Se refiere a un dispositivo capaz de controlar sus capacidades y tener una inteligencia propia. Es el modo de funcionamiento más común en ambientes domiciliarios y oficinas pequeñas, permitiendo que los dispositivos inalámbricos puedan conectarse a Internet o Intranet. En ambientes empresariales más grandes, aún pueden permitir la conectividad entre dispositivos o con otros puntos de acceso, en ocasiones donde la controladora sufra algún tipo de fallo.

Punto de acceso tonto o repetidor

Se refiere a un modo de funcionamiento en el que, el dispositivo básicamente extiende la señal de un punto de acceso maestro, por lo que siempre dependerá de un dispositivo inteligente. En caso de fallos del punto de acceso maestro o de la controladora, el dispositivo no tendrá ninguna funcionalidad, a más de continuar irradiando el o los SSID, sin permitir ningún tipo de conectividad.

Punto de acceso en modo bridge

Tal como refiere su nombre, este tipo de punto de acceso permitirá la comunicación exclusiva entre dos puntos de acceso, en situaciones en las que instalar una interconexión cableada, resulte poco factible.

Clientes

Dispositivos en hardware, software o firmware, que dependen de los servicios que pueda prestar un punto de acceso: asociación, distribución, integración, etc. Generalmente constituyen la interface humano y máquina, realizando las peticiones hacia servidores proveedores de servicios, y recibiendo las respuestas procesadas del mismo.

Los puntos de acceso pueden actuar como clientes, pero los clientes no pueden actuar como puntos de acceso, en una configuración de infraestructura.

Controladora

Una Wireless Lan Controller (WLC) o controladora, es un dispositivo que tiene como principal función configurar los puntos de acceso y contar con gestión y monitoreo de una red inalámbrica. Maneja aspectos como la gestión de los dispositivos que componen la solución, identificando problemas, configurando los puntos de acceso en grupo evitando configurar individualmente, enviando actualizaciones de firmware, como funciones hacia los puntos de acceso, pero también maneja tráfico de la red inalámbrica, logrando monitorizar, priorizar, filtrar y limitar el mismo. Esta segunda opción no siempre está activa, pudiendo un tercer dispositivo componente de la red interna, cumplir con esas funciones.

Actualmente se tienen dos modos de implementación, uno es con un equipo físico o hardware que se incluye en la red interna con los demás dispositivos, y otro es trabajar con una controladora en la nube. Para este segundo caso, el tráfico que manejará será solo el que implica gestión de los puntos de acceso, evitando saturación con tráfico de clientes que tendrá que ser manejado por la red interna y sus dispositivos.

Adicionalmente a los dispositivos anteriormente mencionados, podemos encontrar elementos pertenecientes propios de la red LAN o WAN como enrutadores (router), concentradores (switch, hub, bridge), cortafuegos (firewall), entre otros.

1.2.3. Identificador de red inalámbrica

Cada red inalámbrica debe de contar con un nombre específico que lo diferenciará de las demás redes. El Service Set Identifier SSID, es un nombre que puede ser de hasta 32 caracteres, sin limitaciones, pues el estándar no define si puede incluirse caracteres especiales ni caracteres numéricos.

El SSID es propagado por los puntos de acceso y es compartido por los clientes de la red.

1.3. Estándar IEEE 802.11

Desde su publicación en 1997 por el Institute of Electrical and Electronics Engineers (IEEE), el estándar ha tenido varias modificaciones que resultan en mejoras en el desempeño de las redes inalámbricas de área local, ya que se ha necesitado perfeccionar el desenvolvimiento de este para aplicarlo en el estudio y comportamiento de redes.

Se partió con un estándar que permitió conexiones con un ancho de banda de 2 Mbps en modulación DSSS o hasta 1 Mbps en malas condiciones con modulación FHSS. Ambos en banda no licenciada de 2.4 GHz. Adicionalmente entabló definiciones sobre el medio infrarrojo, a pesar de su limitada utilidad. (Danielyan, s/a)

Los estándares inalámbricos regulan que los diferentes dispositivos utilizados en el despliegue de redes inalámbricas compartan la misma base, con lo cual se puede asegurar que los mismos pueden interactuar entre sí para que exista una correcta interoperabilidad y usabilidad tanto en redes locales como en redes de área metropolitana.

Dependiendo del área de estudio, el estándar se divide en:

Tabla 1.
Áreas de estudio IEEE 802.X

Nombre	Descripción
IEEE 802.1	Puentes y Gestión de Redes
IEEE 802.3	Ethernet
IEEE 802.11	Redes Inalámbricas de Área Local (WLAN)
IEEE 802.15	Redes Inalámbricas de Área Personal (PAN)
IEEE 802.15.1	Bluetooth
IEEE 802.15.2	Coexistencia IEEE 802.15 y IEEE 802.11
IEEE 802.15.3	Redes Inalámbricas de Área Personal (WPAN) y Alta Velocidad
IEEE 802.15.4	Redes Inalámbricas de Área Personal y Baja Velocidad (Por ej. Zigbee)
IEEE 802.15.5	Redes en Malla para WPAN
IEEE 802.15.6	Redes de Área Corporal (BAN)
IEEE 802.16	Acceso Inalámbrico de Banda ancha (base de WiMAX)
IEEE 802.16.1	Servicio de Distribución Local Multipunto (LMDS)
IEEE 802.18	Regulaciones de Radio
IEEE 802.19	Coexistencia
IEEE 802.20	Acceso Inalámbrico Móvil de Banda Ancha
IEEE 802.21	Traspaso (<i>handoff</i>) Independiente del Medio
IEEE 802.22	Redes Inalámbricas de Área Regional
IEEE 802.23	Servicios de Emergencia
IEEE 802.24	Malla Inteligente (<i>Smart Grid</i>)
IEEE 802.25	Red de Área Omni-Range

Fuente: (Butler, 2014)

Desde esta organización, el estándar para el estudio de las redes inalámbricas de área local se subdivide en:

Tabla 2.
Subdivisión del estándar 802.11

Protocolo 802.11	Aprobado	Frecuencia [GHz]	Ancho de banda [MHz]	Tasa de datos por flujo [Mbps]	Alcance aprox. en interiores [m]	Alcance aprox. en exteriores [m]
	Jun-1997	2.4	20	1, 2	20	100
a	Sep-1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	35	120
b	Sep-1999	2.4	20	1, 2, 5.5, 11	35	140
g	Jun-2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	38	140
n	Oct-2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150	70	250
ac	Nov-2011	5	40	Hasta 200		
			80	Hasta 433.3		
			160	Hasta 866.7		
			160 (2x2)	Hasta 1730		

Fuente: (Butler, 2014) (Intel, 2018)

1.3.1. Estándar IEEE 802.11a

Estándar que comprende funcionamiento en banda no licenciada de 5 GHz, sobre OFDM, con anchos de banda de 6 Mbps a 54 Mbps, descritos en la tabla anterior. Para su implementación es requerido como necesario, que cumpla con tasas de 6 Mbps, 12 Mbps y 24 Mbps. Como desventaja se tiene que, por las altas capacidades de ancho de banda, el rango de alcance es bajo. Adicionalmente, debido a características propias de

protocolo como corrección de errores e interferencias y el encabezado del protocolo, el ancho de banda real puede ser menor que el nominal. También se considera el estado de la infraestructura de la red, que, al ser de baja calidad, puede necesitar de correcciones posteriores a la instalación ocasionando costos más altos debido al rango de operación ya que se necesitan mayor cantidad de puntos de acceso.

1.3.2. Estándar IEEE 802.11b

Estándar muy utilizado. Comprende funcionamiento en la banda no licenciada de 2.4 GHz y modulación DSSS, con anchos de banda desde 1 Mbps hasta 11 Mbps, descritos en la tabla anterior, y entre 11 y 14 canales disponibles en radio para su propagación. Es muy probable que si un dispositivo no especifique el tipo de estándar 802.11 que está utilizando, esté trabajando con 802.11b ya que al ser el más común no es necesario especificarlo como característica del producto.

Se asegura que se entregará la máxima velocidad disponible, pero la misma depende de la ubicación del punto de acceso y de las interferencias de radio, que pueden hacer variar la velocidad para asegurar la conectividad.

Ambos estándares descritos anteriormente, utilizan protocolo de control de acceso al medio (MAC) y acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA), lo que las hace idóneas para convivir en un mismo entorno para 1 y 2 Mbps, y para 5.5 y 11 Mbps, ya que cualquier cambio es realizado en la capa física, sin afectar cualquier transición entre ellos.

1.3.3. Estándar IEEE 802.11g

Fue publicado en junio de 2003 como avance de 802.11b. Soporta hasta 54Mbps, superando por mucho a los 11Mbps de su antecesor, aunque en la práctica, como los

demás estándares no alcanzará la velocidad teórica, estimando que la tasa de transferencia de datos está entre 14 Mbps y 31 Mbps, permitiendo que los usuarios trabajen sobre video o juegos en línea son presentar inconvenientes.

Este protocolo funciona sobre Multiplexación por División de Frecuencia Ortogonal (OFDM), lo que le permite alcanzar mayores velocidades que sus antecesores, sobre una frecuencia de 2.4GHz para entregar un mayor alcance. Esto lo define como un estándar con cualidades tanto de 802.11a como de 802.11b.

Se tienen disponibles 14 canales, dependiendo de la regulación de la zona geográfica o de cada país, entre 2.412GHz y 2.484GHz, permitiendo que los dispositivos dentro de ese rango puedan conectarse al punto de acceso, inclusive si mantienen una versión diferente del estándar.

Su principal desventaja, como la mayoría de las variaciones, se tiene en la saturación del dispositivo en caso de conectar varios dispositivos al mismo tiempo. A pesar de este inconveniente, aún es posible encontrar puntos de acceso con esta variante, debido a que son muy económicos. (Bradley, Internet & Network, 2018)

1.3.4. Estándar IEEE 802.11n

Lanzado en 2009, esta variación del estándar, como sus predecesoras, fue concebida como reemplazo a las versiones anteriores, provisionando mejoras significativas. En este punto, con tantas variables, se solicitó que las especificaciones impresas en los empaques de los puntos de acceso muestren los estándares con los que el dispositivo puede trabajar.

Esta variación introdujo el término Multiple In – Multiple Out (MIMO), que permite la convivencia de hasta cuatro señales de radio emitidas por una misma antena, logrando

incrementar las capacidades de la red inalámbrica en cuanto a alcance, rendimiento, y consiguiendo un mayor ancho de banda del canal de la frecuencia por el que transmite. Todo resume a un mayor rendimiento de la tasa de transferencia de datos, que, teóricamente soporta hasta 300Mbps, dependiendo de las características de la antena que utilice el radio del dispositivo que son de 2.4GHz y 5GHz. (Bradley, Internet & Network, 2019)

1.3.5. Estándar IEEE 802.11ac

Fue desarrollado entre 2011 y 2013, como el estándar mejorado de 802.11n, siendo la quinta versión de WiFi, buscando mejorar las capacidades de una WLAN por medio de avances sobre el firmware y hardware de los dispositivos.

Debido al avance de la tecnología y a la necesidad de satisfacer a un mercado que cada vez apunta a un consumo mayor de video en alta definición, servicios de streaming y voz sobre internet, esta versión fue diseñada con el fin de funcionar a la par de una conexión Gigabit Ethernet. De hecho, la velocidad teórica es de 1Gbps, lo cual se alcanza gracias a varios aspectos como: mayor cantidad de antenas MIMO para permitir un mayor flujo de conexiones simultáneas al mismo radio, y canales que utilizan un espacio más ancho en la frecuencia de entre 80MHz hasta 160MHz, que para esta versión es de 5GHz, ya que permite evadir interferencias dentro de 2.4GHz, considerando que la mayoría de dispositivos han sido diseñados para esta frecuencia; y adicionalmente por el hecho de permitir un mayor espacio para los canales, como se lo mencionó anteriormente. Pero, para guardar compatibilidad con estos dispositivos que trabajan en 2.4GHz, 802.11ac también incluye soporte simulando un 802.11n.

Adicionalmente, como uno de los nuevos avances desarrollados, para esta versión se implementó la función de beamforming, la cual consiste en permitir re direccionar la propagación de la señal de radio, en una dirección en específico hacia el receptor y evitando propagarla 180° o 360° (propagación omnidireccional); esto, con la finalidad de asegurar las conexiones inalámbricas, sobre todo en ambientes saturados.

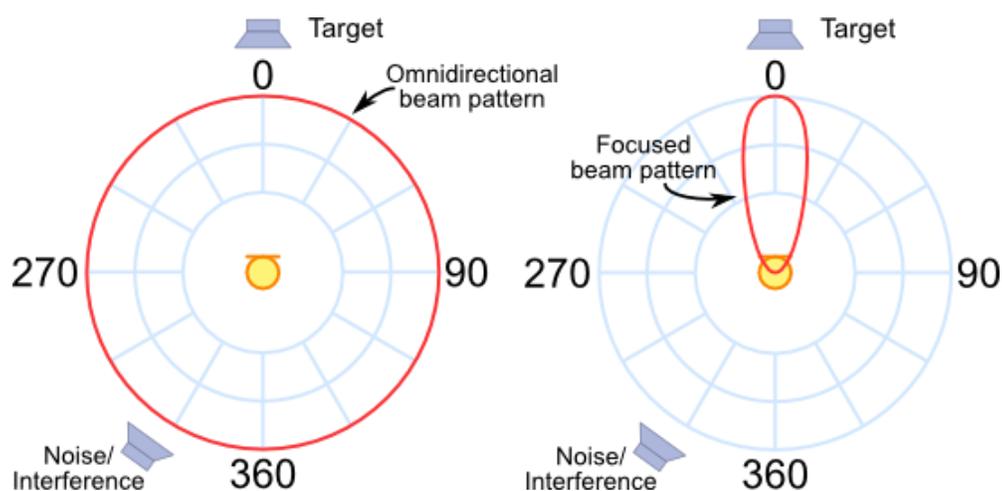


Figura 5. Propagación omnidireccional vs beamforming

Fuente: (Andrew, 2012)

Uno de los problemas que enfrenta el despliegue de esta versión, es la compatibilidad, pues la mayoría de los dispositivos aun funcionan en una versión anterior de estándar en hardware, lo que no permite el acoplamiento con solo realizar una actualización del firmware.

Estándar IEEE 802.11ac Wave1

Se trata de la versión ya aprobada por el IEEE y lo que la mayoría de los dispositivos se encuentran operando. Solo cuenta con la opción de Single User MIMO, hasta 80MHz en ancho de canal y una tasa de transferencia máxima teórica de 845Mbps.

Estándar IEEE 802.11ac Wave2

A pesar de que no ha sido aprobada oficialmente, esta subdivisión del estándar, ya se encuentra desplegada en los dispositivos WiFi 802.11ac, con el fin de poder ofrecer todos los beneficios, lo cuales entre los principales son: Multiple User MIMO, hasta 160MHz en ancho de canal, hasta 4 flujos espaciales y hasta 2.26Mbps en tasa teórica de transferencia de datos.

Una de las actualizaciones más interesantes, es la de SU-MIMO, la cual permite activar el beamforming, con hasta 4 dispositivos, desde un mismo radio, permitiendo un mejor aprovechamiento de la red y del ancho de banda, siempre teniendo en consideración las capacidades del dispositivo cliente, ya que, sobre todo los dispositivos más antiguos, aun no cuentan con esta capacidad, convirtiendo al beamforming en una cualidad que solo aportará en descarga, en sentido hacia el cliente. Si el cliente ya cuenta con la capacidad de beamforming, el sentido del flujo de datos podrá ser bidireccional (carga y descarga).

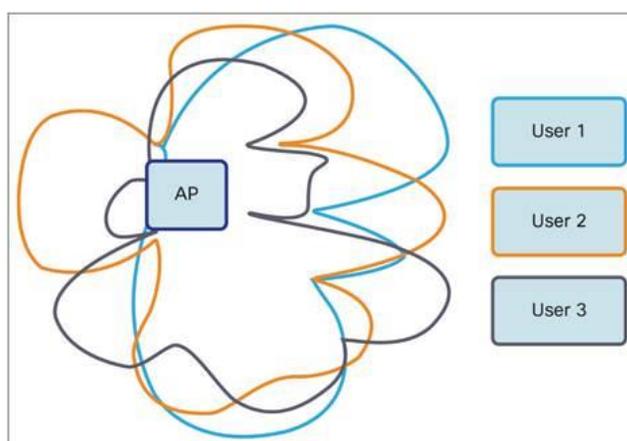


Figura 6. MU-MIMO con varios clientes

Fuente: (Cisco, 2018)

En la figura anterior, podemos observar como un punto de acceso, realiza beamforming con tres clientes, con MU-MIMO, formando un haz de potencia de radio dedicado hacia cada uno de los clientes.

1.4. Técnicas de modulación en 802.11

1.4.1. Espectro Ensanchado por Secuencia Directa

Es común encontrarla en dispositivos con estándar 802.11b. Posee ancho de banda entre 1 Mbps y 11 Mbps dependiendo del esquema de modulación. Consiste en una técnica de modulación del espectro expandido para la transmisión de señales digitales en un medio no físico, en el cual un flujo de datos es transmitido en conjunto con una gran cantidad de bits para dividir la información transmitida sobre el espectro. Esto se convierte en un código redundante, por lo que, si llegan a dañar o perder paquetes el receptor podrá recuperarlos y restaurar el código original. La operación se cumple al multiplicar la portadora de frecuencia y una señal digital de pseudo-ruido que es generada por un modulador que utiliza QPSK o BPSK, resultando en una señal TF que es reemplazada con una señal de ancho de banda equivalente espectral de la señal de ruido. El proceso de demodulación multiplica nuevamente el pseudo-ruido con la señal de radio frecuencia RF entrante para producir una señal con un valor máximo de dos señales correlacionadas, manteniendo el valor de ruido bajo el límite máximo con el fin de evitar la pérdida de información. (techopedia, s/a)

1.4.2. Espectro Ensanchando por Salto de Frecuencia

Esta técnica no es muy utilizada por los fabricantes de dispositivos, teniendo como rival al espectro de secuencia directa (DSSS). De hecho, el mismo grupo de investigación 802.11, reconoce que el espectro ensanchado por salto de frecuencia (FHSS) ha perdido

la batalla, ya que las pudiera de dispositivos son compatibles con DSSS. Algunos investigadores han propuesto ideas sobre que FHSS pudiera contribuir con la seguridad en 802.11, lo cual no ha pasado de expectativas inválidas, ya que sus códigos de salto son de fuente abierta y están disponibles para cualquier persona.

1.5. Movilidad e itinerancia en 802.11

Dentro de 802.11 se implementa la funcionalidad de que un cliente se pueda desplazar por un espacio físico, permitiendo que el dispositivo pueda cambiar de puntos de acceso (Roaming) en la misma o diferente frecuencia o canal. Esta función es permitida gracias a las tramas *Beacon* que contienen toda la información de la red inalámbrica y que comparten todos los puntos de acceso de una misma WLAN.

1.6. Escaneo de redes

Existen dos maneras para explorar redes 802.11:

Modo pasivo: El dispositivo se limita a escuchar tramas *Beacon* que son emitidas por los dispositivos activos.

Modo activo: El dispositivo solicita confirmación de respuesta de dispositivos existentes dentro de la red.

1.7. Seguridad

Dentro de la definición del estándar 802.11, existe un capítulo entero dedicado a describir temas de autenticación y privacidad. El capítulo 8 del desarrollo del estándar detalla de las posibles vulnerabilidades que puede ser víctima una red inalámbrica sobre 802.11, inclusive bajo conocimiento del grupo de desarrollo del estándar. Para contrarrestar, como primer avance se implementó el algoritmo Privacidad Equivalente por Cable (WEP) para mitigar posibles accesos no autorizados.

La seguridad dentro de una red 802.11 puede ser invalidada bajo tres aspectos: encriptado, algoritmos o protocolos de autenticación y marcos de autenticación.

Otros protocolos de autenticación son Protocolo Liviano y Expansible de Autenticación (LEAP) propiedad de Cisco, Protocolo Expansible de Autenticación – Seguridad de la Capa de Autenticación (EAP-TLS) propiedad de Microsoft y disponible desde Windows XP, Servicio de Discado interno para el Acceso Remoto de Usuario (RADIUS) sobre 802.11X. Adicional se tiene disponible 802.11X/LEAP en dispositivos Cisco Aironet 350 para WLAN.

Wired Equivalent Privacy (WEP)

Su definición literal indica que fue diseñado con el objetivo principal de simular o igualar el nivel de seguridad de cualquier red cableada, sin embargo, como toda red, inclusive las que utilizan medio físicos para su despliegue, pueden ser víctimas de ataques por intrusos que escuchan el tráfico que circula dentro de la red. Todo esto, sumado a que en un medio no físico se puede ser más vulnerable a escuchas, da por sentado que Wired Equivalent Privacy (WEP) no fue una solución óptima para certificar la seguridad de 802.11 y de que el solo nombre o el hecho de tratar de igualar la seguridad de una red cableada, no es suficiente.

La principal vulnerabilidad de WEP se encontró en que el encriptado (RC4) de las llaves que son de 40 bits o 128 bits, y que se comparten en 802.11 sobre la capa 2, utilizan un vector de inicialización de 24 bits, lo cual es demasiado pequeño, para el tamaño de las llaves secretas. Además, que, dentro del estándar no se especifica la administración de las llaves secretas, por lo que los códigos son de fuente abierta, hicieron de WEP un sistema de seguridad bastante vulnerable. Varios investigadores han

afirmado que WEP no cumple con los 3 principios básicos de seguridad: integridad de datos, control de acceso y confidencialidad de nombres, a pesar del conocimiento de los desarrolladores, y de hecho se propone penalizar al despliegue de este tipo de cifrado, que es muy utilizado por ser rápido, pero demasiado inseguro. (Nikita, Ian, & David, s/a)

Sobre lo reportado por estos autores, la Wireless Ethernet Compatibility Alliance (WECA), ahora WiFi Alliance, respondió un comunicado confirmando el conocimiento de la vulnerabilidad indicando que *poco es mejor que nada*, y que WEP no fue desarrollado para suplir todas las necesidades de seguridad de 802.11. WECA o WiFi Alliance es la organización responsable de certificar los dispositivos que cumplan con el estándar 802.11 otorgándoles permiso de utilizar el logo WiFi.



Figura 7. Logo de certificación de WiFi Alliance

Fuente: (Wi-Fi Alliance, s/a)

Por su lado, el concejo del IEEE 802.11, en su informe de respuesta, cita comentarios mencionando y aclarando que el desarrollo de WEP fue realizado bajo el mismo esquema, incluso que el mismo estándar 802.11, es decir en código de fuente abierta con el fin de que terceros fuera del grupo de investigación puedan a portar al desarrollo y mejora de estos. Sin embargo, en cuanto a la definición literal de su nombre, el grupo de investigación continúa desarrollando mejoras para lograr alcanzar una seguridad

comparable con la de una red cableada, evitando las vulnerabilidades como las que se presentan en el proceso de salto de frecuencia. (Stuart, 2002)

WiFi Protected Access (WPA)

El Acceso Protegido a WiFi nace a partir de las evidentes falencias de WEP durante el desarrollo de 802.11i como una solución compatible para todas las variaciones de estándar. Luego vendría a ser WAP2 en su solución completamente desarrollada.

En general, WAP basa su seguridad en un algoritmo del Protocolo de Integridad de Clave Temporal (Temporary Key Integrity Protocol: TKIP) que cambia automática y constantemente la clave.

El principio es básicamente el mismo que WEP: se comparte una clave secreta entre los clientes inalámbricos y los puntos de acceso. Estas llaves pre-compartidas (Pre Shared Key: PSK) contienen información importante de la red, pero con el adicional que esta va cambiando la encriptación, llegándose a denominar WPA-Personal por la WiFi Alliance. También existe la variante de WPA-Empresarial utilizando en 802.1X

WPA2-PSK

Con el desarrollo completo del estándar 802.11i, se reflejó que el TKIP presenta vulnerabilidades en modo compatible con versiones anteriores, por lo que algunos ataques pueden mostrar ciertos paquetes que pueden ser descifrados y manipulados.

Para mitigar por completo estos vacíos, se ha desarrollado un nuevo algoritmo de encriptación con el uso del Sistema de Encriptación Avanzada Advanced Encryption System: AES), el cual representa un nivel mucho mejor en cuanto a seguridad, por lo que la recomendación actual es utilizar WPA2 con AES.

2. Capítulo II: Descripción general de la WLAN

Amparados en un proceso público de contratación de servicios, la Universidad de las Fuerzas Armadas - ESPE, solicitó a la empresa proveedora de servicios de telecomunicaciones, entre otros servicios: “Proveer servicios de WIFI gestionado...” con el objetivo principal de proporcionar a la comunidad universitaria, acceso a plataformas tecnológicas para el desarrollo de los diferentes tipos de actividades dentro del campus matriz, como lo son actividades académicas, de investigación y administrativas.

2.1. Equipamiento

Para ejecutar lo solicitado, el proveedor de servicios ha implementado equipos Cisco Aironet 2800, 1560 y la controladora 5520 lo cual es una solución escalable diseñada para abarcar clientes empresariales, así como transnacionales y empresas distribuidas con administración centralizada.

2.1.1. Controladora

Para la solución actual, se cuenta con una controladora Cisco 5520 dentro del datacenter de la Universidad, la cual posee las características:

Hasta 20000 clientes y hasta 1500 puntos de acceso

Estándar 802.11ac Wave 2, con una capacidad de 20Gbps

Soporte para implementaciones centralizadas, distribuidas y tipo Mesh

Gestión centralizada con controladoras adicionales

Alta disponibilidad con interfaces redundantes (Gigabit o 10 Gigabit Ethernet), fuente de alimentación redundante (opcional), reinicio de dispositivo más rápido, hardware sólido sin partes móviles.

Cuenta con gestión local y remota por Graphical User Interface (GUI) la cual permite acceso por http o https en ambiente gráfico, y también por Command-Line Interface (CLI) por puerto de consola (solo local) y con protocolos Telnet o SSH.



Figura 8. Cisco 5520 Wireless Controller

Fuente: (Cisco, s/a)

2.1.2. Puntos de acceso para interiores

Se ubicarán según la mejor disposición planificada, logrando seguridad e integridad física bajo responsabilidad del proveedor.



Figura 9. Punto de acceso para interior Cisco Aironet serie 2800

Fuente: (Cisco, 2018)

Tecnología inalámbrica:

Dual-radio 5GHz 2.4Ghz

802.11ac Wave 2

4x4 MU-MIMO

Capacidad 2.6 Gbps en *throughput* agregado

WiFi multimedia WMM

Hasta 400 clientes asociados concurrentes

Hasta 50 clientes asociados por banda

Interfaz:

Dos interfaces GigabitEthernet: auto censado 100/1000Base-T

PoE y PoE+

Link Aggregation Group

Una interfaz de administración vía consola con conector RJ45

Estándares soportados:

IEEE 802.11a/b/g

IEEE 802.11n

IEEE 802.11h

IEEE 802.11d

IEEE 802.11ac

Modo de operación:

Modo independiente o standalone

Modo controlador en premisa on-Premise

Antena:

Interna omnidireccional en azimut:

2.4 GHz: ganancia 4 dBi

5 GHz: ganancia 5 dBi

Interna direccional con elevación de ancho de haz 90°

5 GHz: ganancia 6 dBi (Cisco, 2018)

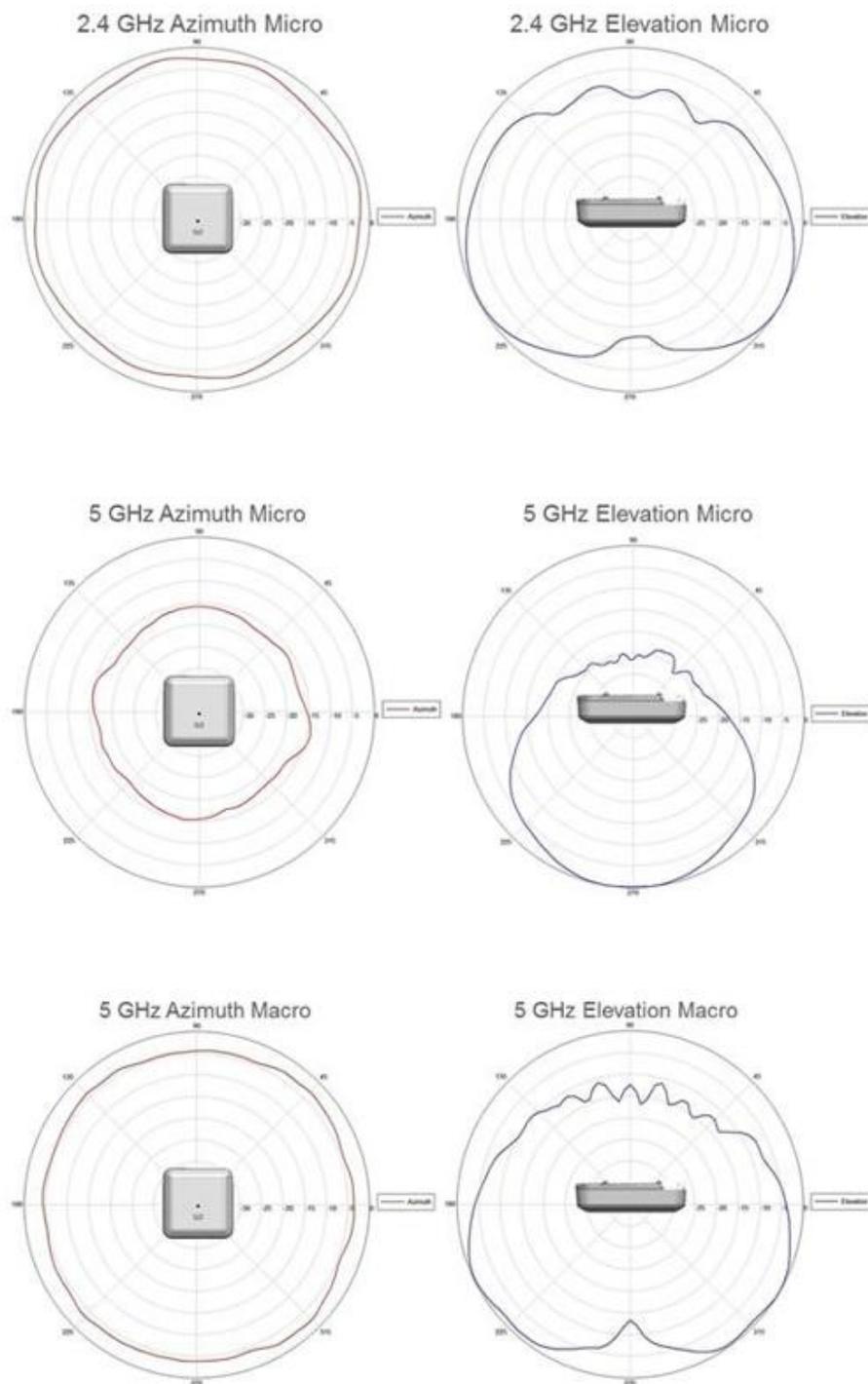


Figura 10. Modelo de propagación punto de acceso interiores

Fuente: (Cisco, 2018)

2.1.3. Puntos de acceso para exteriores

Se ubicarán según la mejor disposición planificada, logrando seguridad e integridad física bajo responsabilidad del proveedor.



Figura 11. Punto de acceso para exterior Cisco Aironet serie 1560

Fuente: (Cisco, 2018)

Tecnología inalámbrica:

Dual-radio (5GHz/2.4Ghz)

802.11ac Wave 1 y 2

3x3 MIMO

Capacidad hasta 1.3 Gbps

Hasta 400 clientes

Hasta 50 usuarios concurrentes por banda

Interfaz

Una interfaz WAN auto censado: 10/100/1000BASE-T Ethernet tipo RJ-45

PoE in

Una interfaz SFP tipo fibra o eléctrico

Una interfaz de administración vía consola con conector RJ45

Estándares soportados (se incluye velocidad de transmisión)

802.11a: 6, 9, 12, 18, 24, 36, 48, y 54 Mbps

802.11b/g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, y 54 Mbps

802.11n: 6.5 Mbps a 450 Mbps para 2.4 GHz y 5 GHz

802.11ac: 6.5 Mbps a 450 Mbps para 5 GHz

Modo de operación

Modo independiente o standalone

Modo controlador en premisa on-Premise

Antena

Integrada semi direccional banda dual tipo 1562I

2.4 GHz: ganancia 7 dBi

5 GHz: ganancia 4 dBi

Bandas de frecuencia seleccionables por software para cada radio

Control de beamforming

2.2. Tiempo de servicio

Se cumple con un tiempo de servicio o vida útil de los equipos por al menos tres años, certificados por el fabricante.

2.3. Características generales

El nivel de intensidad de señal inalámbrica en cada zona de interés como edificios o puntos de acceso, es considerado como idóneo, bueno, bajo y sin señal, según la siguiente referencia:

Tabla 3.
Nivel de señal

Parámetro	Rango [dBm]
Idóneo	-40 a -59
Bueno	-60 a -69
Bajo	-70 a -79
Sin señal	-80 o menos

En caso de presentarse una intensidad inferior a bueno, en los puntos de cobertura establecidos, el proveedor toma acciones correctivas para mejorar dicha cobertura.

El proveedor certifica los niveles de señal inalámbrica mediante mapas de calor obtenidos con herramientas especializadas de certificación de la misma marca de los productos ofertados, o de marcas reconocidas en la industria. Los mapas de calor son entregados al menos dos veces al año a la Unidad de Tecnologías de la Información y Comunicaciones de la ESPE.

2.4. Gestión de red

La solución implementada funciona sobre una plataforma virtualizada VMWare entregada por la Universidad de las Fuerzas Armadas ESPE, con un esquema de alta disponibilidad en un segundo servidor de respaldo. El fabricante recomienda, contar con los siguientes requerimientos mínimos:

Tabla 4.
Requerimientos mínimos para VMWare

Requerimiento	Express	Express-Plus	Standard	Professional
Versión VMware	ESXi 5.5 o 6.0			
CPUs Virtuales	4	8	16	16
Memoria (DRAM)	12 GB	16 GB	16 GB	24 GB
Disco duro	300 GB	600 GB	900 GB	1.2 TB
Throughput	200 MB/s	200 MB/s	200 MB/s	320 MB/s

Características adicionales:

SNMP sobre capa 2 en tiempo real.

HTTP

Orientado a soluciones inalámbricas y cableadas.

Análisis detallado de salud de red para conocer asociación de un usuario, asignación de direcciones IP y servicio de DNS.

Portal cautivo con un diseño independiente por sede.

2.5. Expansibilidad

Se considera, un crecimiento de la infraestructura instalada en cada localidad de hasta un máximo del 30% del total de la cantidad de puntos de acceso, con la finalidad de cubrir nuevas necesidades de la Institución, sin costo adicional para la Universidad.

El proveedor contará con la capacidad de reubicar hasta un 30% de la infraestructura de puntos de acceso instalada en una locación hacia otra o dentro de la misma, sin costo adicional para la Universidad.

2.6. Conectividad

En edificaciones donde no se dispone del cableado estructurado interno, se establece conectividad mediante cableado CAT 6A (o superior) o fibra óptica.

En localidades donde se dispone de cableado estructurado interno, se lo utiliza, bajo la responsabilidad de certificar los enlaces (bloques G y H para campus matriz).

2.7. Propagación de SSID

Para el servicio a usuarios, la implementación cuenta con la capacidad de manejar al menos 14 SSIDs (de 512 SSIDs soportados por la controladora), con seguridad tipo WPA2 Enterprise y cifrado AES, compatible con 802.1x y autenticación web. Para dispositivos inalámbricos que no puedan autenticarse por sí mismos (Ej.: Sensores IoT, cámaras de seguridad, entre otros), se maneja autenticación MAC Bypass.

La autenticación web autoriza, autentica y toma como base de datos de información de usuarios un servidor LDAP provisto por la Universidad de las Fuerzas Armadas ESPE.

La Universidad de las Fuerzas Armadas ESPE, dispone de la red inalámbrica EDUROAM, la misma que es propagada a través de un SSID denominado eduroam, la misma que es mantenida.

La solución implementada estará en la capacidad de diferenciar grupos de usuarios inalámbricos dentro del mismo SSID mediante el motor de servicios de identificación ISE, con capacidad de asignación independiente de políticas de acceso como MAC, políticas AAA, sistemas operativos, hardware, nombres, entre otros.

Los SSIDs propagados serán: ESPE, INVITADOS, eduroam, ESPE_VIP.

2.8. Solapamiento

El proveedor garantiza la convivencia del servicio de red inalámbrica implementada en el Campus Matriz (Arquitectura Cisco) con la nueva solución de WiFi gestionado, mediante los dispositivos Cisco Aironet que brindan convivencia nativa con otros dispositivos Cisco.

También se garantiza que la infraestructura implementada permita realizar cambios automáticos en los canales y potencias que son utilizados por los puntos de acceso a fin de evitar el solapamiento con Radio Resource Manager (RRM), que se encarga de la evaluación dinámica de los canales para hacer asignaciones según algoritmos avanzados de medición de radio frecuencia (FRA, DCA, TPC, CHDM-A, etc.) para evitar el solapamiento y mejorar la cobertura de señal de manera automática.

2.9. Estándares soportados

La solución soporta los siguientes estándares IEEE:

IEEE 802.11b

IEEE 802.11g

IEEE 802.11n

IEEE 802.11ac

IEEE 802.11ac wave 2

802.3at PoE+, Cisco Universal PoE (Cisco UPOE®)

802.3at power injector (AIR-PWRINJ6=)

802.11i, Wi-Fi Protected Access 2 (WPA2), WPA

802.1X

2.10. Movilidad

Se permite el *roaming* de los usuarios entre diferentes puntos de acceso y sus diferentes celdas, sin necesidad de una nueva autenticación y reduciendo ruido con ClientLink 4.0.

2.11. Seguridad

Se cuenta con la implementación de un portal cautivo completamente adaptable a la imagen corporativa de la Universidad y/o de cada localidad, es decir que la URL, el título del portal, las imágenes utilizadas en el mismo, el lenguaje y la información solicitada al usuario serán adaptable a las necesidades, con diseño personalizado mediante ISE y el creador de portales ISEPB.

La infraestructura permite la protección integrada de intrusiones inalámbricas WIPS, protección y mitigación contra DoS, Spoofing, MitM, Puntos de Acceso Intrusos: Rogue AP, de manera que se protege la información de los usuarios manteniendo la confidencialidad, disponibilidad e integridad de la información y soportará los siguientes algoritmos de cifrado: AES, TLS, EAP, TTLS, WPA, WPA2.

Se dispone de la capacidad de monitorear puntos de acceso no autorizados con Wireless Security Module WSM, entregando datos como: estado, canal, SSID, fecha y hora de la conexión, clasificando el grado de amenaza para minimizar los falsos positivos, y generando alertas y reportes ante la detección de amenazas.

Adicional, se permite identificar servicios de seguridad y reputación de IPs, clasificación, bloqueo malicioso de archivos, URLs e IPs.

Estas funciones permiten entregar información sobre el tráfico de usuario, incluyendo: aplicación, categoría de aplicación y reputación de sitio web, por medio de *Web Filter* y *Application Control*.

Para asegurar una óptima operación durante todo el tiempo de servicio, los equipos operan con la última versión de sistema operativo liberado por el fabricante.

2.12. Monitoreo

Se realiza mediante un navegador y provee:

Métricas de rendimiento de dispositivos.

Monitoreo y control en tiempo real de cada punto de acceso mostrando su dirección IP, dirección MAC y número de clientes registrados.

Monitoreo en tiempo real de clientes mostrando su identificación, ancho de banda que utiliza, su direccionamiento IP y MAC, alarmas activas e históricas.

Almacenamiento de alarmas históricas por hasta tres meses.

Información en figuras y tablas.

2.13. Diagnóstico y alertas

Se cuenta con la disponibilidad de configurar diferentes tipos de alertas y su severidad. Las mismas están en conocimiento del personal de la Unidad de Tecnologías de la Información y Comunicaciones por medio de envío de notificaciones vía correo electrónico, así como en la plataforma de gestión de red.

Para compatibilidad con otros sistemas de administración y gestión de red, la plataforma está en la capacidad de enviar paquetes de Protocolo Simple de

Administración de Red SNMP o por medio de una Interfaz para Programación de Aplicaciones API. (Cisco, 2018)

2.14. Soporte técnico

Se dispone de soporte técnico por parte de la empresa proveedora de servicios, con varias alternativas:

Soporte en sitio: Se cuenta con personal calificado para realizar soporte sobre cualquier incidente presentado sobre la WLAN, en horario de oficina, quien también puede realizar monitoreo en tiempo real de toda la infraestructura, inclusive a nivel nacional, con la ayuda de las herramientas propias de Cisco, desde el departamento de UTIC de la Universidad.

Soporte remoto: Se cuenta con el aval de la empresa proveedora de servicios de telecomunicaciones que mantiene el contrato de servicios, la cual deriva una solicitud de soporte hacia la empresa privada que provee los servicios de WiFi gestionado, con la generación de tickets de atención, por medio de los siguientes recursos:

Atención telefónica: 1800-400-404 (Opc. 01) / 1-800-400-408

Atención web: <https://latam.my.level3.com/portal/#/>

Una vez generado el reporte de la incidencia, se cuenta con un Ingeniero de soporte quien realizará todas las validaciones del evento para analizar y ejecutar la solución al mismo.

2.15. Administración y configuración

Se permite la administración y configuración de los puntos de acceso, de manera individual o en grupo, por medio de archivos tipo plantilla, dentro de la herramienta Cisco Prime Infrastructure.

2.16. Roles de usuarios de la plataforma

La plataforma de gestión permite la definición de roles por usuarios con su respectiva contraseña. Dentro de cada perfil se puede limitar el acceso a cada segmento de red. Se cuenta con la disponibilidad de acoplamiento con servidores Active Directory, LDAP o RADIUS, propiedad de la Universidad. (Cisco, 2018)

2.17. Localización

La ubicación de los dispositivos puede ser mostrada con la utilización de mapas geográficos mediante Work with Site Maps, entregando información en tiempo real y pudiendo cargar mapas de calor. (Cisco, 2018)

2.18. Reportes

Para obtener la información detallada del desenvolvimiento de la implementación, se puede acceder a reportes de los puntos de acceso y de la infraestructura de la red, con la opción de configurarlos por día, semana, mes, etc., y que sean enviados vía correo electrónico en formatos XHTML, HTML y PDF. (Cisco, 2017)

2.19. Otros

Por medio de las funciones de Optimized Roaming, se prevé el efecto de *sticky client* para balancear automáticamente los usuarios entre diferentes puntos de acceso y así mejorar el uso de recursos.

La asignación y selección de canal, ajuste de nivel de potencia y selección de frecuencia, de los puntos de acceso es de manera automática con Radio Resource Management RRM, evitando el solapamiento y mejorando la zona de cobertura automáticamente.

El equipamiento es nuevo de fábrica, con una fecha de manufactura a partir del primer semestre de 2017.



Figura 12. Switch LAN dedicado para red inalámbrica

3. Capítulo III: Medición de la WLAN

3.1. Descripción del escenario de pruebas

Para el desarrollo del escenario planteado, se ha propuesto analizar el desempeño de la red inalámbrica del campus, en base a la experiencia del usuario local. Es decir, se tratará de utilizar las características desplegadas de la infraestructura, reflejadas en la apreciación de la calidad de servicio en un usuario que tenga acceso a la red inalámbrica, esto es, un estudiante, profesor o administrativo del campus.

Dado que, un usuario local, podría acceder a la red inalámbrica por medio de un dispositivo móvil o portátil, se desea utilizar estas plataformas de hardware para descargar, instalar y correr aplicaciones que permitan tomar estadísticas, bajo aspectos como: nivel de intensidad de señal, ancho de banda entregado para carga y descarga, cantidad de SSIDs propagados, canales disponibles y ocupados, frecuencias utilizadas, disponibilidad y respuesta de sitios de navegación.

También se podrán ubicar limitaciones de la infraestructura como: puntos muertos o zonas en donde no exista cobertura, puntos o zonas donde exista cobertura, pero no exista conectividad, sobre los cuales se puede generar un informe con un plan de mejoras futuro.

La información será tabulada y contrastada con las mediciones que muestra la herramienta de monitoreo de la implementación.

3.2. Descarga y configuración de aplicaciones para móviles y portátiles

Tal como se ha mencionado en el punto anterior, se desea medir la experiencia del usuario tomando en cuenta la accesibilidad a los diferentes dispositivos que utiliza en su jornada normal de actividades, como, por ejemplo: tabletas, teléfonos móviles,

computadores portátiles, por tanto, las aplicaciones son seleccionadas en base de puntuaciones valoradas por usuarios de estas.

Se ha conseguido utilizar aplicaciones como Net Analyzer, Speedtest, NetSpot, WiFi Analyzer, disponibles en las tiendas de aplicaciones de los sistemas operativos Windows, macOS, Android e iOS.

Las aplicaciones permiten la instalación con configuraciones básicas y rápidas. Se debe permitir el acceso a ciertas características del dispositivo.

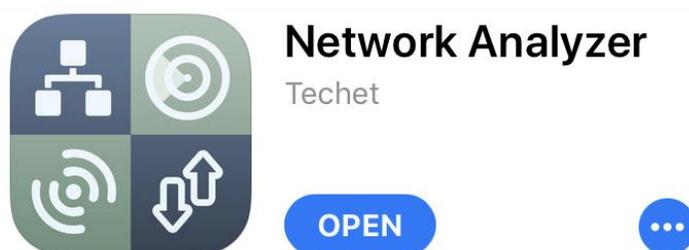


Figura 13. Network Analyzer en AppStore

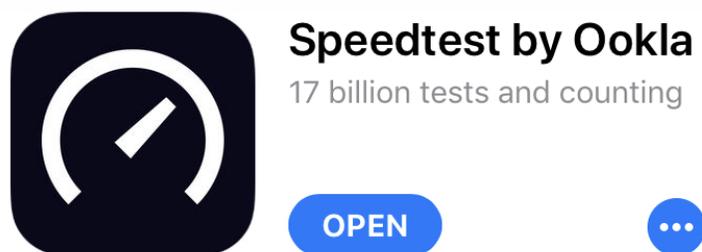


Figura 14. Speedtest en AppStore

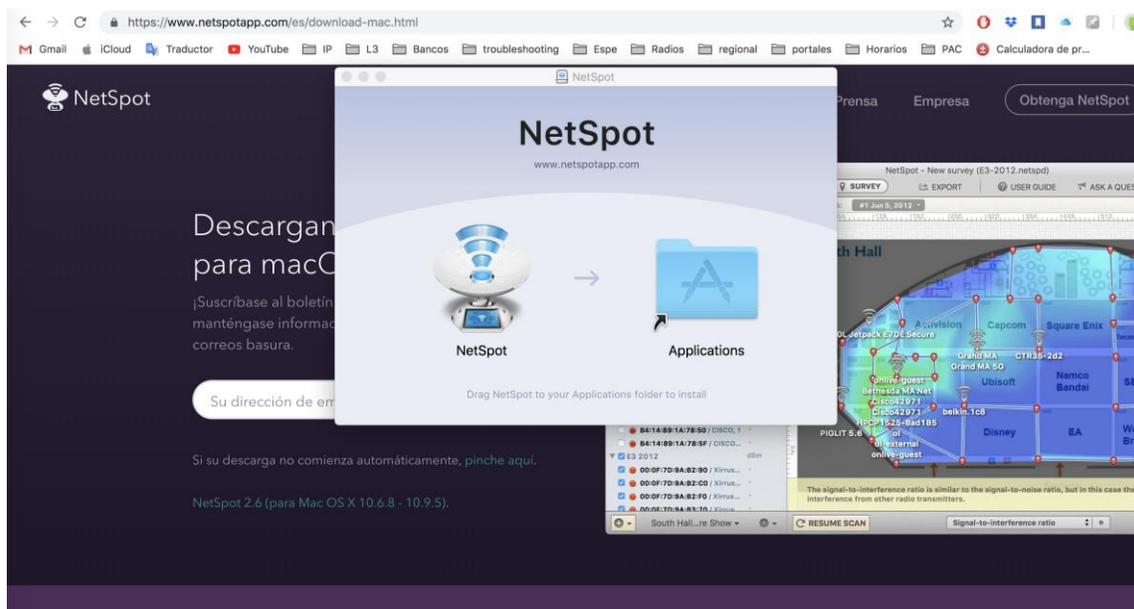


Figura 15. NetSpot para MacOS



Figura 16. WiFi Analyzer en Play Store

3.3. Ejecución del ambiente de pruebas

Se han seleccionado puntos estratégicos de las diferentes zonas al interior de campus, de tal manera que se pueda experimentar el diario vivir de los diferentes tipos de usuarios de la red inalámbrica, dentro de horarios convencionales de clases para contar con un flujo regular de usuarios. Es decir, en un ambiente normal, en base a aplicaciones que utilicen tráfico crítico como voz y video.

Dispositivos incluidos en el ambiente de pruebas:

Dispositivo portátil:



Figura 17. Dispositivo portátil

Dispositivo móvil:

Se emplea el uso de dos diferentes tipos de dispositivos:

Apple iPhone modelo A1660: WiFi 802.11 a/b/g/n/ac (2.4/5GHz) incluido MIMO

Samsung modelo S8+: WiFi 802.11 a/b/g/n/ac (2.4/5GHz), VHT80 incluido MU-MIMO, 1024QAM

Características de descarga de video desde YouTube®, duración 1 minuto.

Resolución 144p: 1,90 MB utilizados por minuto

Resolución 240p: 2,70 MB utilizados por minuto

Resolución 360p: 4,40 MB utilizados por minuto

Resolución 480p: 7,70 MB utilizados por minuto

Resolución 720p HD: 14,50 MB utilizados por minuto

Resolución 1080p FULL HD: 27,61 MB utilizados por minuto

Plan de pruebas

Definición de la ubicación del punto de toma de muestra

Ubicación geográfica

Descripción de la ubicación

Consumidor principal

Captura de muestreo con WiFi Analyzer

Gráfico de canales en banda 2.4GHz

Gráfico de canales en banda 5GHz

Captura de muestreo NetSpot

Gráfico de puntos de acceso disponibles (organizado por nivel de señal recibida SNR, en orden descendente y filtrado por Identificador de Señal SSID, e intervalo de refresco de 10 segundos)

Prueba de descarga de archivos

Prueba de velocidad SpeedTest

Dispositivo portátil

Dispositivo móvil

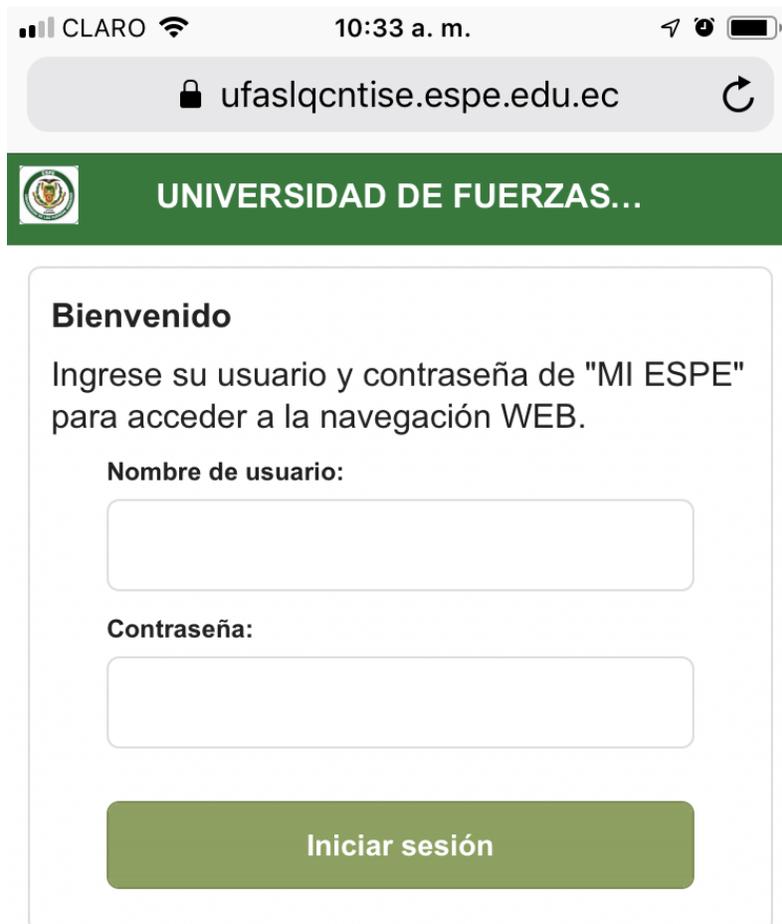
3.4. Registro en la red inalámbrica con SSID ESPE

Para un dispositivo móvil, el primer paso es el registro en la WLAN, buscamos el SSID, seleccionamos ESPE:



Figura 18. Selección de WLAN mediante SSID

El dispositivo automáticamente es redirigido al portal cautivo diseñado con la herramienta ISEPB propia de Cisco, en donde se pide ingresar el usuario y contraseña de Mi ESPE.



CLARO 10:33 a. m.

ufaslqcntise.espe.edu.ec

 UNIVERSIDAD DE FUERZAS...

Bienvenido

Ingrese su usuario y contraseña de "MI ESPE" para acceder a la navegación WEB.

Nombre de usuario:

Contraseña:

Iniciar sesión

Figura 19. Portal cautivo WLAN ESPE

Fuente: (Universidad de las Fuerzas Armadas - ESPE, 2019)

Una vez autenticado, se redirige a la página de bienvenida:

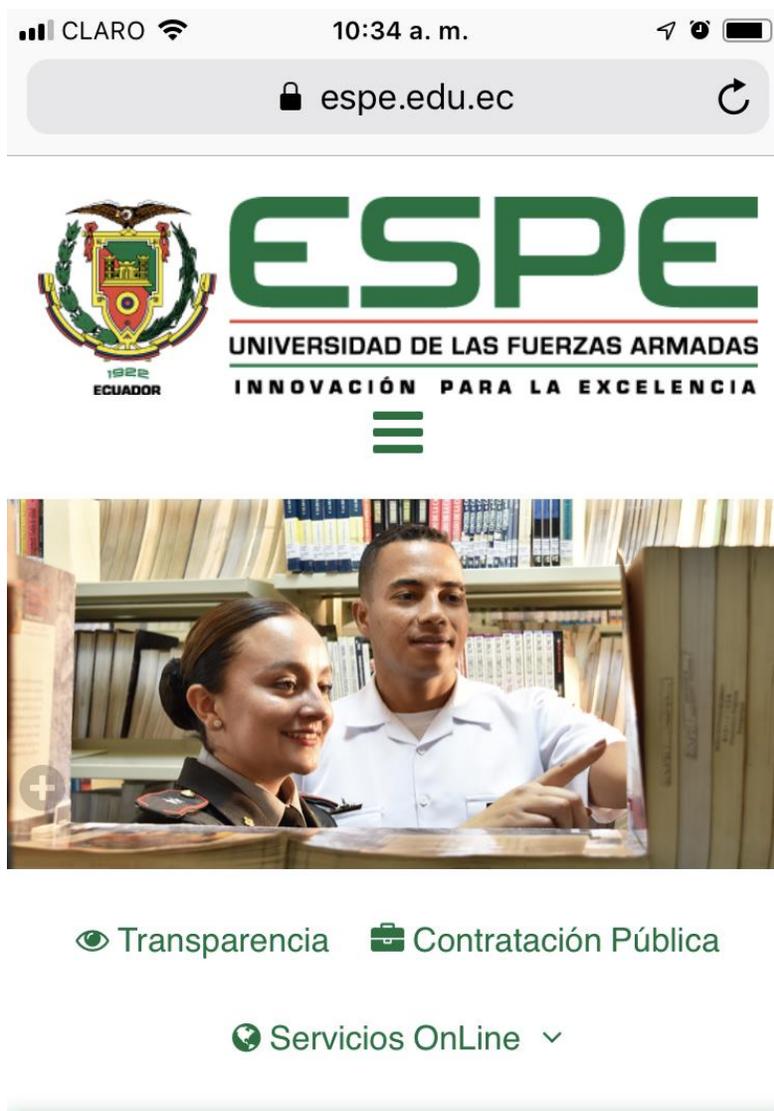


Figura 20. Página de bienvenida

Fuente: (Universidad de las Fuerzas Armadas - ESPE, 2019)

Se debe tener en cuenta que:

Seguridad: la red aparecerá como insegura por ser abierta, sin solicitar WEP o WPA.

Configuración IP: se debe permitir las configuraciones entregadas por la WLAN de forma automática.

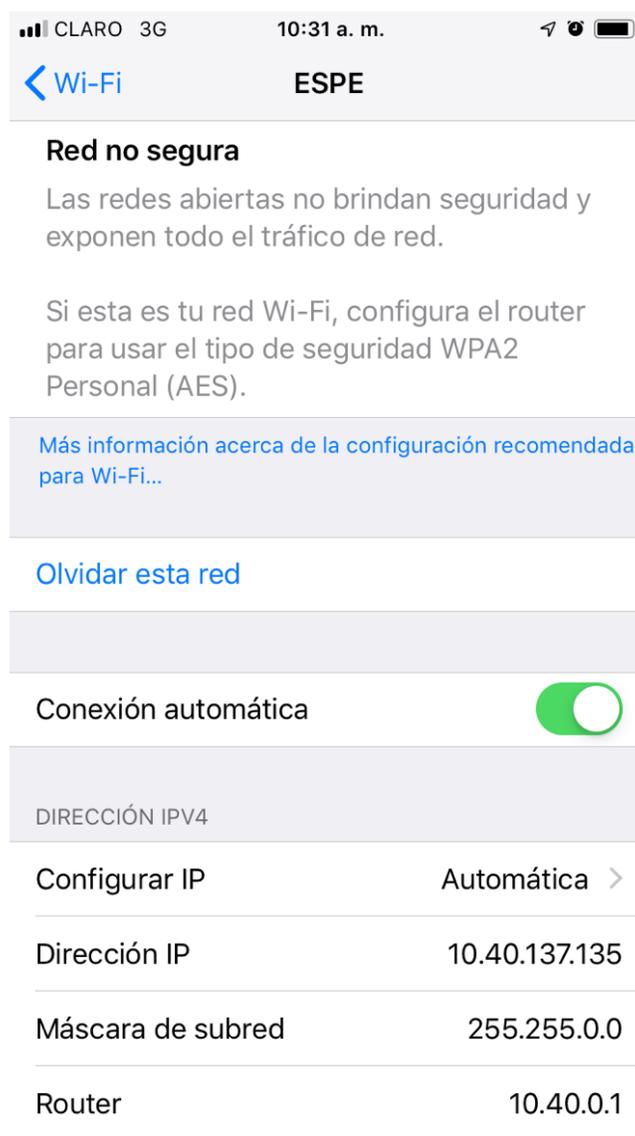


Figura 21. Estado de conexión inalámbrica

Certificado: Es posible que se solicite aceptar el certificado, y se debe aceptar.

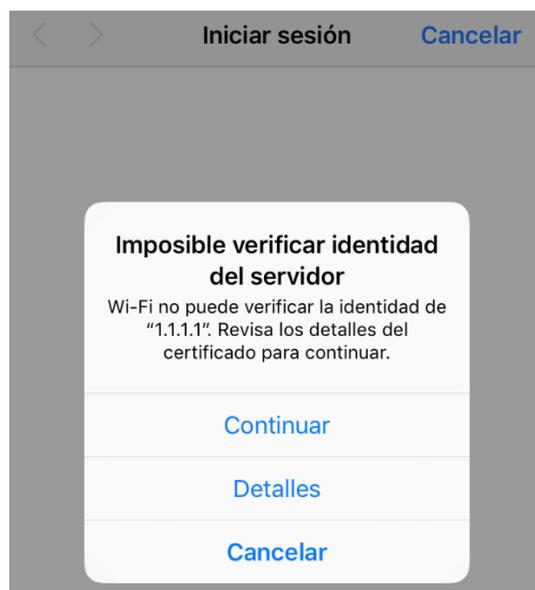


Figura 22. Advertencia de certificado

Número máximo de dispositivos: Si para un mismo usuario ya se han registrado dos dispositivos, sin importar si se encuentren conectados al mismo tiempo, el tercero se podrá registrar cuando se acepte desvincular al primer dispositivo de la WLAN, ya que la controladora solo aceptará dos direcciones MAC por usuario. Pueden existir problemas al tratar de realizar esta operación si todos los dispositivos están conectados simultáneamente, por lo que también se recomienda desconectar de la WLAN al primer dispositivo.



Figura 23. Advertencia máximo de dispositivos

Fuente: (Universidad de las Fuerzas Armadas - ESPE, 2019)

3.5. Toma de muestras

En un esquema de verificar el actual desempeño de la nueva WLAN, se dispuso a partir de dos escenarios: El primero en donde exista conectividad, con un nivel de señal de -80dBm o menor siendo el *Peor Escenario*; y, por otra parte, un segundo escenario en donde se tenga un nivel de señal entre -40dBm y -59dBm siendo el *Mejor Escenario*. Luego, entre estos dos escenarios, poder verificar los cambios según se tenga niveles entre -60dBm y -79dBm.

Descripción del mejor escenario

En un ambiente de pruebas, donde el nivel de señal se considera como idóneo, entre -40dBm y -59dBm, se ha dispuesto trabajar con el plan de pruebas descrito anteriormente, para validar si, cuando se tenga una excelente cobertura, el acceso permite trabajar en buenas condiciones. Se toma el punto 1 como referencia y obteniendo los siguientes resultados:

Definición de la ubicación del punto de toma de muestra

Punto:

17

Ubicación geográfica en grados decimales:

Latitud: -0.314298

Longitud: -78.445283

Descripción de la ubicación:

Edificio Central. Bloque A. Piso 1 (Interior)

Consumidor principal:

Estudiantes y profesores

Captura de muestreo con WiFi Analyzer



Figura 24. Nivel de señal de ESPE

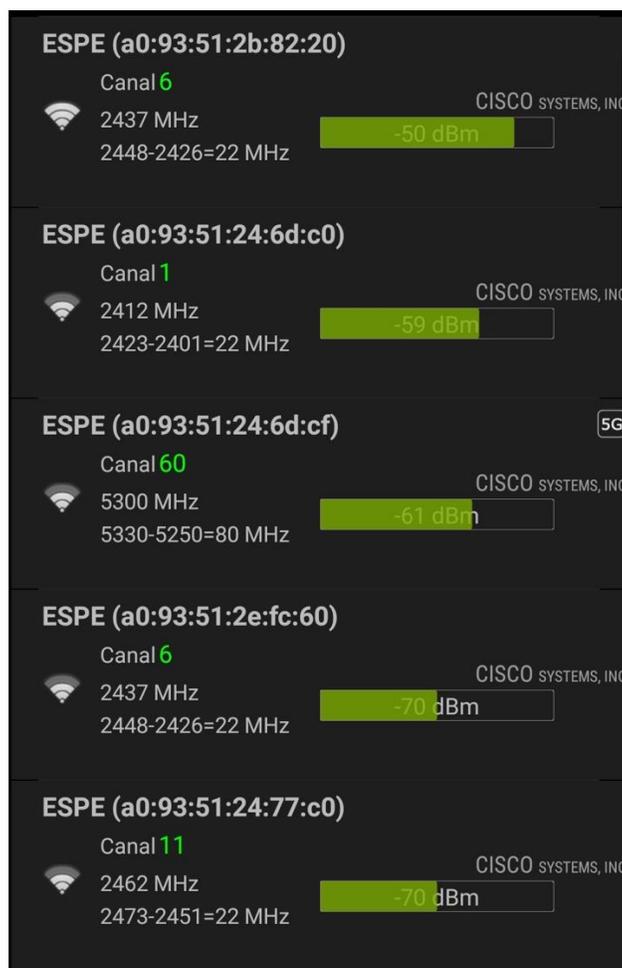


Figura 25. Desempeño de canales de ESPE

Canales en banda 2.4GHz

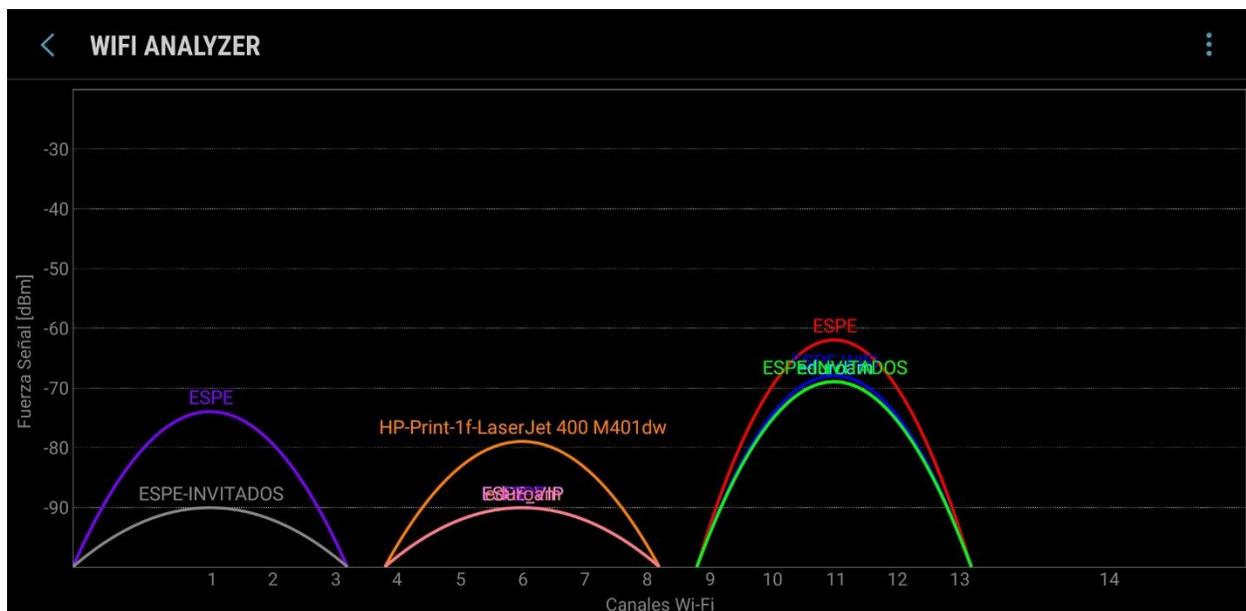


Figura 26. Escaneo de redes en 2.4GHz

Canales en banda 5GHz

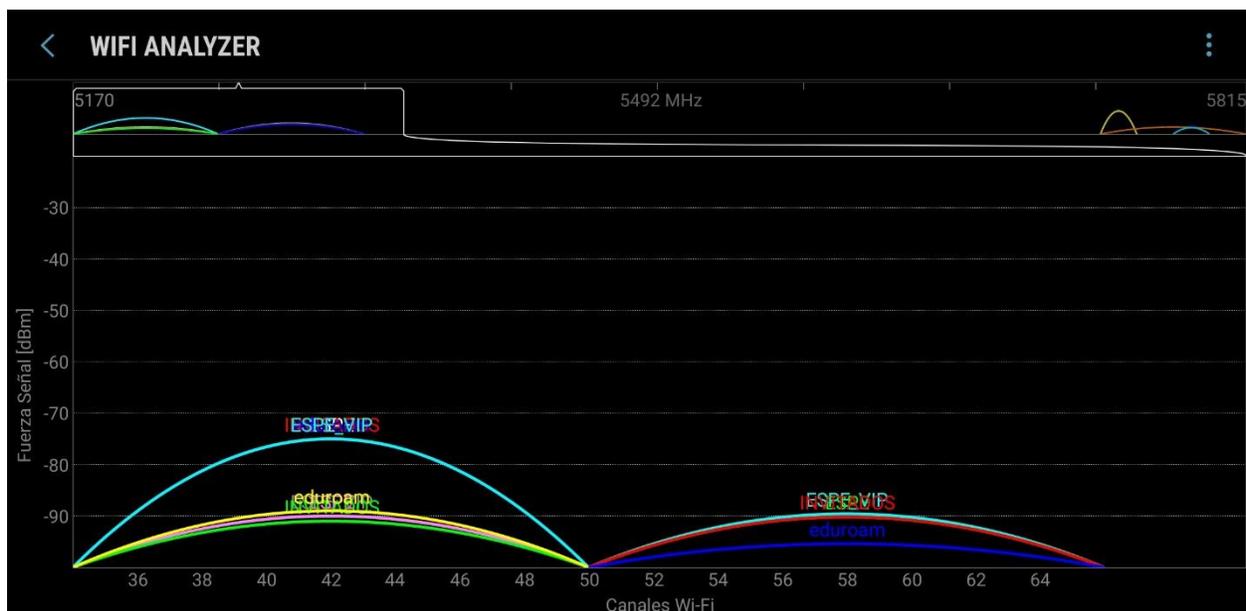


Figura 27. Escaneo de redes en 5GHz

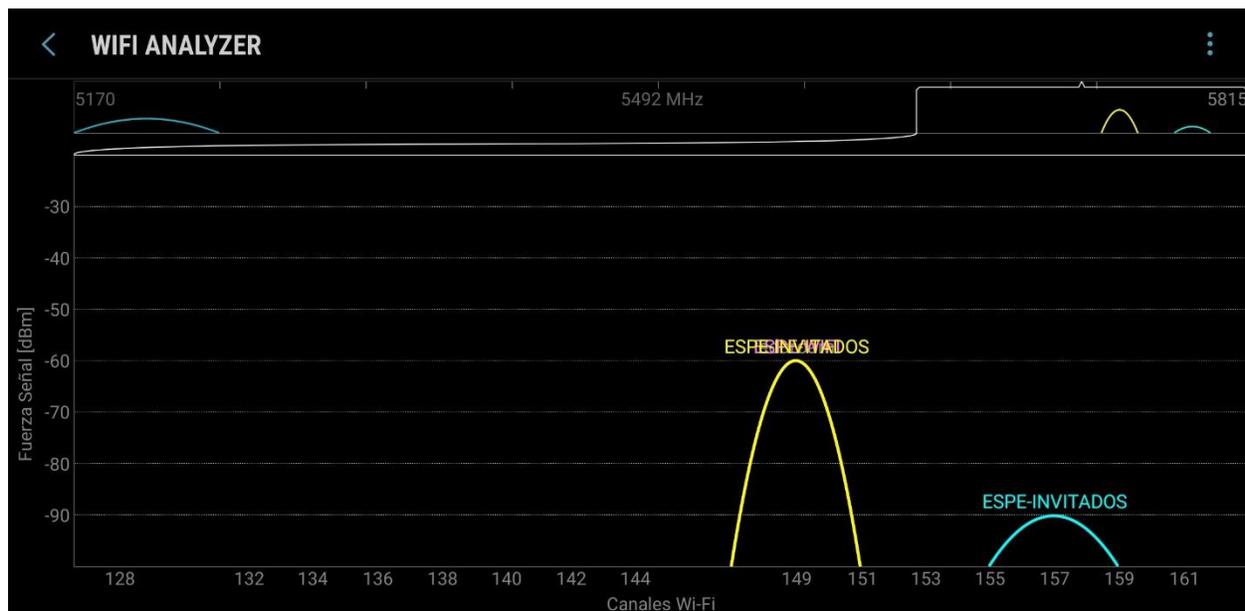


Figura 28. Escaneo de redes en 5GHz

Captura de muestreo NetSpot

Gráfico de puntos de acceso disponibles (organizado por nivel de señal recibida SNR, en orden descendente y filtrado por Identificador de Señal SSID, e intervalo de refresco de 10 segundos)

SSID	BSSID	Alias	Canal	Banda	Seguridad	Vendedor	Modo	Nivel (S...)	Señal	Señal %	Med	Máx	Mín	Ruido	Ruid...	Último
ESPE	70:69:5A:C7:2D:80		11	2.4GHz	Open	Cisco	b/g/n		-42	58%	-45	-36	-48	-96	4%	now
ESPE_VIP	70:69:5A:C7:2D:8C		84	5GHz	WPA Personal	Cisco	ac		-56	44%	-57	-46	-60	-96	4%	now
ESPE	70:69:5A:C7:2D:8F		84	5GHz	Open	Cisco	ac		-56	44%	-57	-46	-60	-92	8%	now
ESPE	70:69											17	-69	-96	4%	now
ESPE_VIP	70:69											7	-70	-96	4%	now
ESPE	28:AC	Gráficos/Pantallas										11	-70	-96	4%	now
ESPE_VIP	70:69	Hardware RAID										11	-68	-96	4%	now
ESPE	70:69	Impresoras										11	-69	-96	4%	now
ESPE	70:69	Lector de tarjeta										11	-69	-96	4%	now
ESPE	28:AC	Memoria										14	-77	-96	4%	now
ESPE_VIP	70:69	NVMeExpress										15	-79	-96	4%	now
ESPE_VIP	70:69	PCI										15	-78	-96	4%	now
ESPE	70:69	SAS										18	-81	-96	4%	now
ESPE	28:AC	SATA/SATA Express										19	-81	-96	4%	now
ESPE_VIP	28:AC	Controladora de disco										19	-81	-96	4%	now

Información de la red actual:	
Modo PHY:	802.11ac
BSSID:	70:69:5a:c7:2d:8f
Canal:	84
Código del país:	EC
Tipo de red:	infraestructura
Seguridad:	Ninguno
Señal / Ruido:	-55 dBm / -93 dBm
Velocidad de transmisión:	878
Índice MCS:	7
Otras redes Wi-Fi locales:	

Figura 29. Escaneo de redes con Netspot

Prueba de descarga de archivos

Con la ayuda del portal en <https://www.thinkbroadband.com/download>, se logra realizar la descarga de archivos de diferente tamaño, con la finalidad de poder tomar una estadística en tiempo para completar la operación. Tomando en

cuenta actividades cotidianas de un estudiante, se utiliza un archivo de 20MB, el mismo que contiene un código aleatorio que no podrá causar daño alguno al dispositivo utilizado, es decir, se lo hace con fines netamente de prueba. El archivo puede bajarse con IPv4 e IPv6, sobre los puertos 80 (Protocolo de Transferencia de Hipertexto - HTTP), 81 (lo utiliza Internet Protocol Suite) y 8080 (HTTP para Tomcat).

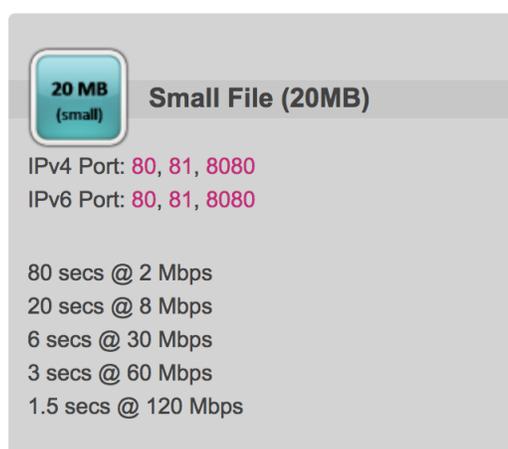


Figura 30. Archivo prueba descarga

Prueba de velocidad SpeedTest

Mediante la aplicación para móviles, computadores o por el enlace <https://www.speedtest.net/> se accede a la herramienta de medición de velocidad de carga y descarga, teniendo en cuenta la capacidad disponible. Es decir, dado que no se puede tener el canal 100% libre de uso, la prueba nos mostrará sólo capacidad libre en velocidad disponible para esa sesión. Mas, vemos que es una velocidad aceptable, inclusive para tráfico sensible a latencias como por ejemplo la utilización de un servicio de *streaming* como Netflix en la que es deseable contar con 5Mbps como velocidad recomendada para calidad Alta Definición (HD); y que

además es simétrica. El tiempo de respuesta de 14ms y jitter de 2.7ms están dentro del rango normal hacia la salida internacional del proveedor Telconet, tomando como referencia datos proporcionados en el Service Level Agreement (SLA) del proveedor el cual indica una latencia de 100ms para servicios de internet dedicado 1:1 como lo hace en el caso de CEDIA y un tiempo de respuesta de 28ms y jitter de 15ms para la red nacional MPLS para una Clase de Servicio (CoS) Premium, siendo la más alta.

Adicionalmente, nos muestra la ubicación desde donde se está realizando la toma de muestra, lo que se confirma con la sección “Ubicación del punto de toma de muestra”.



Figura 31. Prueba velocidad

Servicios disponibles

Para la prueba de servicios disponibles se realizan visitas a varios sitios de internet que contienen alto contenido multimedia, como YouTube® para video en alta definición: 4K, 1080p HD, 720p HD, etc. y cámaras en vivo desde <https://www.skylinewebcams.com/es/webcam/ecuador/tungurahua/banos-de-agua-santa/banos-de-agua-santa.html>

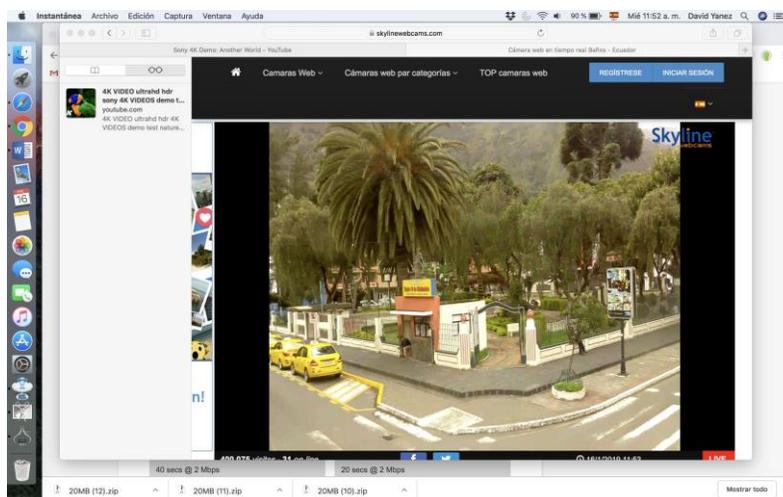


Figura 32. Prueba de streaming en vivo

Las pruebas descritas se las realizan en un ambiente interior considerando que es un lugar destinado para la comunidad estudiantil y su desarrollo de actividades académicas.

Existe una variación de 15dBm al pasar al interior de una de las aulas por efectos de degradación de la pared existente hacia el pasillo. Sin embargo, no es un obstáculo que afecte en el desempeño de la WLAN ya que aún se mantiene dentro del rango idóneo: -40 a -59 dBm. Los equipos utilizados al interior se ubican en el techo de los pasillos y oficinas, contando con seguridad contra manipulación de estos o posibles robos:



Figura 33. Punto de acceso interior



Figura 34. Punto de red para punto de acceso interior

Descripción del peor escenario

Las zonas como peor escenario se toman en cuenta donde existe un nivel de señal de -80dBm o menor considerado como sin señal en donde se realiza el escaneo de redes. Dado que no existirá conectividad, los resultados a tabular serán los de fuera de rango, y se registrarán con el fin de poder ubicarlos en el mapa virtual.

Descripción de Puntos Aledaños

Se consideran los puntos 19 a 50 como puntos aledaños a los lugares designados para desarrollo de actividades netamente académicas para la comunidad estudiantil, como patios, pasillos, comedores, en los que no es imperativo que se tenga cobertura. Esto, con el fin de poder detallar el mapa virtual. También se tiene en cuenta que existen lugares en los que se dispuso puntos de acceso para exteriores como parte de la solución inalámbrica y que van a ampliar la cobertura en ciertas zonas como la cancha principal de fútbol y el bar y su comedor, a los que se llega por fibra óptica que actúa como un cable LAN y así poder ampliar la red.



Figura 35. Punto de acceso exterior



Figura 36. Armario y fuente de poder

4. Capítulo IV: Tabulación de muestras (resultados)

Para la tabulación de las muestras, se ha tomado en cuenta que, dentro de los dos escenarios anteriormente descritos, existen puntos en los que existe diferente nivel de señal recibida y han sido ingresados en tablas. Dentro de éstas, se ha registrado información de cada punto, en base al Plan de Pruebas, entre los que constan: la ubicación del punto mediante coordenadas GMS (grados, minutos, segundos), una descripción del punto, el tipo de conexión con la que se realiza el registro a la red (estándar IEEE 802.11), el nivel de señal recibido, la calificación del rango de calificación según los requerimientos de la UTIC, resultados de medición de la prueba de capacidad del canal (velocidad de transmisión de datos), el tiempo de descarga del archivo de prueba y un breve resumen de los servicios disponibles hacia Internet, y se han resumido en la siguientes tablas:

Tabla 5.
Tabulación de datos

Orden	Ubicación			Descripción	Tipo de conexión	Nivel de señal		Rango	WiFi Analyzer	
	Latitud	Longitud	[msnm]			[GHz]	[dBm]			[%]
Exterior	1	0°18'47"S	78°26'40"O	2510	Idiomas/CENCINAT	2,4	-63	37	Bueno	Si
	2	0°18'46"S	78°26'42"O	2510	Pasillo bloque D y CENCINAT	2,4	-63	37	Bueno	Si
	3	0°18'46"S	78°26'43"O	2500	Pasillo bloque MED y A1	2,4	-68	32	Bueno	Si
	4	0°18'46"S	78°26'44"O	2500	Pasillo bloque A1 y Biotecnología	2,4	-77	23	Bajo	Si
	5	0°18'43"S	78°26'45"O	2500	Pasillo bloque Biotecnología y bloque C1	No existe cobertura	-99	0	Sin Señal	Si
	6	0°18'45"S	78°26'45"O	2510	Pasillo bloque H, bloque B1 y canchas	2,4	-75	25	Bajo	Si
	7	0°18'49"S	78°26'45"O	2500	Pasillo bloque C y bloque B	2,4	-79	21	Bajo	Si
	8	0°18'51"S	78°26'45"O	2500	Mesas entre edificio central y bar	2,4	-60	40	Bueno	Si
	9	0°18'53"S	78°26'47"O	2490	Gradas FIGMA	No existe cobertura	-99	0	Sin Señal	Si
	10	0°18'54"S	78°26'44"O	2530	Bar	5	-46	54	Idóneo	Si
	11	0°18'52"S	78°26'40"O	2510	Descanso superior patio de actos	2,4	-67	31	Bueno	Si
	12	0°18'50"S	78°26'37"O	2500	Entrada biblioteca	2,4	-70	30	Bajo	Si
	13	0°18'51"S*	78°26'21"O	2500	Entrada bloque E	2,4	-47	53	Idóneo	Si
	14	0°19'0"S	78°26'43"O	2490	Secc. sur cancha de fútbol	5	-62	38	Bueno	Si
	15	0°18'57"S	78°26'39"O	2490	Secc. este cancha de fútbol	5	-47	53	Idóneo	Si
Interior	16	0°18'48"S	78°26'39"O	2500	Idiomas/CENCINAT	5	-61	39	Bueno	Si
	17	0°18'47"S	78°26'42"O	2500	Bloque A	5	-55	45	Idóneo	Si
	18	0°18'51"S*	78°26'21"O	2510	Bloque E	5	-50	64	Idóneo	Si

CONTINUÍA

	Orden	Netspot		Speed test		Tiempo descarga 20MB [seg.]	Servicios disponibles			Otros	
		modo	ruido	Descarga	Carga		Video	Voz	Streaming		
Exterior	1	n	-101	5,06	2,44	47,77	Si	480p y 720p	Si	Si	
	2	n	-97	La prueba no se completa		66,00	No	15 segundos de espera para carga	No	No	
	3	n	-97	4,56	5,08	50,50	Si	480p y 720p	Si	Si	La calidad de video sube a los 45 segundos
	4	n	-95	4,39	0,53	90,00	Si	480p y 720p	Si	Si	Móvil no logra establecer una conexión. En portátil calidad de video sube a los 40 segundos.
	5	ninguno	0	0,00	0,00		No				
	6	b/g/n	-96	2,37	0,49	96,00	Si	360p	Robotizado	Pixelado	No se encuentran redes en 5GHz
	7	n	-88	0,00	0,00	1200,00	No	No	No	No	A pesar de tener conectividad, las pruebas no se logran completar.
	8	n	-90	4,19	5,01	48,18	Si	720p	Si	Si	Calidad de video sube a los 10 s.
	9	ninguno	-90	0,00	0,00		No				
	10	ac	-89	4,31	4,51	47,50	Si	720p	Si	S	Lugar concurrido
	11	n	-96	0,26	0,21	900,00	No				La descarga del archivo no logra completarse
	12	n	-92	3,97	3,43	51,50	Si	720p60HD	Si	Si	
	13	n	-96	4,40	5,12	47,00	Si	720p60HD	Si	Si	

CONTINÚA

	14	ac	-89	4,60	4,25	89,49	Si	720p60HD	Si	Si	
	15	ac	-96	5,40	4,73	37,40	Si	720p60HD	Si	Si	Debido a la lluvia del día anterior a la prueba, el AP se encontraba con problemas
	16	ac	-89	5,33	5,07	36,40	Si	720p60HD	Si	Si	2.4GHz tiene mayor nivel de señal, pero se conecta a 5GHz
Interior	17	ac	-93	5,68	5,39	20,00	Si	1080pHD	Si	Si	Con alta concurrencia de estudiantes. Un muro representa 15dBm de pérdida sin afectación.
	18	ac	-93	2,34	4,32	49,69	Si	1080pHD	Si	Si	Baja concurrencia de estudiantes.

Tabla 6.
Resumen de puntos aledaños

	Orden	Ubicación		Descripción	Nivel de señal		Rango	WiFi Analyzer
		Latitud	Longitud		[dBm]	[%]		
Aledaños	19	0°18'50.10"S	78°26'37.90"O	Biblioteca interior	-43	57	Idóneo	Si
	20	0°18'48.60"S	78°26'40.40"O	Idiomas	-65	35	Bueno	Si
	21	0°18'47.40"S	78°26'41.00"O	CENCINAT	-71	29	Bajo	Si
	22	0°18'48.40"S	78°26'41.60"O	Patio de los patos	-68	32	Bueno	Si
	23	0°18'47.70"S	78°26'42.30"O	Patio de los patos	-68	32	Bueno	Si
	24	0°18'48.49"S	78°26'41.37"O	Bloque D	-69	31	Bueno	Si
	25	0°18'48.49"S	78°26'41.37"O	Bloque D	-60	40	Bueno	Si
	26	0°18'45.80"S	78°26'43.30"O	Bloque D	-58	42	Idóneo	Si
	27	0°18'48.8"S	78°26'42.50"O	Patio de los patos	-75	25	Bajo	Si
	28	0°18'48.20"S	78°26'42.80"O	Patio de los patos	-67	33	Bueno	Si
	29	0°18'47.50"S	78°26'43.10"O	Entrada Bloque D	-65	35	Bueno	Si
	30	0°18'47.00"S	78°26'43.50"O	Bloque H	-58	42	Idóneo	Si
	31	0°18'46.20"S	78°26'44.30"O	Bloque H	-61	39	Bueno	Si
	32	0°18'49.90"S	78°26'43.20"O	Bloque B	-74	26	Bajo	Si
	33	0°18'49.2"S	78°26'43.3"O	Bloque B	-74	26	Bajo	Si
	34	0°18'48.20"S	78°26'43.30"O	Bloque C	-65	35	Bueno	Si
	35	0°18'47.80"S	78°26'44.70"O	Bloque C	-47	53	Idóneo	Si
	36	0°18'47.00"S	78°26'44.70"O	Bloque H	-66	34	Bueno	Si
	37	0°18'49.50"S	78°26'43.80"O	Bloque B	-56	44	Idóneo	Si
	38	0°18'48.5"S	78°26'44.50"O	Bloque B	-70	30	Bajo	Si
	39	0°18'48.20"S	78°26'45.20"O	Bloque C	-63	37	Bueno	Si
	40	0°18'47.70"S	78°26'45.40"O	Bloque C	-63	37	Bueno	Si
41	0°18'50.40"S	78°26'43.80"O	Edificio Central	-61	39	Bueno	Si	
42	0°18'49.30"S	78°26'45.20"O	Bloque B	-48	52	Idóneo	Si	

CONTINÚA

43	0°18'49.20"S	78°26'46.70"O	Canchas bloque B	-80	20	Sin Señal	Si
44	0°18'51.50"S	78°26'43.60"O	Bloque A	-48	52	Idóneo	Si
45	0°18'51.50"S	78°26'42.40"O	Bloque A	-49	51	Idóneo	Si
46	0°18'51.00"S	78°26'41.80"O	Patio central	-61	39	Bueno	Si
47	0°18'52.20"S	78°26'41.30"O	Patio central	-53	47	Idóneo	Si
48	0°18'51.00"S	78°26'40.90"O	Patio central	-68	32	Bueno	Si
49	0°18'53.20"S	78°26'40.30"O	Patio central	-82	18	Sin Señal	Si
50	0°18'51.10"S	78°26'40.00"O	Patio central	-77	23	Bajo	Si

4.1. Representación gráfica de resultados (mapa)

Se ha considerado el uso de herramientas de posicionamiento global GPS para ubicar los puntos de muestra sobre un mapa virtual, utilizando varias capas con lo que se ha logrado virtualizar la cobertura de la WLAN, según el nivel de señal recibida en las áreas del campus, de la siguiente manera:

Tabla 7.

Representación gráfica de puntos

Parámetro	Rango [dBm]	Color	Ícono
Idóneo	-40 a -59	Verde	
Bueno	-60 a -69	Amarillo	
Bajo	-70 a -79	Blanco	
Sin señal	-80 o menos	Rojo	

El mapa ha sido desplegado en el sitio <https://goo.gl/8jxHM7> al cual se puede acceder para ver las capas sobre un mapa de Google Maps®, e inclusive considerar que en un futuro se la pueda difundir como una herramienta de guía para los actuales usuarios. El mismo también puede ser compartido por medio del archivo tipo kmz que se puede visualizar desde la aplicación de Google Earth®.

Dentro de esta herramienta se ha logrado construir las áreas de cobertura, en base a las mediciones realizadas, tomando en cuenta las áreas en donde se despliega la infraestructura.

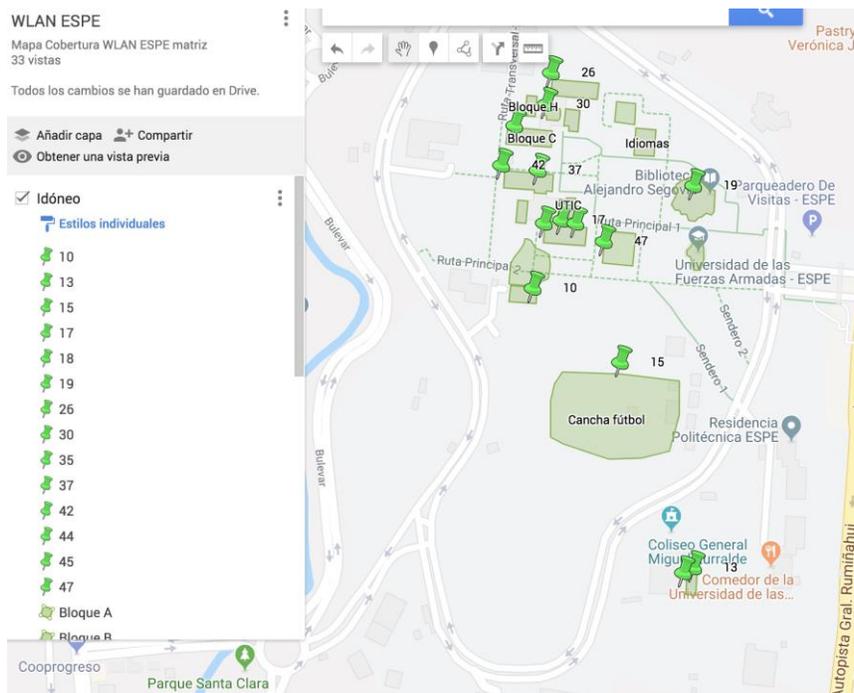


Figura 37. Construcción de mapa de calor - Capa Idóneo

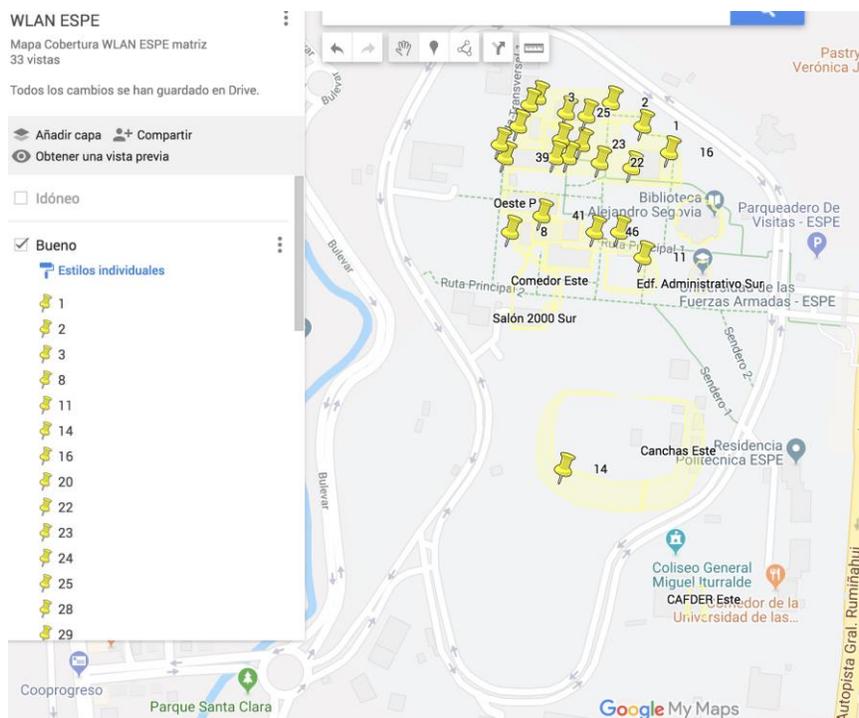


Figura 38. Construcción de mapa de calor - Capa Bueno

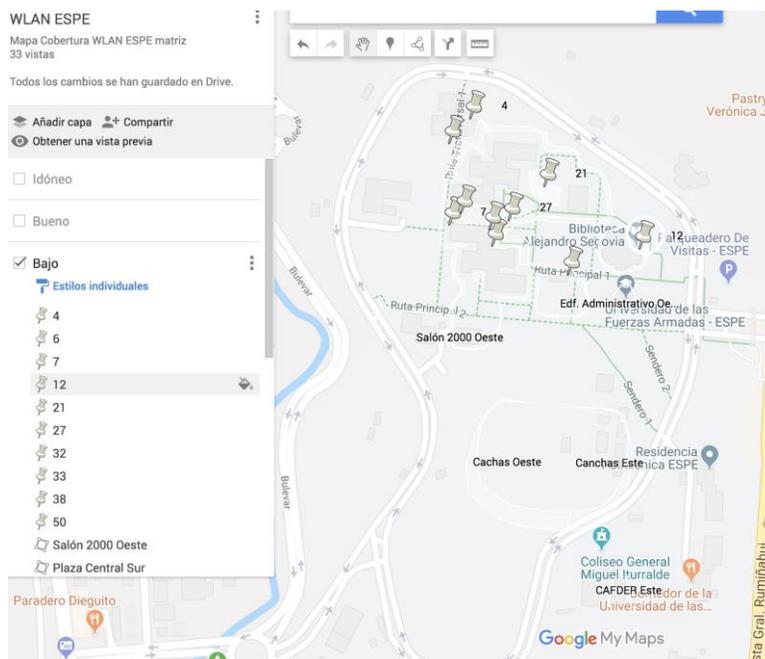


Figura 39. Construcción de mapa de calor - Capa Bajo

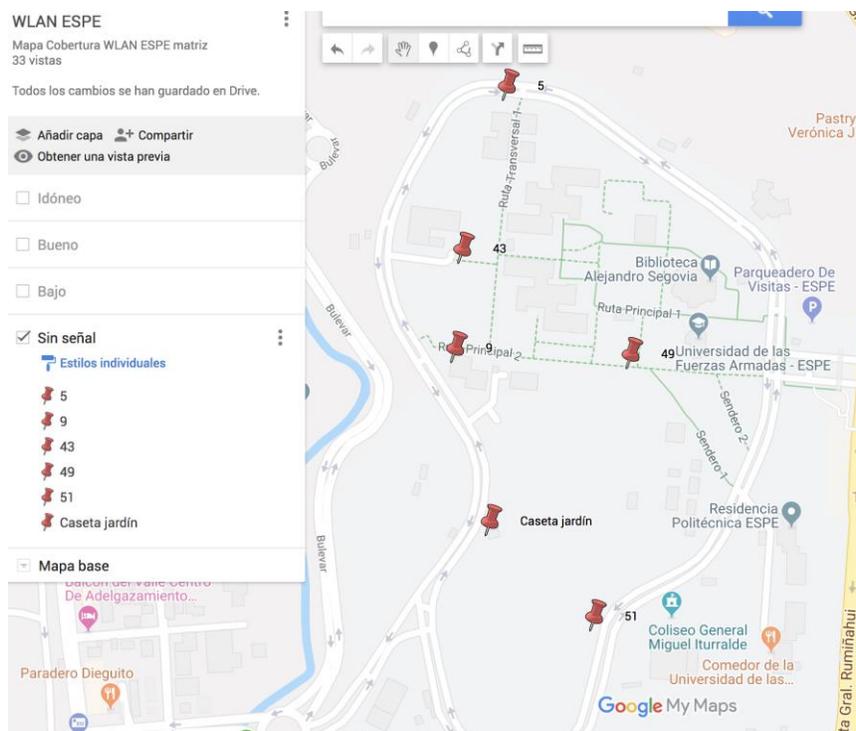


Figura 40. Construcción de mapa de calor - Capa Sin Señal

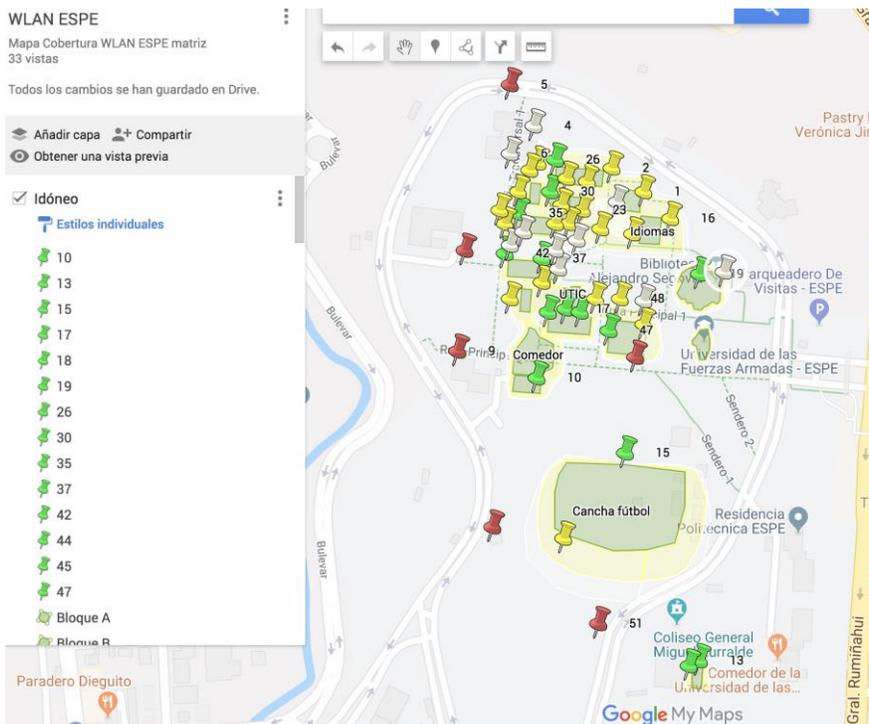


Figura 41. Construcción de mapa de calor - Todas las capas

La siguiente imagen nos muestra un vistazo del mapeo resultante de la ubicación de varios puntos estratégicos de la WLAN en el campus, con la utilización de Google Earth®

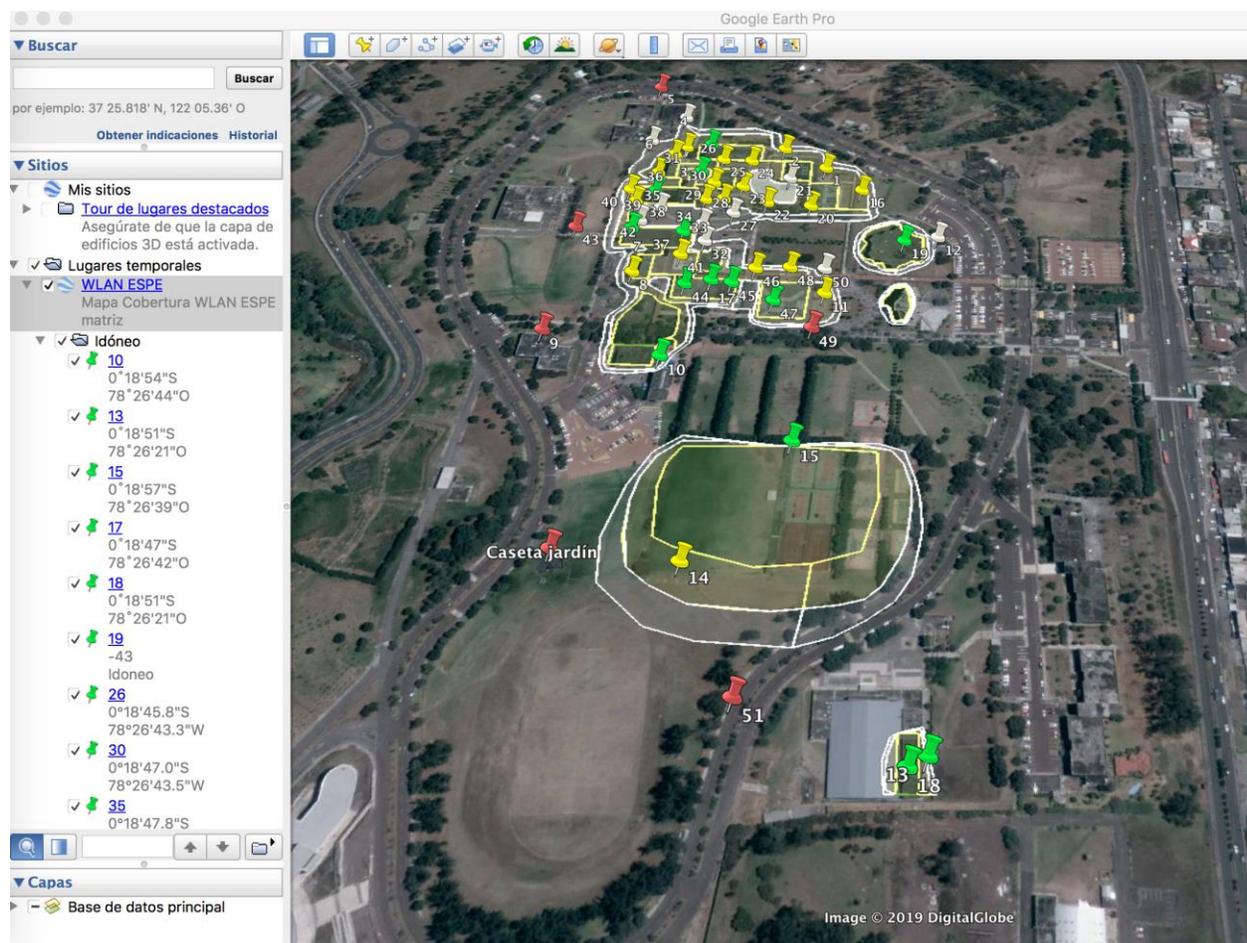


Figura 42. Resultado sobre un mapa 3D sobre Google Earth



Figura 43. Resultado capa Idóneo sobre Google Earth

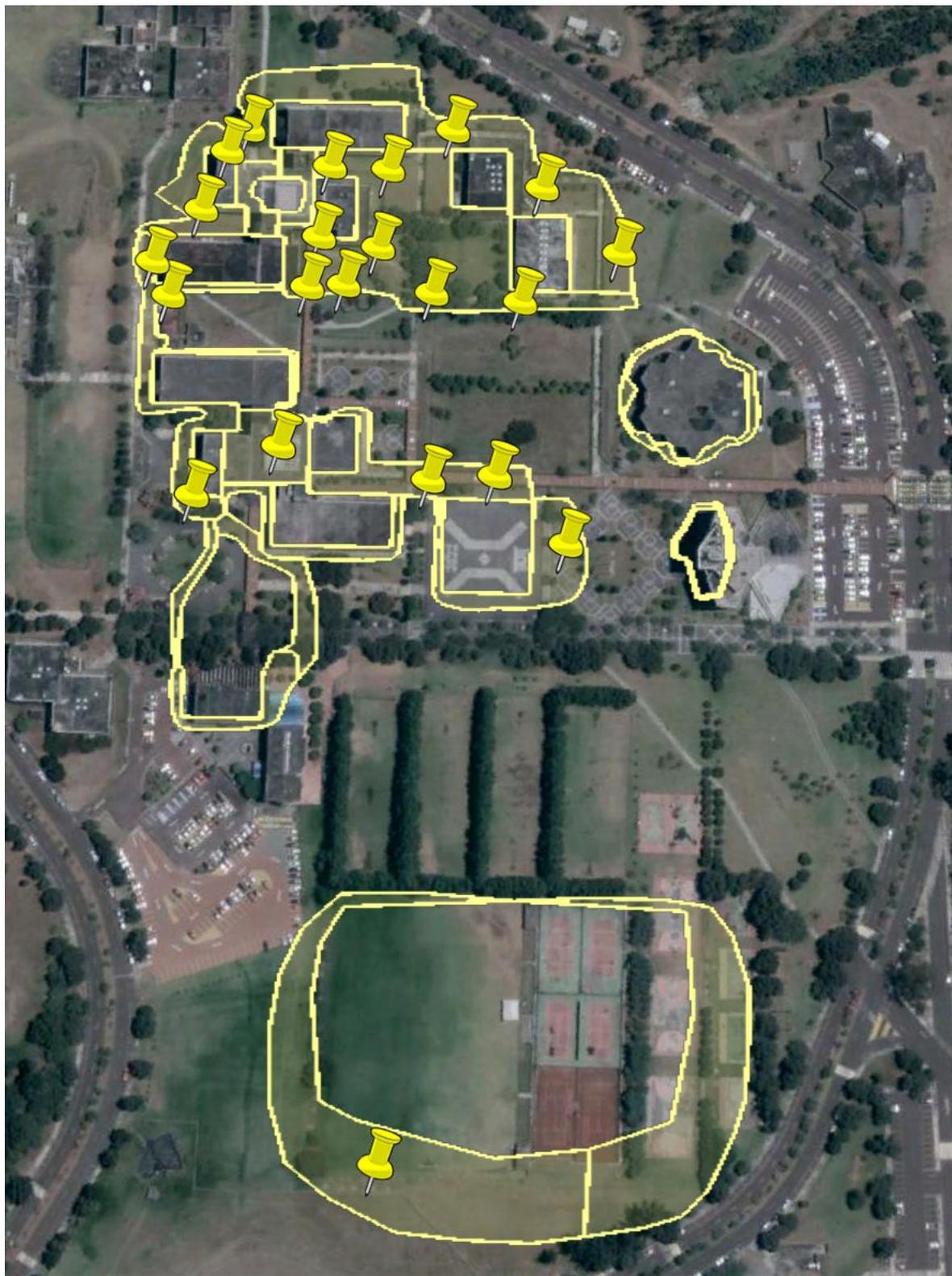


Figura 44. Resultado capa Bueno sobre Google Earth

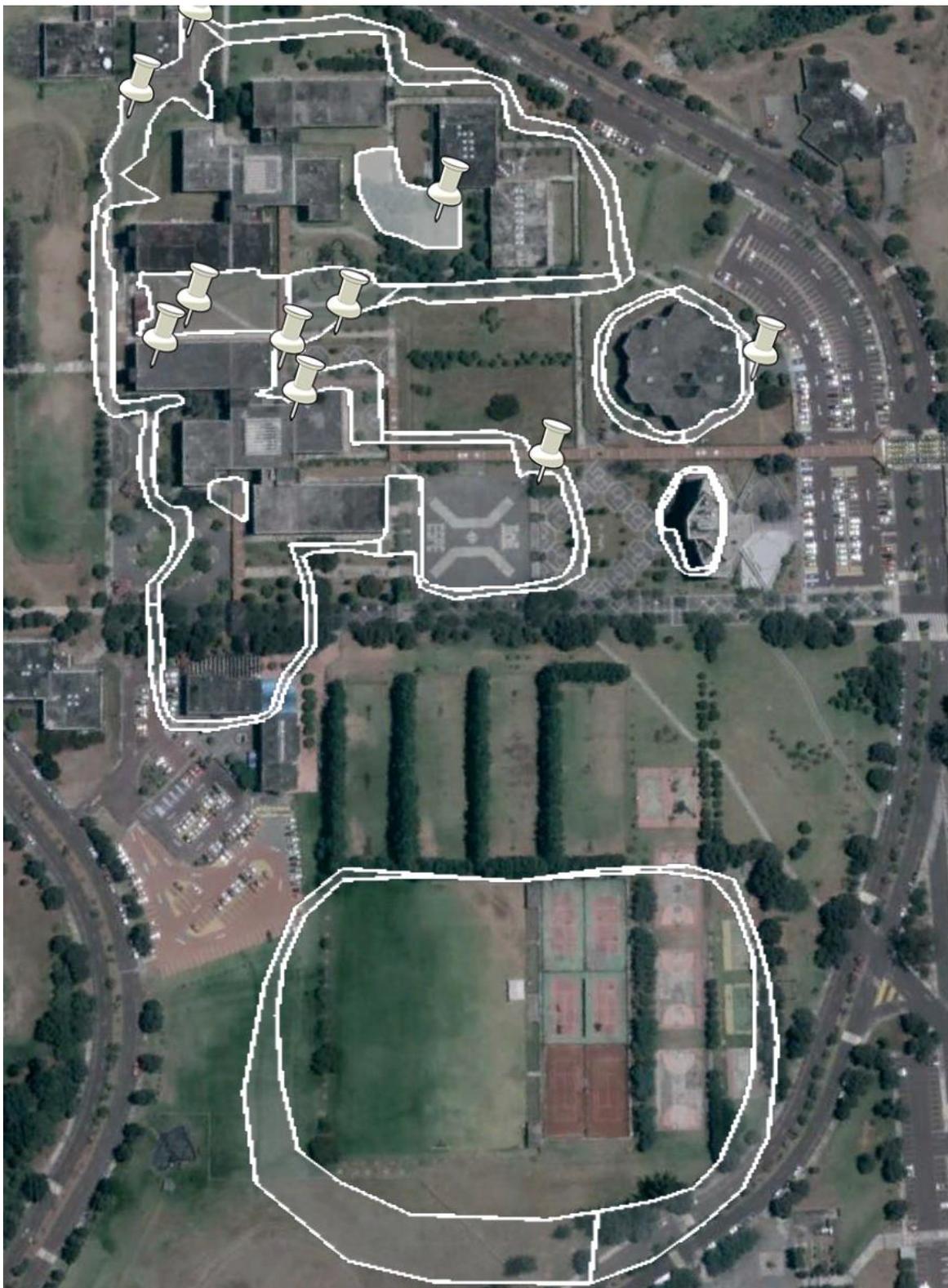


Figura 45. Resultado capa Bajo sobre Google Earth



Figura 46. Resultado capa Sin Señal sobre Google Earth



Figura 47. Resultado todas las capas sobre Google Earth - CAFDER

4.2. Muestras complementarias

Con el fin de agregar valor a las pruebas ejecutadas y a la vez poder contrastar resultados, se realizaron mediciones adicionales con la ayuda de software especializado en mapas de calor como Ekahau HeatMapper y la versión de *Survey* de NetSpot en base a planos del campus que presentan mejor calidad en cuanto a detalle.

Sector exterior

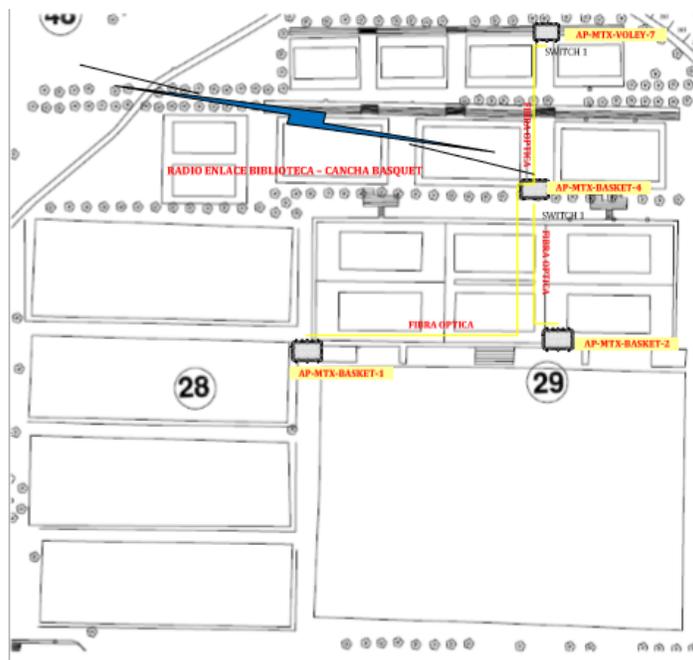


Figura 48. Plano base sector canchas

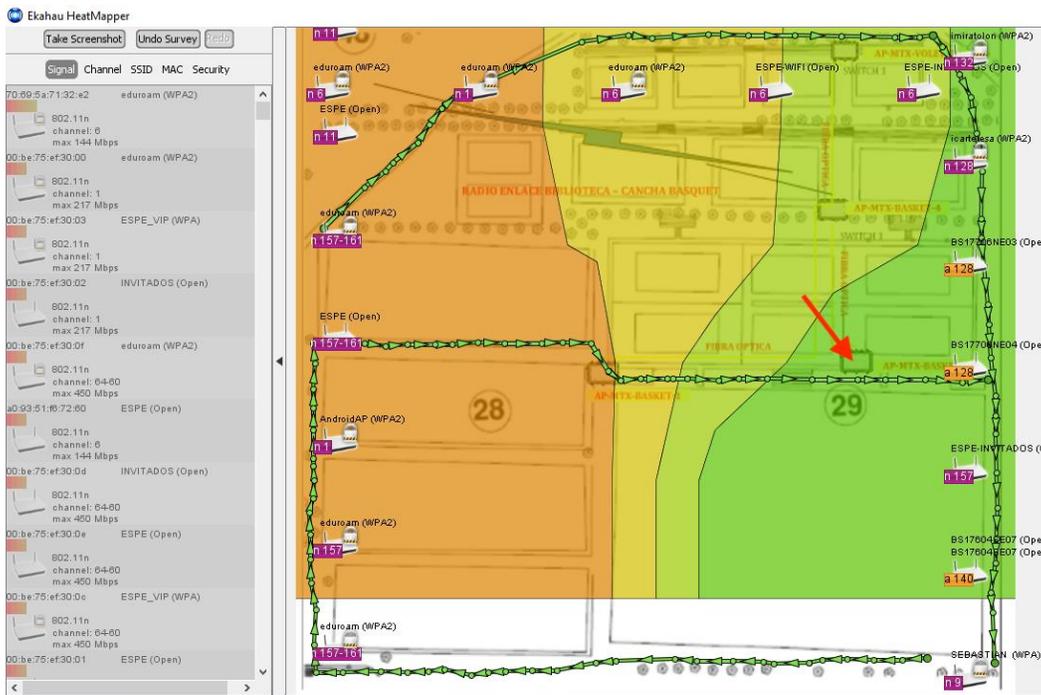


Figura 49. Mapa de calor con Ekahau - canchas

Con Ekahau se validó el comportamiento de cada punto de acceso. Por ejemplo en la figura anterior se puede visualizar el campo irradiado por el AP señalado por la flecha roja simulando su orientación.

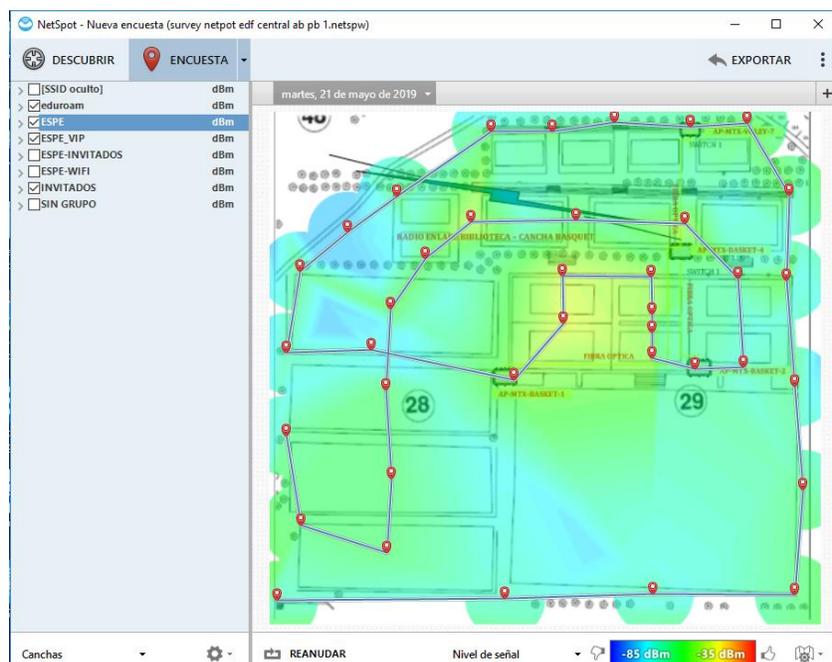


Figura 50. Mapa de calor con NetSpot - canchas

Netspot Survey por otra parte, permitió configurar varios filtros como: SSIDs, dirección MAC del punto de acceso, rango de niveles de señal máximo y mínimo, como lo muestra la figura anterior para la zona de canchas.

Sector interior



Figura 51. Plano base edificio Central PB

La figura 52 permite visualizar el comportamiento de los puntos de acceso ubicados en cada extremo del pasillo del bloque A – planta baja del Edificio Central:

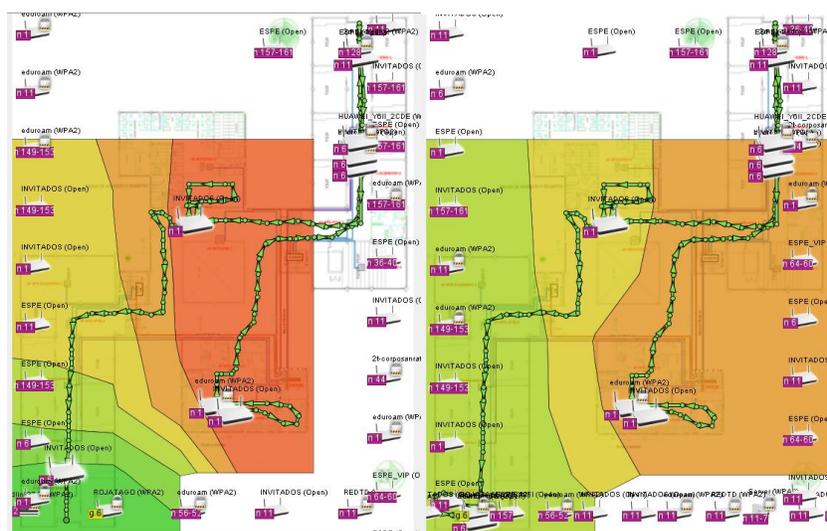


Figura 52. Mapa de calor con Ekahau - bloque A

La figura 53 permite visualizar el comportamiento del punto de acceso ubicado al extremo oeste del pasillo del bloque B – planta baja del Edificio Central. A la derecha, de manera ampliada para el mencionado sector:

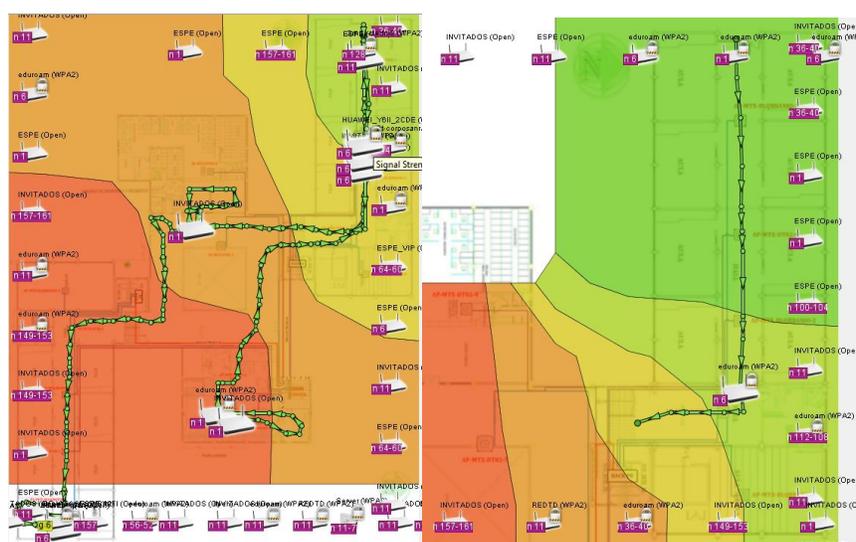


Figura 53. Mapa de calor con Ekahau - bloque B

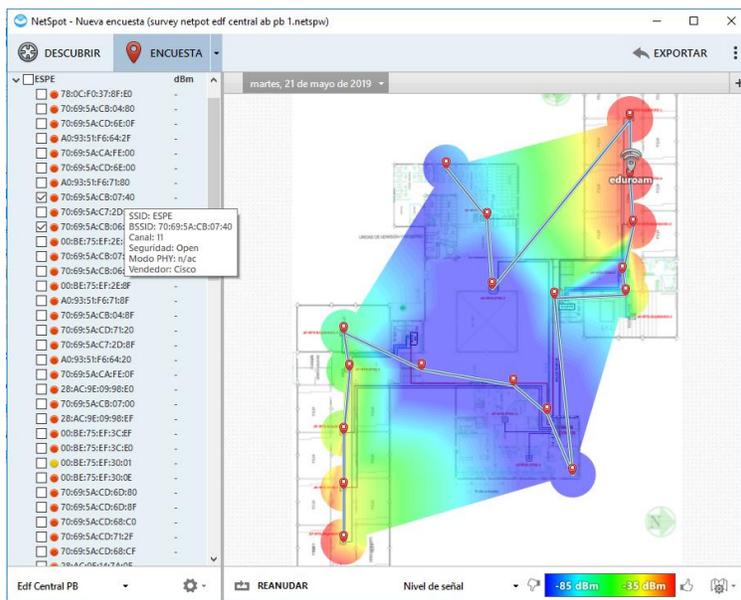


Figura 55. Mapa de calor con Netspot bloques A y B

Otra de las zonas tomadas en cuenta para comparación de resultados, fue el segundo piso de los bloques G y H:

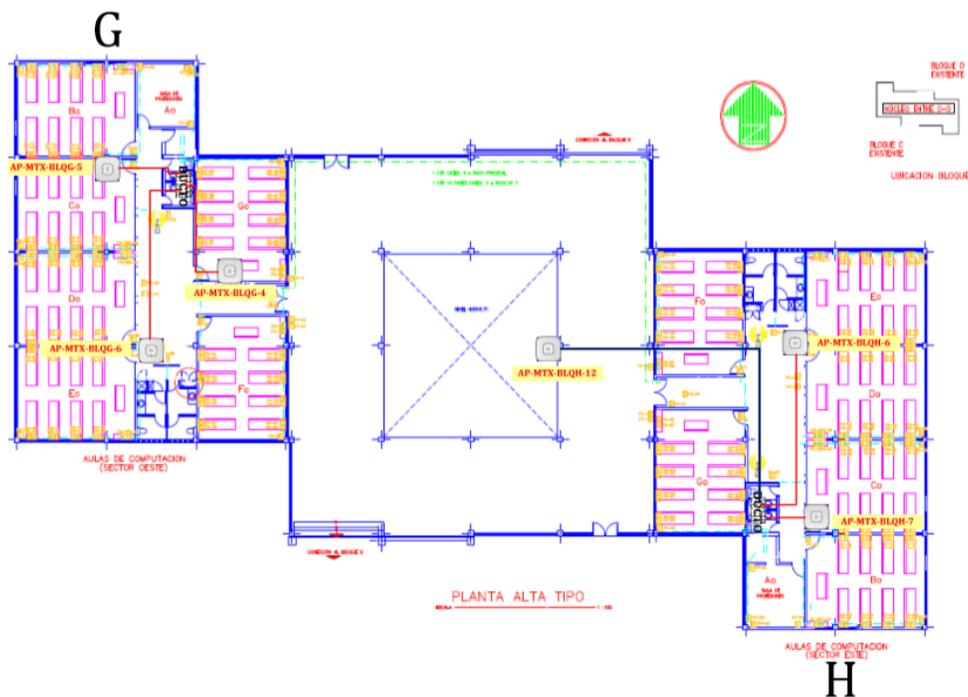


Figura 56. Plano base bloques G y H P2

Se visualiza en la siguiente imagen el resultado del escaneo de redes del sector, filtrando por los SSIDs contemplados dentro de la nueva red inalámbrica: eduroam, ESPE, ESPE_VIP e INVITADOS:

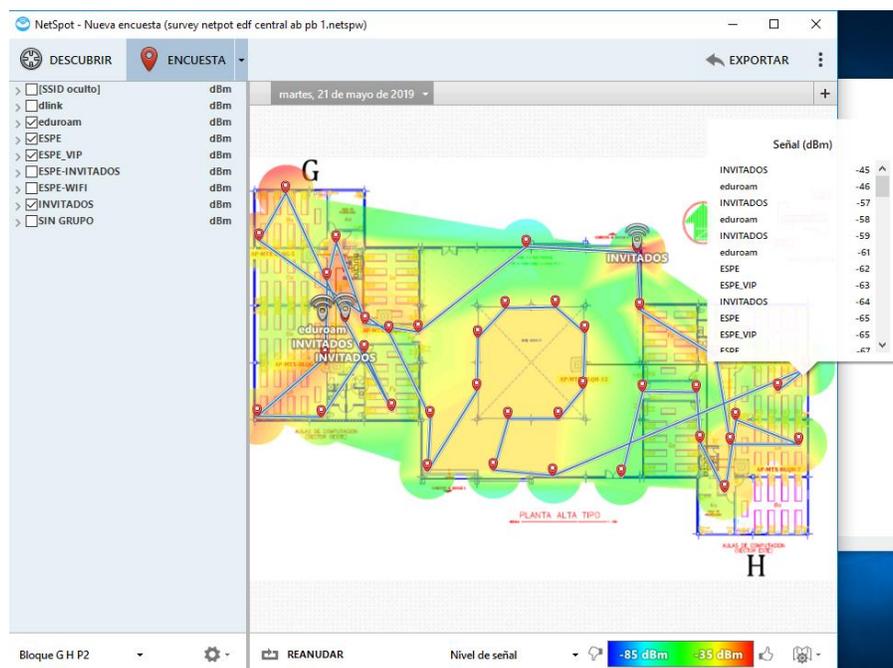


Figura 57. Mapa de calor con Netspot bloques G y H

Estadísticas desde consola de monitoreo

Desde la consola de monitoreo de la WLC se logra visualizar los siguientes datos interesantes:

En la pantalla principal nos muestra un resumen del total de dispositivos conectados, un listado de puntos de acceso operativos, las principales alarmas que aún no han sido clareadas, los SSIDs propagados, entre otros, de tal manera que al operador. Entonces, se logra capturar información en vivo durante una jornada de trabajo (lunes por la mañana).

En esta toma de datos, se determina que en la nueva red inalámbrica del campus matriz Sangolquí existen aproximadamente 4400 clientes conectados a los 4 SSIDs propagados, de la siguiente manera:

Tabla 8.
Clientes por SSID y por estándar

		Clientes
SSID	ESPE	2513
	INVITADOS	1766
	eduroam	77
	ESPE_VIP	29
Estándar IEEE 802.11	a	1
	b	0
	g	7
	an	0
	ac	0
	bn	0
	b/g/n	3639
	a/n/ac	756

4.3. Encuesta de uso de servicios de la red inalámbrica

Con el fin de poder tomar una visión alterna y paralela sobre la apreciación del desempeño de la nueva red inalámbrica, se realizó una encuesta con preguntas de conocimiento general a los tres principales grupos de usuarios del servicio del campus Matriz como tamaño de la población, apoyado en la base de datos de la Universidad como marco de muestra, actualizada a febrero de 2019:

Tabla 9.
División de población entrevistada

Grupo involucrado	Cantidad	Representación [%]
Estudiantes hombres y mujeres	9063	79
Docentes tiempo completo y medio tiempo	1921	17
Administrativos: Código del trabajo, Servidores Públicos y Pasantes	444	4
Total	11428	100

Cálculo del tamaño de la muestra:

Conociendo el número de población involucrada entre los grupos de estudio, se determinó la siguiente muestra que fue distribuida aleatoriamente y de carácter anónimo entre voluntarios:

$$n = \frac{N * Z^2 * p * q}{d^2 * (N - 1) + Z^2 * p * q}$$

En donde:

N = 11428 (tamaño de la población)

Z = 1,96 (para el 95% de nivel de confianza)

P = 0.5 (probabilidad de éxito, o proporción esperada)

Q = 1-P = 0.5 (probabilidad de fracaso)

D = 10% (Error máximo admisible en términos de proporción)

$$n = \frac{11428 * 1.96^2 * 0.5 * 0.5}{0.1^2 * (11428 - 1) + 1.96^2 * 0.5 * 0.5} = 96.07$$

Desarrollo

Para cumplir con esta tarea contamos con el apoyo de Survey Monkey, una herramienta útil para toma de respuestas a una encuesta.

Para dar facilidad a los encuestados, se realizó la toma de respuestas de tres diferentes maneras:

1. Distribuyendo el enlace de la encuesta, el mismo que es <https://es.surveymonkey.com/r/DRTJ79G>

Distribuyendo el código QR de la encuesta, el mismo que es



Figura 58. Código QR encuesta

2. Invitando a los usuarios a visitar la encuesta, sobre los dispositivos utilizados para la toma de muestras.
3. Encuesta impresa, para posterior ingreso a en línea.

Encuesta

El formato de la encuesta se puede consultar en el enlace descrito anteriormente o en la [sección de Anexos de este documento](#), al final.

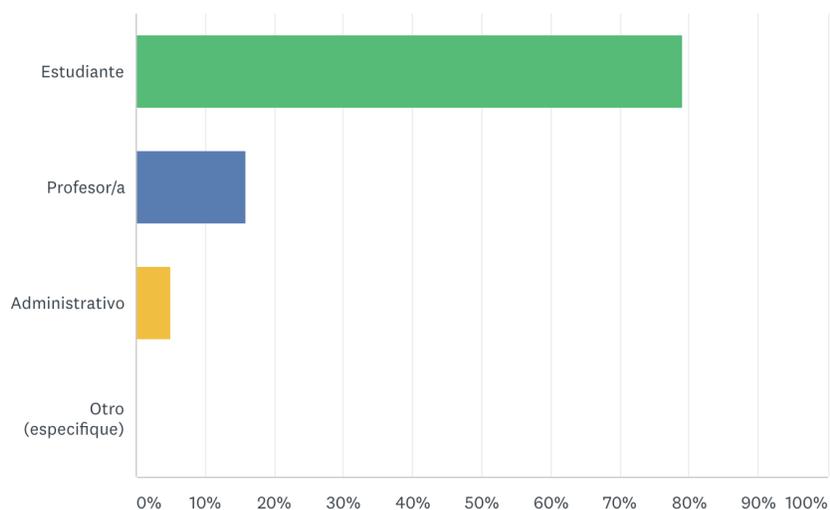
Presentación y análisis de los resultados de la encuesta

Luego de haber cumplido con el objetivo de encuestados, la encuesta arrojó la siguiente información:

Pregunta 1

Seleccione su tipo de usuario:

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
Estudiante	79,00% 79
Profesor/a	16,00% 16
Administrativo	5,00% 5
Otro (especifique)	Respuestas 0,00% 0
TOTAL	100

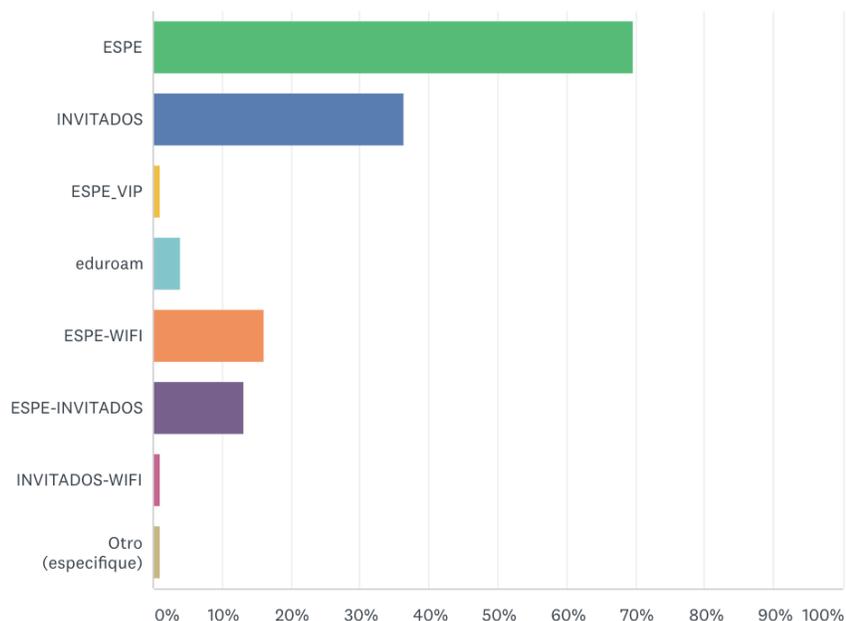
Figura 59. Resultados pregunta 1 de encuesta

Análisis: El grupo de mayoría de usuarios entre los 100 encuestados, es representado por estudiantes con un 79%, seguido por profesores con un 16% y luego por personal administrativo con un 5%. Ningún encuestado se identificó fuera de los tres grupos mencionados.

Pregunta 2

Seleccione la red inalámbrica (WLAN) a la que, principalmente, conecta su o sus dispositivos inalámbricos, para acceder a Internet y servicios de la Universidad (selecciona 1 o varias respuestas):

Answered: 99 Skipped: 3

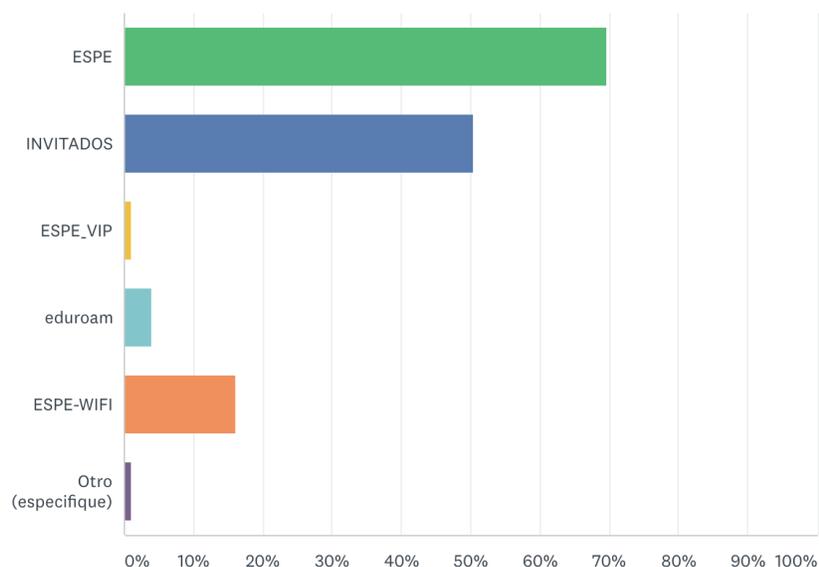


OPCIONES DE RESPUESTA	RESPUESTAS
▼ ESPE	69,70% 69
▼ INVITADOS	36,36% 36
▼ ESPE_VIP	1,01% 1
▼ eduroam	4,04% 4
▼ ESPE-WIFI	16,16% 16
▼ ESPE-INVITADOS	13,13% 13
▼ INVITADOS-WIFI	1,01% 1
▼ Otro (especifique)	1,01% 1
Respuestas	
Total de encuestados: 99	

Figura 60. Resultados pregunta 2 de encuesta

Análisis: Un 69.70% de los encuestados afirma acceder a la red inalámbrica por medio del SSID ESPE, lo cual es bueno. Más, podemos ver un 36.36% conectados a

INVITADOS, un 13.13% a ESPE-INVITADOS y un 1.01% a INVITADOS-WIFI, lo que nos da un total de 50.5%, es decir 50 usuarios que afirman mantener un enlace activo hacia una red de invitados, siendo la segunda más usada luego de ESPE, con una diferencia de 19 puntos:



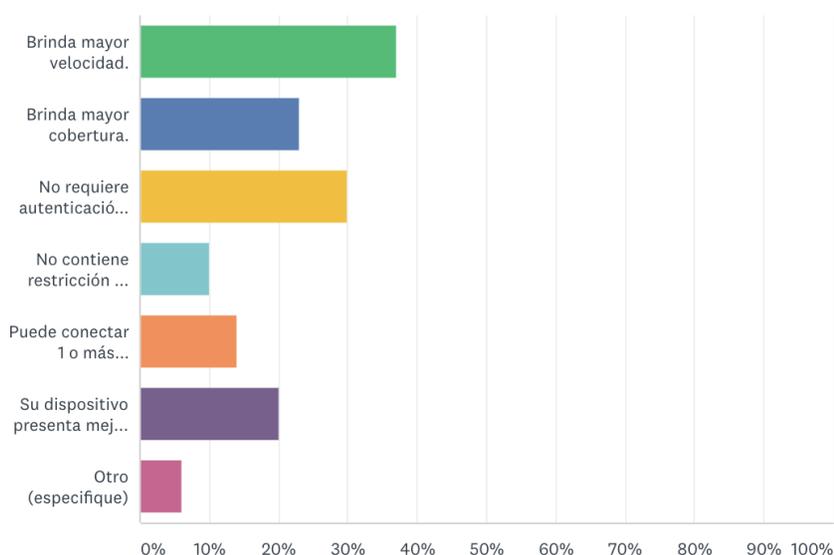
OPCIONES DE RESPUESTA	RESPUESTAS
▼ ESPE	69,70% 69
▼ INVITADOS	50,51% 50
▼ ESPE_VIP	1,01% 1
▼ eduroam	4,04% 4
▼ ESPE-WIFI	16,16% 16
▼ Otro (especifique)	Respuestas 1,01% 1
Total de encuestados: 99	

Figura 61. Combinación redes de invitados

Pregunta 3

El motivo para conectarse a la WLAN que seleccionó, es debido a que (selecciona 1 o varias respuestas):

Answered: 100 Skipped: 2

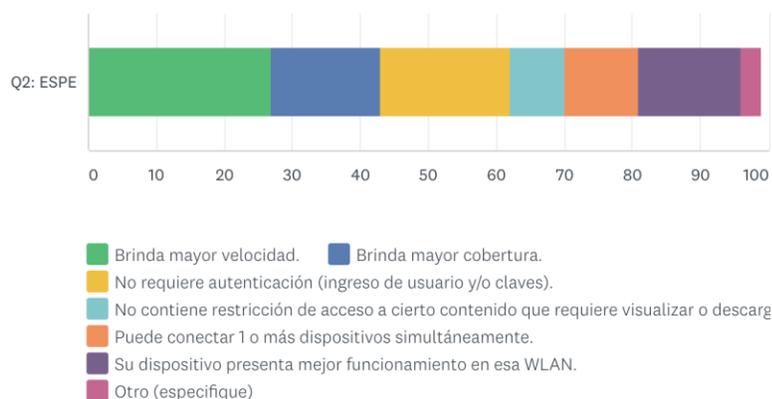


OPCIONES DE RESPUESTA	RESPUESTAS
▼ Brinda mayor velocidad.	37,00% 37
▼ Brinda mayor cobertura.	23,00% 23
▼ No requiere autenticación (ingreso de usuario y/o claves).	30,00% 30
▼ No contiene restricción de acceso a cierto contenido que requiere visualizar o descargar.	10,00% 10
▼ Puede conectar 1 o más dispositivos simultáneamente.	14,00% 14
▼ Su dispositivo presenta mejor funcionamiento en esa WLAN.	20,00% 20
▼ Otro (especifique)	Respuestas 6,00% 6
Total de encuestados: 100	

Figura 62. Resultados pregunta 3 de encuesta

Análisis: En términos generales, los resultados a esta pregunta, nos indica que el usuario utiliza la red que seleccionó por brindar mayor velocidad (37%). Este comportamiento se mantiene al revisar un poco más a fondo sobre los usuarios de ESPE, que indican que los motivos para conectarse a esta red son:

Answered: 69 Skipped: 0



	BRINDA MAYOR VELOCIDAD.	BRINDA MAYOR COBERTURA.	NO REQUIERE AUTENTICACIÓN (INGRESO DE USUARIO Y/O CLAVES).	NO CONTIENE RESTRICCIÓN DE ACCESO A CIERTO CONTENIDO QUE REQUIERE VISUALIZAR O DESCARGAR.	PUEDE CONECTAR 1 O MÁS DISPOSITIVOS SIMULTÁNEAMENTE.	SU DISPOSITIVO PRESENTA MEJOR FUNCIONAMIENTO EN ESA WLAN.
Q2: ESPE	39,13% 27	23,19% 16	27,54% 19	11,59% 8	15,94% 11	21,74% 15
Total de encuestados	27	16	19	8	11	

Figura 63. Filtrado por usuarios de ESPE

El resto de los usuarios, indican como otras opciones:

“Trabajo con mi laptop y es imprescindible usar una red WiFi.”

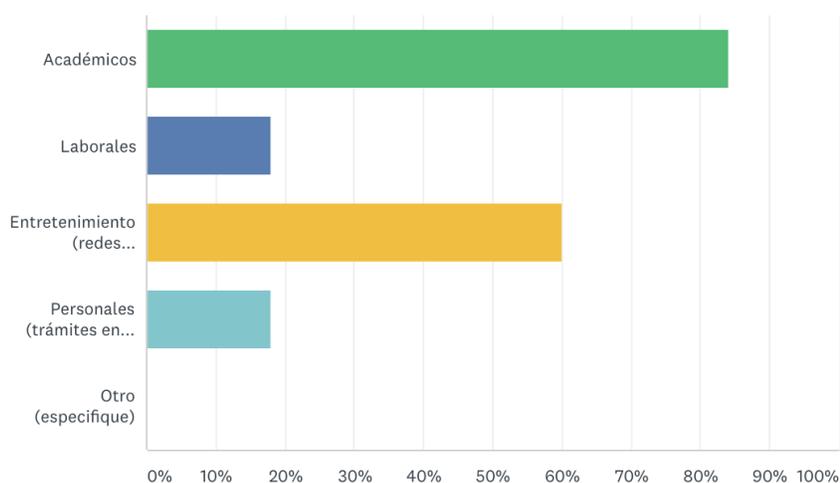
“Hay que probar cual funciona.”

“Son las únicas que existen libres.” Este comentario puede referirse a que, una vez registrados hasta dos dispositivos dentro de un mismo SSID, la autenticación se la realiza una sola vez, por usuario.

Pregunta 4

El principal objetivo para uso de la WLAN es con fines (selecciona 1 o varias respuestas):

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
Académicos	84,00% 84
Laborales	18,00% 18
Entretenimiento (redes sociales, streaming de audio/video, etc)	60,00% 60
Personales (trámites en línea en entidades financieras, de gobierno, públicas y privadas)	18,00% 18
Otro (especifique)	Respuestas 0,00% 0
Total de encuestados: 100	

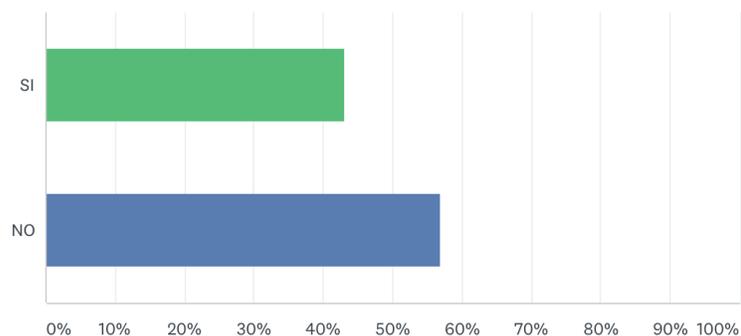
Figura 64. Resultados pregunta 4 de encuesta

Análisis: Esta respuesta confirmaría un correcto uso de los recursos de la Universidad, disponibles para los usuarios que respondieron a fines académicos con un 84%. También, un 60% indica que también utiliza los servicios inalámbricos con fines de entretenimiento, lo que podría provocar un desbalanceo en el tráfico de Internet, de no tener el respectivo control de seguridad perimetral. Compartiendo un 18%, usuarios confirman también el uso del acceso para fines laborales y personales.

Pregunta 5

Conoce las áreas con mejor desempeño de la WLAN que principalmente usa?

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
SI	43,00% 43
NO	57,00% 57
TOTAL	100

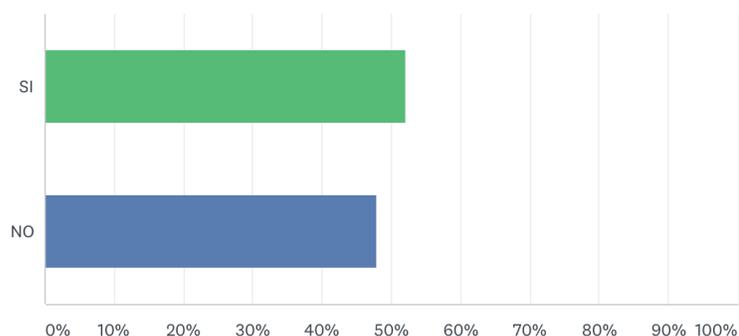
Figura 65. Resultados pregunta 5 de encuesta

Análisis: Respecto a esta pregunta, podemos ver que, la mayoría de encuestados no conoce las áreas con mejor desempeño de la red inalámbrica. Los comentarios indican que, dentro de aulas y pasillos de edificios, la red si funciona.

Pregunta 6

Conoce las áreas con peor desempeño de la WLAN que principalmente usa?

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
SI	52,00% 52
NO	48,00% 48
TOTAL	100

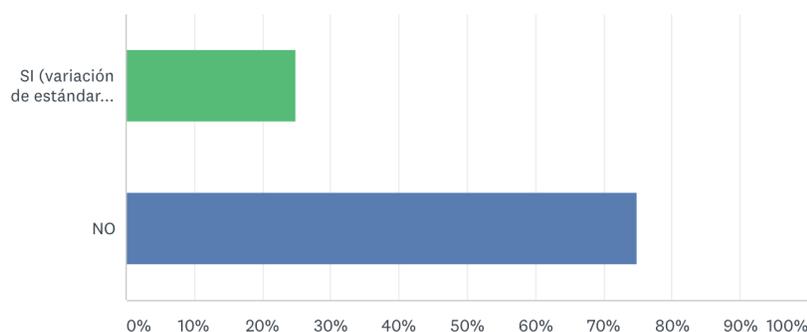
Figura 66. Resultados pregunta 6 de encuesta

Análisis: De manera contraria, a la pregunta anterior, podemos ver que la mayoría de encuestados, con un 52%, asegura que conoce las zonas muertas o en las que no es posible utilizar correctamente los servicios de la red inalámbrica. Esto puede también reflejar la apreciación del usuario de la red.

Pregunta 7

Conoce las especificaciones técnicas inalámbricas del dispositivo que utiliza?

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
SI (variación de estándar 802.11, frecuencia, velocidad)	25,00% 25
NO	75,00% 75
TOTAL	100

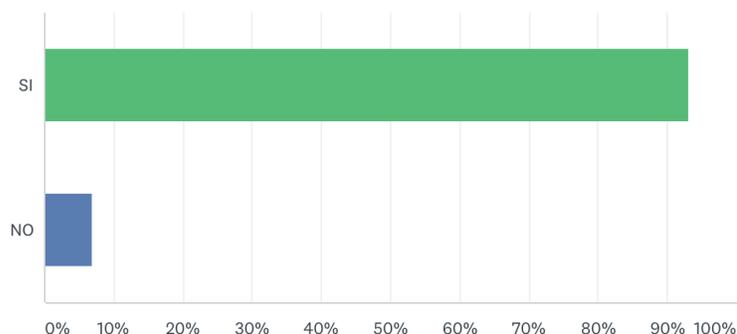
Figura 67. Resultados pregunta 7 de encuesta

Análisis: Resultó la pregunta que más causó confusión entre los usuarios de la red inalámbrica, ya que no disponen de las especificaciones técnicas de sus dispositivos. Esto arroja la cuestión de que no solo la red y su infraestructura puede provocar inconvenientes, sino que también los dispositivos del usuario final pueden causar problemas en configuraciones e incompatibilidades, a pesar de tener un abanico grande de opciones, en cuanto a compatibilidad, de los dispositivos que conforman la red: controladora, puntos de acceso, estándares. Se ha confirmado en la herramienta de monitoreo de la controladora Cisco, que existen dispositivos con estándar 802.11a que aún se conectan a la red, siendo éste un estándar con cerca de 20 años de antigüedad.

Pregunta 8

Ha tenido usted inconvenientes al momento de movilizarse por las diferentes zonas del campus, utilizando un dispositivo inalámbrico, tratando de mantener una conexión activa a la WLAN (capacidad de roaming)?

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
SI	93,00% 93
NO	7,00% 7
TOTAL	100

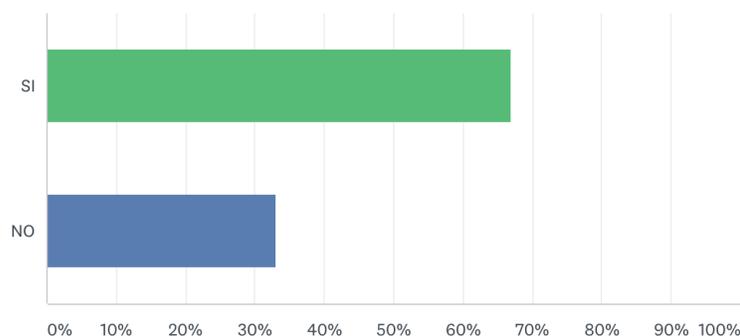
Figura 68. Resultados pregunta 8 de encuesta

Análisis: Existen dos precedentes en cuanto al diseño de la nueva implementación, para analizar este resultado. El primero, que la red tiene como objetivo principal ofrecer servicios de conectividad inalámbrica para aspectos académicos. Segundo, la densidad de usuarios calculada por zona. En conjunto estos parámetros, han dejado de lado cumplir con un 100% de cobertura dentro de los edificios, por lo que aún existen zonas con nula o poca cobertura, provocando que Roaming no esté altamente disponible.

Pregunta 9

Utiliza o ha utilizado redes inalámbricas con identificadores diferentes a los gestionados por la Universidad (ESPE, INVITADOS, ESPE_VIP, eduroam, ESPE-WIFI, ESPE-INVITADOS, INVITADOS-WIFI):

Answered: 100 Skipped: 2



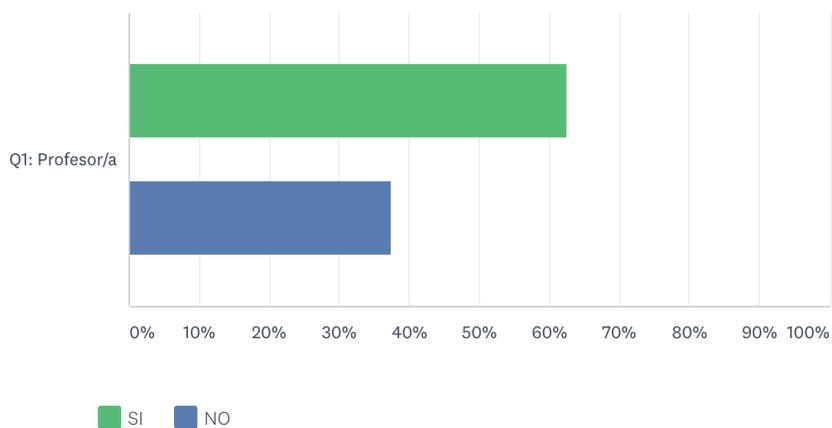
OPCIONES DE RESPUESTA	RESPUESTAS
SI	67,00% 67
NO	33,00% 33
TOTAL	100

Figura 69. Resultados pregunta 9 de encuesta

Análisis: Un 67% de encuestados afirma utilizar o haber utilizado una red inalámbrica, diferente a las gestionadas por la UTIC. Este resultado se puede confirmar con los resultados de las pruebas con WiFi Analyzer y Netspot, en las que se ha detectado que existen puntos de acceso intrusos dentro del campus, con SSIDs públicos y ocultos, inclusive sin seguridad de autenticación. La zona con mayor población de puntos de acceso intrusos es Laboratorios de Electrónica.

Filtrado por usuarios, tenemos que, los estudiantes son los que más se conectan a una red alterna, teniendo en consideración solo el parámetro de “funciona o no funciona”:

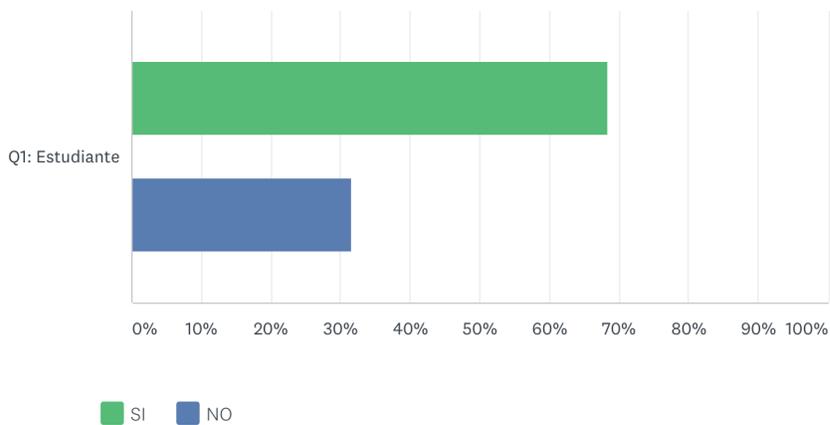
Answered: 16 Skipped: 0



	SI	NO	TOTAL
Q1: Profesor/a	62,50% 10	37,50% 6	100,00% 16
Total de encuestados	10	6	16

Figura 70. Pregunta 9 filtrado por profesores

Answered: 79 Skipped: 0



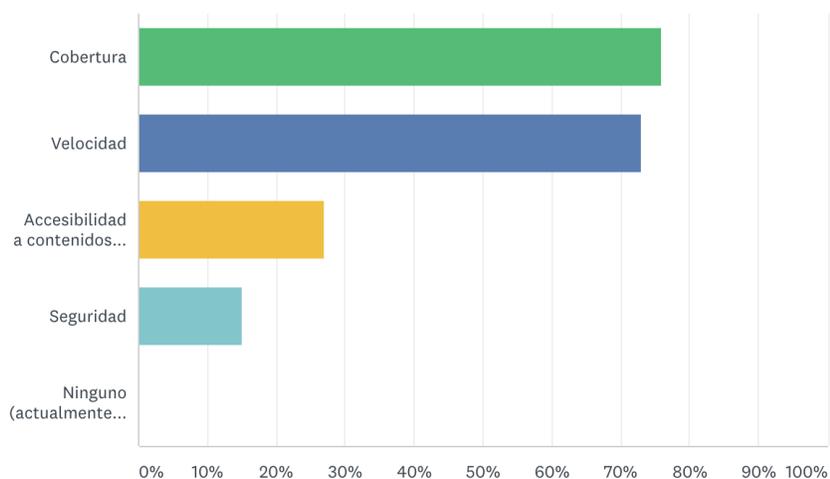
	SI	NO	TOTAL
Q1: Estudiante	68,35% 54	31,65% 25	100,00% 79
Total de encuestados	54	25	79

Figura 71. Pregunta 10 filtrado por estudiantes

Pregunta 10

Cual es el aspecto que, a su consideración, necesita mas atención sobre el desempeño actual de la WLAN que usa principalmente dentro del campus? (selecciona 1 o varias respuestas):

Answered: 100 Skipped: 2



OPCIONES DE RESPUESTA	RESPUESTAS
▼ Cobertura	76,00% 76
▼ Velocidad	73,00% 73
▼ Accesibilidad a contenidos restringidos	27,00% 27
▼ Seguridad	15,00% 15
▼ Ninguno (actualmente la WLAN que utiliza principalmente funciona de manera correcta)	0,00% 0
Total de encuestados: 100	

Figura 72. Resultados pregunta 10 de encuesta

Análisis: Un 76% de encuestados sugiere mejorar la cobertura de la red inalámbrica, lo que se podría solventar con una ampliación de los términos de contratación del servicio, provocando una mejor percepción del usuario final. También se solicita mejorar la velocidad del flujo de datos por un 73% de encuestados, pero, teniendo en cuenta que

no existe un correcto uso de los SSIDs, este porcentaje podría ser menor al utilizar los recursos correctamente. Con una minoría se solicita ampliar las restricciones a contenidos restringidos por un 27% de encuestados, argumentando que también se debe considerar contenido de entretenimiento para los estudiantes en sus tiempos libres, sobre todo contenido visual de streaming; Lo que nos lleva al siguiente 15% que solicita mejorar la seguridad, lo cual está siendo controlado por los equipos firewall para seguridad perimetral, para disminuir el consumo de ancho de banda del acceso a internet y evitar posibles ataques externos. Lamentablemente sin una política interna de regulación y control de utilización de equipos no homologados por la UTIC, no es posible elevar los niveles de seguridad internos.

5. Capítulo V: Conclusiones y recomendaciones

5.1. Conclusiones

Se ha comprobado que aún existen puntos o zonas dentro del campus, que están fuera del rango Idóneo o Bueno del nivel de señal, al no estar contemplados como zonas en las que un estudiante requerirá el acceso inalámbrico con fines académicos. Esto junto a la poca difusión de información sobre el correcto uso y manejo de los servicios inalámbricos, provoca que los usuarios se registren en cualquier red inalámbrica disponible como la red antigua, redes no manejadas por la UTIC o redes públicas o abiertas, lo que provoca que no cuenten con Roaming dentro de una misma red, una correcta respuesta de los servicios de navegación, o parámetros de seguridad o encriptación de la información transmitida/recibida.

También se ha logrado verificar que, dentro de la Universidad de las Fuerzas Armadas – ESPE existen varios Puntos de Acceso, no gestionados por la UTIC, sino por los diferentes tipos de usuarios de la red interna del campus, con SSIDs tanto visibles como ocultos, con y sin parámetros de seguridad de autenticación, y de varias tecnologías, convirtiéndolos en Puntos de Acceso Intrusos para la red inalámbrica gestionada por la UTIC.

Como consecuencia de lo expuesto en el análisis de la encuesta, queda en evidencia que, no se tiene un correcto uso de ingreso a la red inalámbrica por parte de un 50.5% de usuarios que se conectan a la red INVITADOS, ya que dicho SSID no requiere autenticación, provocando que el acceso a los servicios de conectividad muchas veces se vea limitado, al saturar esta salida, provocando tener una mala percepción de las capacidades de la red implementada.

En cuando a lo concluido con anterioridad, se puede confirmar, que los usuarios no conocen los canales de contacto para solicitar soporte por parte de la UTIC de la Universidad, y realizar un correcto proceso de autenticación e ingreso a la red inalámbrica, en caso de tener algún inconveniente con esta tarea.

Como parte de la solución de seguridad, se ha corroborado que, un mismo usuario puede ingresar sólo hasta dos dispositivos a un mismo SSID sin tener que realizar un nuevo proceso de autenticación, provocando que un tercero tenga problemas en conectividad, mientras no se desvincule el primer dispositivo que fue registrado en la red inalámbrica.

5.2.Recomendaciones

Actualmente no existen políticas de control o restricción sobre la implementación de Puntos de Acceso Intrusos dentro del campus, por lo que se recomienda contar con normas, que regulen la implementación de dispositivos propios de los usuarios, a manera de controlar la convivencia de todos los dispositivos dentro del campus, y que además eleve el nivel de seguridad de la red interna.

Se sugiere crear una campaña de difusión sobre el uso correcto de la red inalámbrica dentro de la Universidad para los diferentes tipos de usuarios, tipos de dispositivos y tipos de acceso a la red interna y externa, recalcando los beneficios personales e institucionales que representa ingresar al SSID correcto, contando con el apoyo de los grupos de difusión de la Universidad, como lo son redes sociales, radio y TV ESPE, portal Mi ESPE, correo institucional de Comunicación Social en base de contenido interactivo y multimedia. Aprovechando la campaña, se debería de asesorar a

los usuarios de la red inalámbrica, sobre los canales de contacto para solicitar soporte desde la UTIC.

De igual manera, con el equipamiento actual y las prestaciones que soporta, se debería tratar de ayudar a los usuarios a un correcto proceso de autenticación al SSID ESPE, configurando parámetros que representen una diferencia en la apreciación del desempeño de las redes, como por ejemplo, utilizando un contador de tiempo para una conexión y enlazándolo a la dirección MAC del dispositivo, con lo que la red INVITADOS cumpliría con su objetivo principal que es la de brindar acceso a un dispositivo que no sea concurrente en su actividad dentro de la Universidad.

Actualmente el uso de dispositivos inalámbricos está en auge por todos los beneficios antes mencionados, por lo que se aconseja aumentar el número máximo de dispositivos permitidos dentro de un mismo SSID para el mismo usuario, o activando la posibilidad de realizar una solicitud individual a la UTIC de la Universidad, que permita acceder a los servicios de la red inalámbrica por más de dos dispositivos simultáneamente.

En cuanto al 30% de expansibilidad, se aconseja que, se aprovechen estos recursos de una manera adecuada para lograr suplir las deficiencias en zonas con cobertura baja o nula en donde se requieren servicios de conectividad; y en caso de necesitar implementar cobertura en zonas no contempladas en el primer estudio de factibilidad, se realice una segunda fase del proyecto, para de esta manera continuar ampliando los servicios.

BIBLIOGRAFÍA

- Butler, J. (2014). *Redes Inalámbricas en los Países en Desarrollo* .
- Netkrom Group. (s/d de s/m de s/a). *AIRNET 54Mb 802.11b/g Indoor High Power Access Point* . Obtenido de NETKROM GROUP Sol.:
http://www.netkrom.com/legado/prod_airnet_54mb_indoor_highpower_accesspoint.php?item=productos&off1=indor
- Netkrom Group. (s/d de s/m de s/a). *Metro Mesh Network*. Obtenido de NETKROM GROUP Sol.: http://www.netkrom.com/legado/sol_mesh.php?item=solutions
- Danielyan, E. (s/d de s/m de s/a). CISCO. Recuperado el Enero de 2019, de IEEE 802.11 - The Internet Protocol Journal - Volume 5, Number 1:
<https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-21/ieee.html>
- Hersman, E. (12 de Mayo de 2014). *Thinking Unidirectional and Omnidirectional Antennas*. Obtenido de BRCK: <https://www.brck.com/2014/05/thinking-unidirectional-and-omnidirectional-antennas/>
- N. B., I. G., & D. W. (s/d de s/m de s/a). *UC Berkeley*. Recuperado el Enero de 2019, de Intercepting Mobile Communications: The Insecurity of 802.11:
<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>
- Wi-Fi Alliance. (s/d de s/m de s/a). *Wi-Fi Alliance*. Recuperado el Enero de 2019, de Inicio: <https://www.wi-fi.org/>
- S. K. (s/d de s/m de 2002). *IEEE Standards Association*. Obtenido de IEEE Standards Association - Documents: <https://mentor.ieee.org/802.11/documents?n=459>
- Cisco. (15 de Noviembre de 2018). *Cisco Aironet 1560 Series Outdoor Access Points*. Obtenido de Cisco Aironet 1560 Series Outdoor Access Points Data Sheet:
<https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1560-series/datasheet-c78-737416.html>
- Cisco. (12 de Octubre de 2018). *Cisco Aironet 2800 Series Access Points*. Obtenido de Cisco Aironet 2800 Series Access Points Data Sheet:
<https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2800-series-access-points/datasheet-c78-736497.html>
- Cisco. (17 de Julio de 2018). *End-User Guides*. Obtenido de Cisco Prime Infrastructure 3.2 User Guide:
https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/user/guide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide/bk_CiscoPrimeInfrastructure_3_1_0_UserGuide_chapter_0111.html
- Cisco. (18 de Septiembre de 2017). *Technical References*. Obtenido de Cisco Prime Service Catalog 12.1 Reporting Guide:
https://www.cisco.com/c/en/us/td/docs/net_mgmt/datacenter_mgmt/intel_auto/service_portal/v_12_1/reporting/guide/CiscoPrimeServiceCatalog-12-1-ReportingGuide/CiscoPrimeServiceCatalog-12-0-ReportingGuide_chapter_01.html?dtid=osscdc000283

- Cisco. (17 de Mayo de 2018). *Data Sheets*. Obtenido de Cisco Identity Services Engine Data Sheet: https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html
- Cisco. (21 de 12 de 2018). *Cisco Prime Infrastructure*. Obtenido de Cisco Prime Infrastructure Programming Guides: <https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-programming-reference-guides-list.html>
- Intel. (13 de Septiembre de 2018). *Redes Inalámbricas*. Obtenido de Diferentes protocolos de Wi-Fi y velocidades de datos: <https://www.intel.la/content/www/xl/es/support/articles/000005725/network-and-io/wireless-networking.html>
- B. M. (10 de Enero de 2019). *Internet & Network*. Obtenido de 802.11n Wi-Fi in Computer Networking: <https://www.lifewire.com/802-11n-wireless-network-818281>
- B. M. (21 de Noviembre de 2018). *Internet & Network*. Obtenido de What Is 802.11g Wi-Fi?: <https://www.lifewire.com/history-of-wireless-standard-802-11g-816556>
- A. G. (27 de Octubre de 2012). *The Lab Book Pages*. Obtenido de Delay Sum Beamforming: <http://www.labbookpages.co.uk/audio/beamforming/files/delaySum/beam.png>
- Cisco. (26 de Noviembre de 2018). *802.11ac Wave 2 Gigabit and Enterprise Wi-Fi Solutions*. Obtenido de 802.11ac Wave 2 FAQ: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html>
- techopedia. (s/d de s/m de s/a). *Networking*. Obtenido de Direct Sequence Spread Spectrum (DSSS): <https://www.techopedia.com/definition/14804/direct-sequence-spread-spectrum-dsss>
- Cisco. (s/d de s/m de s/a). *Cisco 5500 Series Wireless Controllers*. Recuperado el Enero de 2019, de Cisco 5520 Wireless Controller: <https://www.cisco.com/c/en/us/products/wireless/5520-wireless-controller/index.html>
- Universidad de las Fuerzas Armadas - ESPE. (s/d de Enero de 2019). *Portal Bienvenida*. Obtenido de Portal Cautivo: ufaslqcntise.espe.edu.ec
- Universidad de las Fuerzas Armadas - ESPE. (s/d de Enero de 2019). *Portal Cautivo*. Obtenido de Pagina Bienvenida: espe.edu.ec