

Msc (C)

NANCY EDITH OCHOA GUEVARA



- Ingeniera de sistemas, Universidad INNCA de Colombia
- Te(r).Teniente efectivo Profesional del Cuerpo Administrativo del Ejército Nacional de Colombia
- Especialista en el Diseño y Construcción de Soluciones Telemáticas, Universidad Autónoma de Colombia.
- Autora del Libro Científico “RESILIENCIA EN EL AULA VIRTUAL” y “ACCESIBILIDAD EN LA RED PARA TODOS”.
- Docente Investigadora de la Escuela Colombiana de Carreras Industriales.
- Candidata a Magister en Educación Virtual ON-LINE - Universidad Nacional Abierta y a Distancia - UNAD.
- Directora de la red de investigación RedVida, avalada por la Universidad Nacional Abierta y a Distancia - UNAD.

## REDES INALAMBRICAS ACADEMICAS EN LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - RIU-UNAD.



Actualmente, las redes de área local inalámbricas, WLAN (Wireless Local Area Network) han cobrado mucha fuerza debido, en gran medida, a las ventajas de movilidad para los usuarios y al precio competitivo que tienen en relación con las redes alámbricas convencionales. Las redes locales inalámbricas utilizan ondas electromagnéticas para transportar información de un punto a otro sin necesidad de una conexión física. Las ondas de radio frecuencia a menudo se refieren como portadoras de radio, debido a que su única función consiste en entregar la energía que conlleva al receptor remoto.

Los datos que se desean transmitir se superponen sobre la portadora de forma tal que en el lado receptor puedan ser precisamente recuperados, este proceso es conocido como "modulación de la portadora", por la información que se desea transmitir. Una vez que la portadora ha sido modulada, la señal de radio ocupa más de una frecuencia, ya que la frecuencia de la información moduladora se añade a la portadora. Pueden existir varias portadoras en el mismo espacio de forma simultánea, sin interferirse mutuamente, siempre y cuando se transmitan en diferente frecuencia. Para extraer los datos, el receptor de radio se sintoniza para seleccionar una frecuencia de radio y rechazar señales en otras frecuencias.

La ejecución del proyecto de la RIU-UNAD por fases, presentado por la Gerencia de Innovación Tecnológica y Desarrollo en el año 2008, fortalecerá la cobertura y velocidades de estas redes bajo la tecnología 802.11n para Redes Inalámbricas WI-FI, suministrando velocidades superiores a 100 mbps lo cual duplica la velocidad de 802.11g y 802.11a, que es de 54 mbps. Es un sistema muy novedoso que se basa en la tecnología MIMO (Multiple Input Multiple Output). Las ondas de RF son "Multi-Señal" y siempre existe una onda primaria y varias secundarias. Hasta ahora, sólo se aprovechaba la onda primaria y las otras eran vistas como "interferencias" o "ruidos". El algoritmo MIMO envía señal a 2 o más antenas y luego las recoge y re-convierte en una. Según la propuesta final que se adopte para el estándar Wi-Fi 802.11n funcionará en las bandas de 10, 20, o 40 MHz y se alcanzarán velocidades superiores a 100 Mbps. Estas podrían superar también los 300 Mbps. Otro tema a tener en cuenta es el alcance de la nueva tecnología, cuyas ondas de RF podrían llegar hasta casi 500 metros del emisor.

Red, Inalámbricas, Protocolos, Velocidades, Distancias, Alcances, Estudiantes, Universidades, Comunicación, Cables, Ethernet estándares, Normas.

## Abstract

Currently, the wireless local area networks, WLAN (Wireless Local Area Network) have become stronger, due mainly, to the advantages of mobility for the users and to the competitive price that they have in relationship to the conventional wire nets. The wireless local networks use electromagnetic waves to transport information, from a point to another one, without needing a physical connection. The radio frequency waves are often related to radio carriers, whose unique function consists of giving the energy they entail to the remote receiver.

The data to transmit superpose on the carrier so that in the receiving side they can indeed be recovered, this process is known like "carrier modulation", by the information that is desired to transmit. Once the carrier has been modulated, the radio signal takes up more than a frequency, since the frequency of the modulator information is added to the carrier. It might be several carriers in the same space, in a simultaneous way, without interfering mutually, as long as they are transmitted in different frequency. In order to extract the data, the radio receiver is tuned to select a RF and to reject signals in other frequencies.

The wireless networks RIU-UNAD, are an access points network (APs) installed throughout the University and which bases their operation on the communication protocols 802.11a, 802.11b, 802.11g and soon on 802.11n. They are standards developed by the IEEE (Institute of Electrical and Electronics Engineers) for the wireless communication in local area networks. 802.11b or Wi-Fi is the standard that operates in the 2.4GHz band for theoretical terminal velocities of 11Mbps (mega bps), also the standard 802.11g operates in the same 2.4GHz frequency band but for terminal velocity of 54Mbps. Finally, 802.11a is a different standard which operates in the 5.8GHz band with terminal velocities of 54Mbps. The RIU is a complement of the wire network of the Universities that allows the access to Internet, providing probability for the university student and academic community.

The execution of RIU-UNAD project by phases, presented by the Gerencia de Innovación Tecnológica y Desarrollo in 2008, will fortify the cover and speeds of these networks under the technology 802.11n for WI-FI wireless networks, having provided speeds up to 100 mbps which duplicate the speed of 802.11g and 802.11a, of 54 mbps. It is a very novel system based on MIMO (Multiple Input Multiple Output) technology. The RF waves are “Multi-Signal” and it always exists a primary wave and several secondary ones. Until now, only the primary wave took advantage and the other were seen like “interferences” or “noises”. Algorithm MIMO sends signal to 2 or more antennas and gather them soon and reconvert one. According to the final proposal adopted for the standard Wi-Fi 802.11n it will work in the bands of 10, 20, or 40 MGHZ and will reach speeds up to 100 Mbps. These could also surpass the 300 Mbps. Another subject to consider is the reach of the new technology, whose waves of RF could arrive until almost 500 meters from the emitter.

## Abstract

Network, Wireless, Protocols, Speeds, Distances, Reaches, Students, Universities, Communication, Cables, Ethernet, Standards, Norms.

## Introducción

Aunado a ello, la falta de una recomendación que permitiera la interoperabilidad entre equipos de diferentes productores, contuvo el despliegue masivo de las WLANs. No fue sino hasta mediados de la década pasada que se publicó el estándar que dictaba las especificaciones y criterios que debían aplicarse consistentemente en la fabricación y aprovisionamiento de productos inalámbricos.

## 1. Estandares WLAN

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades. Los estándares WLAN principiaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original, incluyendo 802.11a y 802.11b. La tabla No.1 contiene las variantes relacionadas al estándar 802.11.

## 2. Estándares para redes inalámbricas

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

Tabla No.1 Variantes relacionadas al estándar 802.11.

La especificación 802.11b fue ratificada por el IEEE en julio de 1999, y opera en un ancho de banda que abarca las frecuencias dentro del rango de 2.4 a 2.497 GHz del espectro de radio. El método de modulación seleccionado fue DSSS (Modulación de Secuencia Directa de Espectro Extendido) usando CCK (Modulación por Cambios de Código Complementarios), que permite una velocidad máxima de 11 Mbps. La especificación 802.11a también fue ratificada en esa fecha, pero los productos se hicieron disponibles en el mercado en el año 2001, de tal forma, que su despliegue no fue tan amplio como sucedió con 802.11b. 802.11a opera en frecuencias entre 5.15 y 5.875 GHz y utiliza el método de modulación OFDM (Multiplexación por División de Frecuencias Ortogonales), el cual hace posible velocidades de hasta 54 Mbps.

Los usuarios finales acceden la WLAN a través de adaptadores inalámbricos, implementados en tarjetas PC para computadoras portátiles (Laptops), adaptadores ISA o PCI para computadoras de escritorio (Desktops) o mediante adaptadores totalmente integrados en asistentes personales digitales (PDA, por las siglas de Personal Digital Assistant).

Los adaptadores WLAN proporcionan la interfaz entre el sistema operativo de red del cliente y las ondas electromagnéticas por conducto de la antena. La naturaleza de la conexión inalámbrica es transparente al sistema operativo de red.

Las redes inalámbricas Universitarias RIU son una red de puntos de acceso (APs) instalados a lo largo de la Ciudad Universitaria y que basan su funcionamiento en los protocolos de comunicación 802.11a, 802.11g y 802.11b ó Wi-Fi. La RIU es un complemento de la red alamburada de las Universidades que permite el acceso a la Internet proveyendo movilidad para la comunidad estudiantil y académica universitaria.

La RIU usa ondas de radio para enviar y recibir datos. Como en cualquier otra red inalámbrica, tanto los dispositivos móviles como los puntos de acceso (APs) convierten la información digital (1s y 0s) en ondas de radio, lo que permite su transmisión usando el aire como medio de transporte. La RIU opera bajo bandas de frecuencias no licenciadas o libres como son la 5.7 GHz y 2.4GHz basándose en los estándares internacionales de redes inalámbricas de área local 802.11a, 802.11b y 802.11g.

Los APs soportan los estándares 802.11 a, b y g para su comunicación inalámbrica, y el protocolo WPA para proveer mayor seguridad tanto de la información como de sus usuarios. Los sistemas operativos soportados por la RIU son Windows XP, Windows Vista, Macintosh y Linux.

### 3. Topologías

De acuerdo con la funcionalidad que se desea obtener con este tipo de redes se tienen dos configuraciones: redes Ad-Hoc (también denominadas WLANs independientes) y redes de Infraestructura. La configuración más simple de una WLAN conecta un conjunto de PCs con adaptadores inalámbricos. Cuando dos o más de estos equipos están dentro del rango de alcance de sus adaptadores pueden establecer una red independiente. Estas redes generalmente no requieren administración o preconfiguración alguna. En este tipo de redes, varios puntos de acceso enlazan la WLAN con la red alamburada, de esta forma, éstos también fungen como mediadores de tráfico hacia el vecindario inmediato. La cobertura inalámbrica puede ser extendida en un edificio completo, si así se requiere.

### 4. Costo

El despliegue de una red inalámbrica implica dos tipos de costos: el generado para la infraestructura, por los puntos de acceso inalámbricos; y el derivado de los adaptadores WLAN para los usuarios. La valía de esta tecnología depende principalmente del número de puntos de acceso, mismo que se relaciona con el área de cobertura requerida, así como el número y tipo de usuarios que serán servidos.

El costo de instalación y mantenimiento de una WLAN es generalmente menor al correspondiente a una LAN alámbrica, por dos razones: a) Elimina el costo generado por el tendido del cableado y las actividades asociadas de mantenimiento y reparación. b) Simplifica movimientos de la infraestructura, crecimientos y cambios, por consiguiente, disminuye los costos generados durante estas actividades.

### 5. Alianza Wi-Fi

La alianza Wi-Fi es una asociación internacional sin fines de lucro, formada en 1999, para certificar interoperabilidad entre productos WLAN basados en la especificación IEEE 802.11. El logotipo Wi-Fi CERTIFIED viene de la alianza Wi-Fi e indica que el producto ha cumplido con rigurosas pruebas de interoperabilidad, para asegurar que aquéllos de diferentes proveedores operen de manera adecuada en conjunto.

Otra de las actividades de esta alianza involucra el trabajo activo en la creación de nuevos y más robustos estándares de seguridad, como WPA (Wi-Fi Protected Access), así como la proliferación de hotspots (lugares públicos como cafeterías, hoteles y aeropuertos en donde el acceso WLAN está disponible, usualmente bajo alguna tarifa). Wi-Fi Protected Access es un estándar desarrollado para aumentar la seguridad de la información así como el control de acceso de los usuarios.

La RIU utiliza WPA como protocolo de cifrado para la protección de la información asegurando que sólo usuarios autorizados pueden hacer uso de la infraestructura.

## 6. Para conectarse a una RIU

Para estar en posibilidad de usar la red, es preciso contar con un dispositivo portátil como un Laptop que cuente con tarjetas de acceso inalámbricas compatibles con la red. Algunos de los estándares de comunicación soportados son 802.11a, 802.11b y 802.11g. En cuanto a seguridad el protocolo soportado puede ser el WPA. Dentro de la configuración de redes inalámbricas, es posible establecer el tipo de autenticación que se requiere. Si WPA es soportado, debiera aparecer como uno de los tipos de autenticación.

## 7. Las redes universitarias vs. Enseñanza universitaria

Las redes inalámbricas revolucionaron los métodos de enseñanza y de aprendizaje. Las nuevas tecnologías han cambiado la logística

de los universitarios. Es impresionante e incontable la nueva información que se almacena diariamente en la Red universitaria, es más, se cuenta en terabytes que es equivalente a mil gigabytes, estas redes poseen un conjunto de antenas con las que se proporciona Internet a más de 300 mil universitarios, preparatorianos, profesores, investigadores y personal administrativo. La RIU ha venido cambiando la imagen cotidiana de las Universidades, pues cada vez es más común ver a jóvenes por los campus virtuales con sus laptop, cubriendo en gran parte los territorios nacionales.

Para el investigador en desarrollo educativo, las reglas del juego tienen que cambiar. Los profesores deben valerse de las nuevas tecnologías para enseñar. "Ahora todo es más sencillo, las computadoras en clase pueden ahorrarte tiempo, en la Red hay libros digitalizados, bases de datos que enriquecen la enseñanza, siempre y cuando el alumno no abuse del Messenger o el solitario".

## 8. La tecnología Wi-Fi 802.11n

Es un sistema muy novedoso que se basa en la tecnología MIMO (Multiple Input Multiple Output). Las ondas de RF son "Multi-Señal" y siempre existe una onda primaria y varias secundarias. Hasta ahora, sólo se aprovechaba la onda primaria y las otras eran vistas como "interferencias" o "ruidos". El algoritmo MIMO envía señal a 2 o más antenas y luego las recoge y re-convierte en una. Según la propuesta final que se adopte, para el estándar Wi-Fi 802.11n funcionará en las bandas de 10, 20, o 40 MHz y se alcanzarán velocidades superiores a 100 Mbps. Estas podrían superar también los 300 Mbps. Otro tema a tener en cuenta es el alcance de la nueva tecnología, cuyas ondas de RF podrían llegar hasta casi 500 metros del emisor.

## Ventajas de la tecnología 802.11n

- El acceso inalámbrico es más rápido que otro. Aunque la velocidad de una red inalámbrica WI-FI, la fija el usuario más lento, de nada sirve tener un Access Point muy rápido si la mayoría de los usuarios son lentos.
- La compatibilidad. Obligar a una tecnología como la de 802.11n a interactuar o "juntarse" con 802.11b y 802.11g significa un gran "sacrificio" de recursos tecnológicos.
- Como se mencionó anteriormente, la transmisión de información en redes inalámbricas Wi-Fi 802.11b y 802.11g tiene lugar en la banda de 2.4 GHz, que está muy poblada y sólo se dispone de 3 canales no superpuestos con un ancho de 20 MHz por canal, por donde sube y baja la información. En 802.11n se propone utilizar canales de 40 MHz de ancho. Para compatibilizar las 2 tecnologías se "degrada" a 802.11n, perdiéndose muchas de sus ventajas. En 802.11a se trabaja en la banda de 5 GHz, mucho más despoblada y con 8 canales como mínimo para elegir, por ello, aún hay muchos que abogan por "impedir" a 802.11n que incluya la opción de funcionar en 2.4 GHz.
- Cuando se adoptaron los primeros estándares de Wi-Fi, había muy pocos "jugadores en la cancha". Básicamente era un tema de computación y de la industria del hardware. En la actualidad, debido a la convergencia que se está produciendo entre la informática, las comunicaciones y los juegos, la situación es mucho más compleja, pues en la elaboración del estándar 802.11n se han dado cita los "peces gordos" de cada mercado.

• Los fabricantes de teléfonos: La difusión de los teléfonos celulares duales GSM / WI-FI, está aumentando a pasos agigantados y dentro de un par de años se estima que todos los teléfonos celulares soportarán WI-FI. A estos fabricantes les interesa conseguir que el estándar que se apruebe no exija un gran consumo de energía, pues deben economizar en el tamaño de la batería.

## 9. Digitalizar la enseñanza en la UNAD

Las redes inalámbricas y el acceso a una computadora puede ser el futuro de las clases en el país, las Universidades tienen una demanda mayor de la que pueden cubrir. Si logramos crear una digitalización impecable y buenos métodos de enseñanza, las universidades podrían atender a más estudiantes por medio de Internet. La demanda de sitios para conectarse en lugares públicos es creciente, pues 11.5% de los cerca de 15 mil cibernautas se conectan de forma móvil en la UNAD.

## 10. Especificaciones técnicas de los equipos

Para su conexión a la RIU, los equipos móviles deben:

- Contar con sistema operativo Windows XP, MacOS X o superior y Linux.
- Contar con una tarjeta de acceso inalámbrico que soporte los protocolos 802.11a - 802.11b u 802.11g.
- Soportar el protocolo de cifrado WPA (Wi-Fi Protected Access)

## 11. Velocidad de la RIU

La RIU como cualquier red inalámbrica basa su comunicación en la transmisión de ondas de radio frecuencia entre la tarjeta de red y el punto de acceso (AP). Estas señales no son inmunes a la interferencia de otros dispositivos inalámbricos y pudieran no penetrar adecuadamente a través de ciertos materiales. Debido a estas condiciones, las velocidades, la recepción y la distancia al punto de acceso variarán con respecto a las especificadas en los estándares. Las velocidades esperadas pueden ser para los estándares 802.11 a y g de 6 a 54Mbps y para el estándar 802.11 b de 2 a 11Mbps.

## 12. Dispositivo móvil y su conexión a AP

La distancia para una conexión efectiva con un AP depende de muchos factores entre los que destacan la interferencia de otros dispositivos y las obstrucciones físicas (paredes, libreros, etc.). Con las condiciones adecuadas, si la conexión es al aire libre con línea de vista al AP, la conexión puede lograrse en 80m o más. En áreas cerradas, se puede lograr conexión a una distancia de 20 o 30m.

## 13. Seguridad en las redes inalámbricas

La RIU tiene como característica el uso del protocolo WPA que permite una mayor seguridad para el acceso a los usuarios y el cifrado de su información. Como sabemos, la seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

## 14. Interferencia en las señales de la RIU

Como cualquier red inalámbrica, otros dispositivos que operen en las frecuencias de 2.4GHz y 5.8GHz cerca de los dispositivos de conexión a la RIU pueden afectar el desempeño de la conexión e incluso terminarla. Dispositivos que operan en estas frecuencias, particularmente la 2.4GHz son teléfonos inalámbricos, hornos de microondas, cámaras y otros dispositivos.

## 15. Mecanismos de seguridad

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle. Existe el término “wardriving”, que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

## 17. Propósito de uso

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP (Wired Equivalent Privacy) es un método de cifrado para la seguridad de las redes inalámbricas, sin embargo, por la debilidad del algoritmo que puede ser descifrado relativamente fácil, no se aplica en la RIU, puede ser deducida y se puede ganar acceso no autorizado. Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica. La seguridad WLAN abarca dos elementos: el acceso a la red respectivamente), como se puede observar en la figura No.1

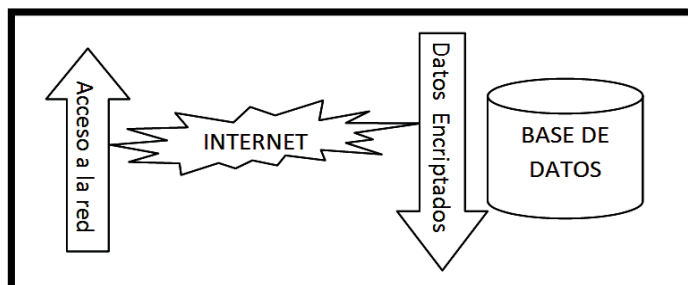


Figura No.1- Seguridad WLAN

Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquellos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos). Estos “hoyos” en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta. La tabla siguiente contiene los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

## 16. Usuarios autorizados

Son los que, previa autorización y cumplimiento de los requisitos correspondientes, tienen acceso a la RIU-UNAD y hacen uso de los servicios. Estos comprenden a los alumnos, académicos e investigadores de la Universidad así como estudiantes, académicos e investigadores invitados de otras instituciones.

En apego al quehacer de la UNAD, el uso de los recursos para estos servicios deberá estar relacionado con las actividades académicas, de investigación y difusión de la cultura.

Queda prohibido:

- El uso personal de los recursos de estos servicios que generen un costo directo a la UNAD.
- El uso simultáneo de una cuenta desde dos dispositivos móviles diferentes.
- El uso para generar ganancias monetarias personales o propósitos comerciales que no estén directamente relacionados con asuntos que la propia Universidad autoriza, difunde y solicita a la comunidad universitaria incluyendo situaciones de contingencia.
- Enviar copias de Documentos o inclusión de trabajos de otros en el correo electrónico como propios violando las leyes de derechos de autor.
- Descargar servicios broadcast, como audio y video.
- Compartirse archivos, carpetas y otros servicios (impresión, etc.).
- Usar programas "peer to peer" (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
- Extender el servicio de acceso a la RIU a más equipos por medio de una sola conexión a la red inalámbrica (ej.: por medio de NAT, túneles, conexión compartida, etc.)
- Extender el alcance de la red por medio de cualquier dispositivo físico o lógico (ej. antenas) más allá de los límites físicos de la Universidad. El acceso a la red inalámbrica se restringe al campus universitario.
- El uso del servicio para molestar, acosar, intimidar, amenazar a otros, atentar contra la integridad de los usuarios o interferir con asuntos propios de las autoridades Universitarias.
- El uso del servicio para violar las políticas de uso aceptable del correo electrónico.
- Transgredir cualquier recurso computacional, sistemas o sitios de telecomunicaciones a los que no le está permitido acceder.
- Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.

## 18. Disponibilidad del servicio

El servicio de conexión a la Red Inalámbrica Universitaria estará disponible las 24 horas del día, todos los días del año. Salvo en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos relacionados a la prestación del servicio de Internet.

## Configuración

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas, las prestaciones de unas y otras, al día de hoy, no pueden compararse. Sin embargo, la pacífica convivencia de las redes cableadas y las inalámbricas, da lugar a una nueva generación de redes híbridas que cubren por completo, según su configuración y diseño, las necesidades de conectividad tanto fija como móvil, que toda empresa moderna y competitiva requiere. Las redes inalámbricas (wireless) han venido a revolucionar el mercado de las comunicaciones no sólo de datos sino también de voz y video propiciando una integración total de medios para las empresas, las instituciones y el servicio público en general.

La RIU es un complemento de la red inalámbrica de la Universidad Nacional Abierta y a Distancia - UNAD que permite el acceso a la Internet proveyendo movilidad para la comunidad estudiantil y académica Unadista, logrando prestar un servicio de alta calidad de manera oportuna y eficaz.

La ejecución del proyecto de la RIU-UNAD por fases, presentando por la Gerencia de Innovación Tecnológica y Desarrollo en el año 2008, fortalecerá la cobertura y velocidades de estas redes bajo la tecnología 802.11n para Redes Inalámbricas WI-FI, suministrando velocidades superiores a 100 mbps lo cual duplica la velocidad de 802.11g y 802.11a, que es de 54 mbps. Es un sistema muy novedoso que se basa en la tecnología MIMO (Multiple Input Multiple Output). La llegada de la tecnología 802.11n traerá mayor velocidad y alcances en la RIU-UNAD, fortaleciendo los procesos académicos en los estudiantes, cuerpo académico, investigadores y administradores.

## Recomendaciones

Para un mejor uso de las Redes Inalámbricas Universitarias, es importante tener presente las siguientes recomendaciones:

- Utilice sitios web seguros. Los sitios seguros advierten cuando accede a ellos mostrando una leyenda que indique precisamente que está a punto de abrir un sitio seguro.
- Instale y actualice constantemente herramientas que protejan contra virus y archivos espías.
- Notifique inmediatamente el robo o extravío de su equipo o su contraseña. Hágalo también cuando sospeche que la contraseña ha sido conocida por otros.
- La compatibilidad que ofrece la tecnología 802.11n con las demás tecnologías, debe analizarse con mucho cuidado ya que por querer innovar y no realizar los cambios al ciento por ciento, se puede sacrificar las grandes ventajas de esta tecnología y se le obligaría a tomar las características de las tecnologías antiguas como la del 802.11a, 802.11b y 802.11g.

## Siglas

**AUI:** UNIDAD DE ACOPLAMIENTO DE INTERFASE.  
(ATTACHMENT UNIT INTERFASE)

**BS:** ESTACION BASE. (BASE STATION)

**CSMA/CD:** SENSOR DE MEDIO DE ACCESO MULTIPLE/CON DETECCION DE COLISION.  
(CARRIER SENSE MULTIPLE ACCESS /COLLISION DETECT) CP SEÑAL DE PRESENCIA DE COLISION.  
(COLLISION PRESENCE).

**MR:** RUTEADOR MOVIL. (MOBIL ROUTER)  
**OSI:** INTERCONEXION DE SISTEMAS ABIERTOS.  
(OPEN SYSTEM INTERCONNECTION)

**DSSS:** SECUENCIA DIRECTA DEL ESPECTRO DISPERSO (DIREC SECUENCE SPREAD SPECTRUM)

**IEEE:** INSTITUTO DE INGENIEROS ELECTRICOS Y ELECTRONICOS. (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS)

**IRMAU** UNIDAD ADAPTADORA AL MEDIO INFRAROJO. (INFRARROJA MEDIUM ADAPTER UNIT)

**ISM:** BANDAS DE APLICACIONES INDUSTRIALES, CIENTIFICAS Y MÉDICAS. (BANDS INDUSTRIAL, SCIENTIFIC AND MEDICAL)

**JAM:** SEÑAL DE PRESENCIA DE COLISION.

**KBPS:** KILO BITS POR SEGUNDO.

**LAN:** RED DE AREA LOCAL. (LOCAL AREA NETWORK.)

**LLC:** CONTROL DE ENLACE LOGICO. (LOGIC LINK CONTROL)

**MAN:** RED DE AREA METROPOLITANA. (METROPOLITAN AREA NETWORK)

**MAC:** CONTROL DE ACCESO AL MEDIO. (MEDIUM ACCESS CONTROL)

**MAU:** MEDIUM ADAPTER UNIT. UNIDAD ADAPTADORA AL MEDIO.

**MBPS:** MEGA BITS POR SEGUNDO.

**MC:** COMPUTADORA MOVIL. (MOBIL COMPUTER)

**MCU:** UNIDAD CONVERTIDORA AL MEDIO. (MEDIUM CONVERTER UNIT)

**MDI:** INTERFASE DEPENDIENTE DEL MEDIO. (MEDIUM DEPENDENT INTERFASE)

**MEGA:** UN MILLON.

**PMA:** CONEXION AL MEDIO FISICO. (PHYSICAL MEDIUM ATTACHMENT)

**RAM:** MEMORIA DE ACCESO ALEATORIO. (RANDOM ACCESS MEMORY)

**S.C.T.:** SECRETARIA DE COMUNICACIONES Y TRANSPORTE.

**TCP/IP:** PROTOCOLO DE CONTROL DE TRANSMISION/PROTOCOLO

**INTERNET:** (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOLO)

**UDP:** PROTOCOLO DE DATAGRAMA DE USUARIO. (USER DATAGRAMA PROTOCOLO)

## Referencias bibliográficas

- Adam Engst, Glenn Fleishman. (2003): Introducción a las redes inalámbricas: Windows y Macintosh.
- Adam Engst, Glenn Fleishman. (2003): Introducción a las redes inalámbricas, Redes de ordenadores.
- Adithya Raghunathan. (2005): Ventajas económicas de la infraestructura inalámbrica para el desarrollo. Government publication; Wireless Internet (Latin America).
- A. Javier Martínez Sáez, José Manuel Riera Salís. (2005): Redes inalámbricas de Área Local (wlan). Simulación de la red IEEE 802.11
- Alberto Bastardo Rodríguez, Francisco Javier Merino Caminero. (2003): Riuva red inalámbrica de la Universidad de Valladolid.
- Andreas Schmid. (2000): Cómo localizar y reparar averías en receptores vía satélite. Artificial satellites in telecommunication (Maintenance and repair); Wireless communication systems (Maintenance and repair).
- Antonio Sillero García, Sebastián Ventura Soto. (2004): Diseño de una red inalámbrica para el Campus Universitario de Rabanales.
- Arturo Pérez Hernando, José Ramón Cerquides Bueno. (2004): Estudio y diseño de una red wireless.
- Bates, R.J. (1994): Comunicaciones en redes inalámbricas, NY: McGraw-Hill.
- Ben Forta, Keith D Lauver. (2001): Desarrollo WAP con WML y wmlscript.
- Carlos Fuentes Reñones, Eduardo Ballesteros Martínez. (2005): Análisis de prestaciones en redes inalámbricas IEEE 802.11

- César del Río García, Iván González Diego. (2005): Caracterización de la capacidad de sistemas Wi-Fi utilizando GTD/UTD.
- Christophe Mialy Lagasse (2005): Diseño y configuración de una red Wi-Fi en un entorno profesional.
- Daniel Iglesias Santamaría, José Luis García García. (2004): Desarrollo de una red inalámbrica de sensores para aplicaciones domóticas.
- David Ferrero Álvarez. (2005): Herramienta comparativa de modelos de cobertura en redes inalámbricas.
- David Pellón Corchuelo, Manuel Ocaña Miguel. (2004): Localización mediante GPS y Wi-Fi sobre PDA.
- Davis P.T. y McGuffin, C.R. (1995): Redes de Área Local Inalámbricas. NY: McGraw-Hill.
- Diego Hernández Climent. (2005): Diseño de una red Wi-Fi para ofrecer distintos tipos de servicio dentro de la Dársena Portuaria.
- Documento IEEE "Redes Híbridas" pág. 21-26, 1992 Universidad de Aveiro, Portugal.
- Eduardo Sáez Caro, Juan José Murillo Fuentes (2003): Caracterización y diseño de nodo de red inalámbrica Wi-Fi
- Elena Alcántud Pérez. (2004): Problemática de la seguridad en redes inalámbricas: Una solución basada en software libre.
- Estudio de impacto Ambiental Categoría II: Cable de fibra Óptica Arcos-1, zona de Ustupu-ogobsum, Fiber optic. cables (Environmental aspects, Panamá
- Fernando García Rubiño, Juan Antonio Rodrigo Yanes. (2006): Protocolos de seguridad en redes inalámbricas, Norma IEEE 802.11
- Francisco Javier Alcázar Rodríguez, Alejandro Carballar Rincón (2004): Diseño e instalación de un sistema wireless de televigilancia y domótica en un entorno.
- Javier Bejarano Palma, Rubén Martín Clemente. (2005): Estudio y despliegue de redes Wi-Fi.
- Javier Guillermo Monzón Romero, Luis Castejón Martín. (2004): Redes Wi-Fi. Proyecto de campus inalámbrico.
- Jesús Goya Abaurrea, Juan José Murillo Fuentes. (2005): Seguridad y autenticación en redes inalámbricas.
- Jes Nyhus. (2006): Redes y redes inalámbricas.
- Jorge Juan Fernández Arroyo, José María Rivero Cuadrado. (2004): Wireless Lan. Dotación de una red de servicios inalámbricos para la Escuela Técnica Superior.
- José Alberto Rodríguez Salazar, José Ignacio Alonso Montes. (2005): Despliegue de redes inalámbricas de área local: Planificación radio.
- José Antonio Carballar. (2004): Wi-Fi: Cómo construir una red inalámbrica, Redes de banda ancha; Procesado de señales; Modulación (Electrónica); Comunicaciones inalámbricas, Sistemas de Comunicaciones .
- Laurence Soyer. (2005): Wi-Fi: Instalar una red inalámbrica en casa, Sistemas de telecomunicaciones de banda ancha (Sistemas de telecomunicaciones de banda ancha); Sistemas de telecomunicaciones sin hilos.
- Luis Evelio Martín Pérez, Pilar Martín Martín. (2002): Tarjeta de red inalámbrica Prism1kit-eval por DSSS: Estudio didáctico del proceso de modulación.
- Luis Miguel Gómez Sánchez, Pilar Martín Martín. (2002): Tarjeta de red inalámbrica Prism1kit-eval por DSSS: Estudio del proceso de conversión de la señal.
- Luis Zarzo Fuertes, Manuel Ocaña Miguel, Kent Palmkvist. (2005): Diseño de la Capa Física de Una Red Local Wireless (WLAN) Basado en El Standard IEEE 802.11 a
- Manuel Pérez Marín, Álvaro Suárez Sarmiento. (2002): Herramienta multimedia para redes inalámbricas.
- María Jesús García Crespo, Paula Gómez Suárez, Diego Rafael Llanos Ferraris. (2004): Estudio de viabilidad, análisis y diseño de una red inalámbrica para la Escuela Universitaria.
- María Paz Valenzuela Gamboa, Miguel Nussbaum Voehl. (2003): Búsqueda social en redes inalámbricas. Thesis/dissertation; Redes Sociales (Innovaciones Tecnológicas), Sistemas de Comunicación Inalámbrica (Chile).
- María Rosa Román del Molino, Carlos Crespo Cadenas. (2005): Configuración de la seguridad, estudio de cobertura y herramienta docente de una red inalámbrica.



- Mariano Martínez Fernández. (2004): Estudio de viabilidad de tecnología Wi-Fi como modelo de negocio en el sector hotelero.
- Mercedes Fuertes. (2005): Redes inalámbricas municipales: Nuevo servicio público.
- Miguel Ángel Dancausa Lacruz, José Ramón Gállego
- Martínez. (2003): Análisis de la tecnología de banda ultra-ancha aplicada en redes inalámbricas.
- Miguel Expósito Martín, Constantino Pérez Vega. (2004): Diseño y simulación de una antena triédrica para redes inalámbricas
- Neil Reid, Ron Seide (2004): 802.11 (Wi-Fi): Manual de redes inalámbricas.
- Neil Reid, Ron Seide; traducción Jorge Omar Fuentes Zárate. (2004): Manual de redes inalámbricas, Sistemas de transmisión de datos, Sistemas inalámbricos de comunicación, Redes de áreas locales de computadora.
- Pablo Fuertes Huerta, Ander Marín Albarrán. (2004): Estudio de las oportunidades de negocio de las redes basadas en Wi-Fi. Aplicación para hoteles.
- Pablo Gallardo Gens, José Ruiz Más. (2004): Seguridad Wireless fortificación.
- Pablo Navas Cañete. (2006): Sistema de autenticación de redes inalámbricas basada en criptografía de clave pública
- Pedro Mario González Gast, Juan Pablo de Castro Fernández, María de los Ángeles. (2004): Cabecera de una red wireless.
- Revista PC/Tips Byte pág. 94-98 artículo: "Redes Inalámbricas", Abril 1992 Nicolás Baran.
- Revista PC/Magazine pág. 86-97, artículo: "Sin Conexión", Marzo 1995 Padriac Boyle.
- Ricardo Borrero Gavilán, Juan José Murillo Fuentes. (2003): Estudio de las redes inalámbricas de área local y metropolitana basadas en el estándar IEEE.
- Rubén Toledo Valera. (2005): Seguridad en una red inalámbrica utilizando criptografía de curva elíptica.
- Rubén Vera Rodríguez, Carlos Crepo Cadenas. (2006): Redes inalámbricas: Configuración, seguridad y estudio de cobertura para 802.11 b/g.
- Rui T. Valadas, Adriano C. Moreira, A.M. de Oliveira Duarte (1992): Documento IEEE "Ruteando con TCP/IP" pág. 7-12, 1992 IBM T.J.
- Sebastián Rodríguez Nuñez, Pilar Martín Martín. (2002): Tarjeta de red inalámbrica Prism1kit-eval por DSSS: Análisis del tratamiento de la señal en banda.
- Tomás Mingo Seligrat, Bernardo Alarcos Alcázar. (2004): Estudio y diseño de una red inalámbrica de datos en el edificio Politécnico.
- Vanesa Salas Martín, Christian Fraboul. (2004): Estudio de viabilidad y prototipo de un puente entre la Red Ethernet 802.3 y la red inalámbrica.
- Watson Research Center Charles E. Perkins (1992): Documento IEEE "Características de una Radio LAN" pág. 14-19, LACE Inc. Chandos A. Rypinski.
- [http://lat.3com.com/lat/technology/technical.papers/wireless\\_qa](http://lat.3com.com/lat/technology/technical.papers/wireless_qa).
- <http://www.wirelessethernet.com>

