UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

BUENAS PRÁCTICAS PARA AUDITAR REDES INALÁMBRICAS APLICADAS A LAS EMPRESAS DEL RUBRO HOTELERO DE LA CIUDAD DE CHICLAYO.

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

BACH. FRANCK JHONATHAN SANTA MARIA BECERRA.

Chiclayo 30 de Octubre de 2012

BUENAS PRÁCTICAS PARA AUDITAR REDES INALÁMBRICAS APLICADAS A LAS EMPRESAS DEL RUBRO HOTELERO DE LA CIUDAD DE CHICLAYO

POR:

SANTA MARIA BECERRA, FRANCK JHONATHAN

Presentada a la Facultad de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo para optar el título de

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR EL JURADO INTEGRADO POR

_____

Ing. León Tenorio, Gregorio Manuel
PRESIDENTE

_____

Ing. Otake Oyama, Luis A.
SECRETARIO

_____

Ing. Bravo Jaico, Jessie Leila
ASESORA

DEDICATORIA

A Dios por haberme colmado de bendiciones y guiado en el camino para lograr mis objetivos a lo largo de mi formación profesional.

A mi madre Ana María Becerra Olivera, quien ha sido, es y seguirá siendo mi fuente de inspiración, sostén y apoyo en mis esfuerzos de superación a lo largo de mi vida personal y profesional. Por haberme apoyado en todo momento incondicionalmente, por la motivación constante que me permitió hacer frente nuevos retos que me hicieron crecer como persona y profesionalmente, por su ejemplo de perseverancia, constancia y superación que la caracteriza y que me ha infundado siempre y por su valor mostrado de salir adelante al igual que mi abuela y mi tío.

A mis maestros por su asesoría y apoyo constante durante el desarrollo de esta investigación, por su amistad, enseñanza y oportunidades brindadas que impulsaron el desarrollo de mi formación profesional en el campo de la auditoría.

AGRADECIMIENTOS

Gracias en primer lugar a Dios por haberme
Colmado de salud en todo momento
Y permitirme el desarrollo de
Esta investigación,
A la vez un sincero agradecimiento
A mi asesora Jessie Bravo Jaico,
Por haberme brindado su tiempo,
Apoyo y guía permanente,
Y finalmente agradecer a mi familia
Por el constante apoyo al igual
Que a mis compañeros de aulas.

INDICE GENERAL

INDICE TABLAS

INDICE FIGURAS

Glosario

AES	Advanced Encryption Standard
BSSI	Basic Service Set Identifier
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hoping Spread Spectrum
GNU	GNU Not UNIX
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU-T	International Telecommunication Unit – Telecommunication Standardization Sector
IV	Initialization Vector
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
PHP	PHP (Personal Home Page Tools) Hypertext Pre-processor
PSK	Pre-shared Key
OSI	Open Systems Interconnection
RADIUS	Remote Authentication Dial-In User Server
RTS	Request to Send
SSID	Service Set Identity
TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
AICPA	American Institute of Certified Public Accountants
ISO 27001	Sistemas de Gestión de la Seguridad de la Información.

RESUMEN

A medida que surgen nuevos cambios en la tecnología informática, también surgen nuevas necesidades de servicios, nuevas formas de transportar la información, utilizando la movilidad y las comunicaciones, el ser humano siempre busca nuevas formas de poder realizar sus actividades desde la comodidad de su hogar de una forma fácil y movible, por ello nace la necesidad de implementar las redes inalámbricas.

Sin embargo actualmente no se cuenta con una guía de buenas prácticas que sirva de ayuda al auditor con experiencia y sin las herramientas necesarias para la auditoría en redes inalámbricas, en la cual los encargados del control la tomen de apoyo para realizar sus labores, realizándose el proceso de auditoría basados en la experiencia y de la mano con herramientas de monitoreo WLAN, monitoreando sólo canales de emisión, nivel de señal y tipo de claves, tomando más tiempo del que debería al no tener una guía de apoyo en la auditoría a la red inalámbrica.

Al presentar esta investigación, se propone buenas prácticas para el desarrollo de auditorías de redes inalámbricas aplicadas a las empresas del rubro hotelero. La propuesta está basada en el estudio de las empresas del rubro hotelero de la ciudad de Chiclayo con el fin de mejorar la disponibilidad, confiabilidad e integridad de la información, cotejando metodologías existentes que ayuden auditar redes inalámbricas, y desarrollando la propuesta de las buenas prácticas.

En base a las metodologías COBIT 4.1, NTP – ISO – IEC 27001, NTP – ISO – IEC 27002, Osstmm Wireless 2.9, ENISA, RED-M, Information networks planning and design (INPD) y metodología para administrar redes 3.0., se elaboraron buenas prácticas para auditar redes inalámbricas. Como parte de las buenas prácticas se encuentra, los dominios Diseño, Administración y Seguridad, y cada una presenta sus buenas prácticas, a la vez cada de estas tiene su objetivo, actividades o tareas, herramientas de apoyo y un Checklist para auditar la red inalámbrica.

Se utilizó la entrevista, encuesta, análisis de la red inalámbrica y documentos para recaudar información a través de los archivos históricos referentes a la aplicación de metodologías o guías de auditoría en la red inalámbrica.

Se realizó un estudio pre_experimental, realizándose una encuesta a las entidades hoteleras para poder determinar si cuentan con una red inalámbrica, si se realizaron auditorías a la red inalámbrica, si se basaron en algún documento, norma o guía de buenas prácticas, etc.; basándose en la información recopilada anteriormente se determinó una entidad hotelera para desarrollar y aplicar la propuesta para las buenas prácticas en la auditoría de la red inalámbrica, y por último evaluar si lo hecho sirve para cualquier institución.

La investigación es un aporte para personas y/o instituciones interesadas en realizar y aplicar buenas prácticas para auditar redes inalámbricas.

PALABRAS CLAVE: Redes inalámbricas, firewall, VPN, Wi-Fi, Punto de acceso, Red Ad Hoc, Sniffer, token, Radius.

ABSTRACT

As there are new changes in computer technology, also new needs for services, new ways to convey information, using mobility and communications, human beings always looking for new ways to carry out its activities from the comfort of your home in an easy and mobile, so comes the need to deploy wireless networks.

However there is currently a best practice guide that is helpful to the auditor with experience and without the necessary tools for auditing wireless networks, in which managers take control of the support to do their jobs, performing the audit process based on experience and hand with WLAN monitoring tools, monitoring only broadcast channels, signal level and key type, taking longer than it should to not have a fence into the network audit Wireless.

In presenting this research, we propose best practices for the development of wireless network audits applied to companies in the hospitality field. The proposal is based on the study of companies in the hotel business in the city of Chiclayo in order to improve the availability, reliability and integrity of information, collating audit methodologies that help wireless networks, and developing best practice proposal .

Based on the methodologies COBIT 4.1, NTP - ISO - IEC 27001, NTP - ISO - IEC 27002, OSSTMM Wireless 2.9, ENISA, RED-M, Information networks planning and design (INPD) and methodology for managing networks 3.0., Were developed best practices for auditing wireless networks. As part of good practice is, domains, design, management and security, and each has their good practices, while each of these has its purpose, activities or tasks, support tools and a checklist to audit wireless network .

We used the interview, survey, wireless network analysis and documents to collect information through the historical archives relating to the application of audit methodologies or guidelines on the wireless network.

Pre_experimental A study, carried out a survey of hotel companies to determine if they have a wireless network, if audits were performed to the wireless network, whether based on a document, standard or best practice guide, etc..; Based on information gathered above found a hotel establishment to develop and implement the proposal for good practice in the audit of the wireless network, and finally evaluate whether it actually serves to any institution.

The research is a contribution to individuals and / or institutions interested in making and implementing good practices for auditing wireless networks.

KEY WORDS: Wireless Networking, Firewall, VPN, Wi-Fi Puntos de acceso, Ad Hoc Network, Sniffer, token, Radius.

I. INTRODUCCION

Debido al importante crecimiento de las redes inalámbricas, las auditorías WLAN se han incrementado en los últimos años considerablemente en todo el mundo, porque se hace necesaria la realización de evaluaciones en distintas áreas de la red inalámbrica para optimizar su funcionamiento. Así mismo surgen nuevos cambios en la tecnología informática, también surgen nuevas necesidades de servicios, nuevas formas de transportar la información, utilizando la movilidad y las comunicaciones, el ser humano siempre busca nuevas formas de poder realizar sus actividades desde la comodidad de su hogar de una forma fácil y movible, en ello se muestra la necesidad de implementar las redes inalámbricas.

No obstante ante el incremento de esta necesidad emergen ciertos mecanismos fraudulentos que afectan el entorno de estas redes y su seguridad y por ende a la información que estos entes respaldan.

Los mecanismos fraudulentos en la mayoría de casos afectan a la seguridad de las redes inalámbricas, trayendo como consecuencia diferentes riesgos informáticos, y esto genera un gran impacto negativo si no se tiene el control respectivo dentro de dicha entidad.

Se define control informático como "la seguridad de los sistemas de información, la cual la definimos como la doctrina que trata de los riesgos informáticos, en donde la auditoría se involucra en este proceso de protección y preservación de la información y de sus medios de proceso". Y tomando en cuenta este concepto, si este control informático es llevado de manera inadecuada surge una nueva necesidad, la de auditar dicho control para determinar las amenazas, vulnerabilidades y riesgos que tiene el servicio informático relacionados con las redes inalámbricas (Arteaga 2009).

Sin embargo actualmente no se cuenta con una guía de buenas prácticas que sirva de ayuda al auditor con experiencia y sin herramientas necesarias para la auditoría en redes inalámbricas, en la cual los encargados del control la tomen de apoyo para realizar sus labores, realizándose el proceso de auditoría basados en la experiencia y de la mano con herramientas de monitoreo WLAN, realizándose sólo el monitoreo de canales de emisión, nivel de señal y tipo de claves, tomando más tiempo del que debería al no tener una guía de apoyo en la auditoría a la red inalámbrica, preguntándonos así si es posible desarrollar buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo.

Una posible respuesta ante este problema fue si la elaboración de buenas prácticas para auditar redes inalámbricas permitirá mejorar la ejecución de los procesos de auditoría a redes inalámbricas en las empresas del rubro hotelero de la ciudad de Chiclayo.

Para ello se definió proponer buenas prácticas para auditar redes inalámbricas aplicadas a las empresas del rubro hotelero de la ciudad de Chiclayo, realizando

un estudio de las empresas pertenecientes al rubro con el fin de mejorar la disponibilidad, confiabilidad e integridad de la información, cotejando las metodologías, manuales y buenas prácticas nacionales e internacionales existentes que ayuden a auditar redes inalámbricas, desarrollando la propuesta de buenas prácticas plasmada en una guía para auditar redes inalámbricas, planteando dominios, actividades a seguir, herramientas y Checklist que mejoren los procesos de auditorías a las redes inalámbricas, facilitando el trabajo y optimizando el tiempo para auditar redes inalámbricas y aplicando las buenas prácticas plasmada en una guía.

Al realizar esta guía de buenas prácticas se contribuyó con el desarrollo de auditorías de redes inalámbricas con la cual se facilite el trabajo, reduzca tiempos, y apoye la labor de los auditores en el desarrollo de auditorías a redes inalámbricas, cumpliendo con los estándares de seguridad de manera completa y sencilla.

II. MARCO TEÓRICO

2.1. Antecedentes de Investigación.

Antecedente 1

Título: "Wi-Fi RF AUDIT"
Autor: Red-M Group Limeted
Lugar y fecha: Graylands - Setiembre del 2007
Propósito:
En esta investigación se centra en la auditoría para responder a los problemas de acceso del usuario, rendimiento y servicio, tratar con los problemas de seguridad, planificación para el crecimiento, integración de nuevas tecnologías, comprobación de una red nueva o existente y establecer una línea de base de diseño para la instalación de nuevas redes Wi-Fi. Por lo cual se propone un marco más amplio que incluye el Diseño y Seguridad de la Red Inalámbrica y una solución segura para la red, en base a buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de un cuestionario y un Checklist de forma que se podrá así desarrollar una auditoría Wlan (Red M 2002).

Antecedente 2

Título: "Plan de cinco pasos para la seguridad del Enterprise WLAN"
Autor: Lisa Phifer - CORE COMPETENCE INC.
Lugar y fecha: Sunnyvale - Noviembre del 2006
Propósito:
En esta investigación se centra en diseñar una infraestructura para garantizar la seguridad de una red inalámbrica y la integridad de las redes empresariales en cinco pasos esenciales, que consistió en la salvaguardia de los clientes inalámbricos y de datos, control de conexiones Wi-Fi, auditoría de la actividad inalámbrica y la aplicación y cumplimiento de las políticas inalámbricas. Presentando un alcance limitado debido que se centra en la seguridad inalámbrica. Por lo cual se propone un marco más amplio que incluye el Diseño y Administración de la red inalámbrica y una solución segura, en base buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de un cuestionario y un checklist de forma que se podrá así desarrollar una auditoría Wlan (CORE 2006).

Antecedente 3

Título: "Wi-Fi Wireless LAN de Auditoría de Seguridad"
Autor: Cypress Solution.
Lugar y fecha: India – Septiembre del 2008
Propósito:

En esta investigación se centra en garantizar la Seguridad WLAN, que consistió en la revisión de cuentas de seguridad Wi-Fi conteniendo una variedad de pruebas, encontrando debilidades en sus puntos de acceso haciendo uso de las últimas herramientas de gestión inalámbrica para averiguar si la misma está transmitiendo fuera de las paredes de la organización de manera incontrolada e insegura, conocidas como redes de los puntos de acceso deshonestos (Networks Rogue). Por lo cual se propone un marco más amplio que incluye el Diseño y Administración de la red inalámbrica y una solución segura para la red, en base buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de un cuestionario y un Checklist de forma que se podrá así desarrollar una auditoría Wlan (Cypress 2008).

Antecedente 4

Título: "Audit Briefing"
Autor: AuditNet.
Lugar y fecha: Unites States – Abril del 2005
Propósito:
En esta investigación se centra en una auditoría de información, dicha información reunida tenía por objetivo proporcionar el conocimiento de problemas de seguridad de los clientes, que se deben tener en cuenta en la planificación para su uso. Por lo cual se propone un marco más amplio que incluye el Diseño, Administración y Seguridad de la red inalámbrica y una solución segura para la misma, en base buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de un cuestionario y un checklist de forma que se podrá así desarrollar una auditoría Wlan (AuditNet 2005).

Antecedente 5

Título: "OSSTMM Wireless 2.9"
Autor: Peter Herzog - ISECOM.
Lugar y fecha: Unites States – Octubre del 2003
Propósito:
En esta investigación se centra en proporcionar un método aceptado para la realización de pruebas de seguridad completa, siendo un conjunto de reglas y normas. Este manual es una estándar profesional que consiste en pruebas de seguridad aplicadas a cualquier medio de afuera hacia adentro, incluyendo reglas de contrato, la ética para el probador profesional, las legalidades de la seguridad de pruebas, y un conjunto de test de seguridad; las pruebas de seguridad externas van de un ambiente no privilegiado a uno privilegiado, para evitar/vulnerar los componentes de seguridad, procesos, y alarmas para ganar acceso privilegiado. Por lo cual se propone un marco más amplio que incluye el Diseño y Administración de la red inalámbrica y una solución segura para la misma, en base buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de un cuestionario y un checklist de forma que se podrá así desarrollar una auditoría Wlan (ISECOM y Herzog 2003).

2.2. Bases Teóricas

2.2.1. Redes inalámbricas.

2.2.1.1. Definición de Red de Área Local Inalámbrica.

Una red inalámbrica es un sistema de comunicación de datos que proporciona conexión inalámbrica entre equipos situados dentro de la misma área (interior o exterior) de cobertura. En lugar de utilizar el par trenzado, el cable coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas.

Las redes WLAN se componen fundamentalmente de dos tipos de elementos, los puntos de acceso y los dispositivos de cliente. Los puntos de acceso actúan como un concentrador o hub que reciben y envían información vía radio a los dispositivos de clientes, que pueden ser de cualquier tipo, habitualmente, un PC o PDA con una tarjeta de red inalámbrica, que se instala en uno de los slots libres o bien se enlazan a los puertos USB de los equipos.

Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 54 Mbps, frente a los 10 y hasta los 1000 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.
El uso más popular de las WLAN implica la utilización de tarjetas de red inalámbricas, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una conexión física (Oliver y Escudero 1999).

2.2.1.2. Características

Una red inalámbrica ofrece:

a. **Movilidad:** Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica.

b. **Simplicidad y rapidez en la instalación:** La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tirar cable a través de paredes y techos.

c. **Flexibilidad en la instalación:** La tecnología inalámbrica permite a la red ir donde la cableada no puede ir.

d. **Costo de propiedad reducido:** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una red cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior.

e. **Escalabilidad:** Los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red (Oliver y Escudero 1999).

2.2.1.3. Configuraciones WLAN.

La complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que se quiera implementar, se pueden utilizar diversas configuraciones de red tales como:

Punto a Punto o Ad-Hoc.

La configuración más básica es la llamada punto a punto o Ad–Hoc, consiste en una red de dos o más terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas; en la Figura. N° 01 se muestra un ejemplo. En esta modalidad no existe un dispositivo central encargado de concentrar y coordinar las comunicaciones, sino que cada nodo existente en la red se comunica directamente con los demás y no hay nodo preponderante alguno.

Para que la comunicación entre estas estaciones sea posible, hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra.

Las redes de tipo ad-hoc son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa. También este tipo es conocido como IBSS - Independent Basic Service Set (Oliver y Escudero 1999).

Figura N° 01: Configuración punto a punto o Ad–Hoc.
Fuente: (Oliver y Escudero 1999)

2.2.1.4. Normalización IEEE para WLAN.

La norma 802 fue desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), y versa sobre la arquitectura de redes de datos LAN (Local Área Network).
Esta norma establece un estándar de tecnología en el mercado mundial, garantizando que los productos compatibles con la norma 802 sean también compatibles entre sí.
La norma posee muchos apartados, que describen y especifican las distintas funciones que se implementan en una comunicación de datos de red. Ejemplos de estos apartados se detallan en la Tabla N° 01.

Apartado	Descripción
802.1	Describe las funciones de Bridging.
802.2	Controla el enlace lógico.
802.4	Método de control de tráfico Token-Passing.
802.5	Método de control de tráfico Token-Ring.
802.10	Seguridad en comunicaciones de datos, etc.
802.11	Describe y especifica una interface inalámbrica para comunicaciones de datos compatibles con la Norma IEEE 802.

Tabla N° 01: Norma IEEE 802.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades (34 TELECOM 2005).

WLAN 802.11.

La tecnología clave que contiene el estándar 802.11 es el espectro de dispersión de secuencia directa (DSSS). El DSSS se aplica a los dispositivos inalámbricos que operan dentro de un intervalo de 1 a 2 Mbps.
Un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma. El siguiente estándar aprobado fue el 802.11b, que aumentó las capacidades de transmisión a 11 Mbps. Aunque las WLAN de DSSS podían interoperar con las WLAN de espectro de dispersión por salto de frecuencia (FHSS), se presentaron problemas que motivaron a los fabricantes a realizar cambios

en el diseño. En este caso, la tarea del IEEE fue simplemente crear un estándar que coincidiera con la solución del fabricante (Cisco 2009).

WLAN 802.11b (Wi-Fi).

802.11b también recibe el nombre de Wi-Fi™ o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps. Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso.
Los dispositivos de 802.11b logran un mayor índice de tasa de transferencia de datos ya que utilizan una técnica de codificación diferente a la del 802.11, permitiendo la transferencia de una mayor cantidad de datos en la misma cantidad de tiempo. La mayoría de los dispositivos 802.11b todavía no alcanzan tasa de transferencia de 11 Mbps y, por lo general, trabajan en un intervalo de 2 a 4 Mbps (Cisco 2009).

WLAN 802.11a (Wi-Fi 5).

802.11a abarca los dispositivos WLAN que operan en la banda de transmisión de 5 GHZ. El uso del rango de 5 GHZ no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHZ. 802.11a puede proporcionar una tasa de transferencia de datos de 54 Mbps y con una tecnología propietaria que se conoce como "duplicación de la velocidad" ha alcanzado los 108 Mbps. En las redes de producción, la velocidad estándar es de 20-26 Mbps (Cisco 2009).

WLAN 802.11g.

802.11g ofrece tasa de transferencia que 802.11a pero con compatibilidad retrospectiva para los dispositivos 802.11b utilizando tecnología de modulación por multiplexión por división de frecuencia ortogonal (OFDM). Cisco ha desarrollado un punto de acceso que permite que los dispositivos 802.11b y 802.11a coexistan en la misma WLAN. El punto de acceso brinda servicios de 'Gateway' que permiten que estos dispositivos, que de otra manera serían incompatibles, se comuniquen (Cisco 2009).

2.2.1.5. Extensiones de la Norma 802.11.

Las extensiones de las Norma de describen a continuación en la Tabla N° 02.

Extensión	Descripción
802.11e	Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.
802.11i	Su objetivo es la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11. Proporciona una alternativa a la privacidad equivalente cableada (WEP) con nuevos métodos de encriptación y procedimientos de autentificación. IEEE 802.1x constituye una parte clave de 802.11i.
802.11d	Constituye un complemento al nivel de control de acceso al medio (MAC) en 802.11. Para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11 permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.
802.11f	Su objetivo es lograr la interoperabilidad del punto de acceso dentro de una red WLAN multiproveedor. El estándar define el registro del punto de acceso dentro de una red y el intercambio de información entre dichos punto de acceso cuando un usuario se traslada desde un punto de acceso a otro.
802.11h	El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 Ghz requieren que los productos tengan control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el Punto de Acceso para reducir al mínimo la interferencia con otros sistemas Ej.: radar.

Tabla N° 02: Extensiones de la Norma 802.11.

Cabe mencionar que la banda de frecuencia 2.4 Ghz, utilizada por la tecnología 802.11b, es una banda no licenciada lo que significa que su uso es libre.

La norma 802.11b, es la que actualmente se comercializa en forma masiva a través de una gran variedad de productos y aplicaciones. La norma 802.11a está evolucionando, y se supone que en un futuro cercano también ofrecerá soluciones económicas al mercado de datos inalámbricos al igual que el 802.11g.

Resumiendo los conceptos más relevantes de la norma 802.11b:

- Es un estándar internacional en comunicaciones de datos.
- Tecnología probada por muchos años a nivel mundial.
- Existe gran variedad de productos orientados a distintas aplicaciones.
- Opera en una banda no licenciada (Briones y Geannina 2005).

2.2.1.6. Hardware de Red Inalámbrica

2.2.1.6.1. Punto de acceso

El Punto de acceso opera en las capas 1 y 2 del modelo de referencia OCI. Aquí es también donde operan el bridge inalámbrico y el bridge de grupos de trabajo.
Un Punto de acceso es un dispositivo WLAN que puede actuar como punto central de una red inalámbrica autónoma. Un AP puede utilizarse también como punto de conexión entre redes inalámbricas y cableadas. En grandes instalaciones. La funcionalidad de roaming proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente a través de la instalación, a la vez que se mantiene un acceso sin fisuras e ininterrumpido a la red.
Normalmente un WAP (Wireless Access Point) también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.
Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.
Los puntos de acceso inalámbricos tienen un radio de cobertura aproximado de 100m, aunque esto varía bastante en la práctica entre un modelo y otro; y según las condiciones ambientales y físicas del lugar.
Los puntos de acceso se agrupan en dos categorías (Cisco 2009).

2.2.1.6.2. Bridges

Los bridges están diseñados para conectar dos o más redes ubicadas en general en diferentes edificios. Proporciona elevadas velocidades de datos y un throughput superior para aplicaciones intensivas en cuanto a los datos, de línea de visión. Los bridges conectan sitios difíciles de cablear, pisos no continuos, oficinas satelitales, instalaciones de campus de escuelas o corporaciones, redes temporales y depósitos. Pueden configurarse para aplicaciones punto a punto o punto multipunto.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.
No filtra los broadcast, que son paquetes genéricos que lanzan los equipos a la red para que algún otro les responda, aunque puede impedir el paso de determinados tipos de broadcast. Esto es típico para solicitar las cargas de software, por ejemplo. Por tanto, al interconectar segmentos de red con bridges, podemos tener problemas de tormentas de broadcast, de saturación del puente por sobrecarga de tráfico, etc.
El número máximo de puentes en cascada es de siete; no pueden existir bucles o lazos activos, es decir, si hay caminos redundantes para ir de un equipo a otro, sólo uno de ellos debe estar activo, mientras que el redundante debe ser de backup. El peligro de los bridges es cuando hay exceso de broadcast y se colapsa la red. A esto se le llama tormenta de broadcast, y se produce porque un equipo está pidiendo ayuda (falla) (Cisco 2009).

Figura N° 02: Bridge

2.2.1.6.3. Switch

Un Switch se describe a veces como un puente multipuerto. Mientras que un puente típico puede tener sólo dos puertos que enlacen dos segmentos de red, el Switch puede tener varios puertos, según la cantidad de segmentos de red que sea necesario conectar. Al igual que los puentes, los Switchs aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los Switchs utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un computador a otro de la red.
Aunque hay algunas similitudes entre los dos, un Switch es un dispositivo más sofisticado que un puente. Un puente determina si se debe enviar una trama al otro segmento de red, basándose en la dirección MAC destino. Un Switch tiene muchos puertos con muchos segmentos de red conectados a ellos. El Switch elige el puerto al cual el dispositivo o estación de trabajo destino está conectado. Los Switchs Ethernet están llegando a ser soluciones para conectividad de uso difundido porque, al igual que los puentes, los Switchs mejoran el rendimiento de la red al mejorar la velocidad y el ancho de banda (Cisco 2009).

Figura N° 03: Switch

2.2.1.6.4. Router

Los routers son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Dentro de un entorno de LAN, el router contiene broadcast, brinda servicios locales de resolución de direcciones, tal como ARP, y puede segmentar la red utilizando una estructura de subred. Para brindar estos servicios, el router debe conectarse a la LAN y a la WAN.

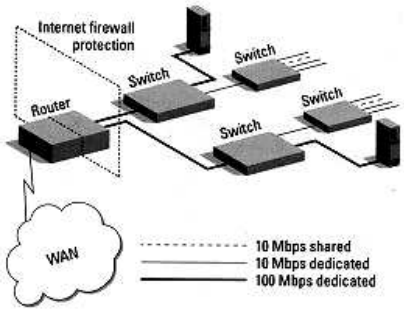

Figura N° 04: Diagrama de Funcionamiento
Fuente: Redes Linux[1].

El enrutador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un Switch. Al funcionar en una capa mayor que la del Switch, el enrutador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DEC net. Esto le permite hacer una decisión más inteligente que al Switch, al momento de reenviar los paquetes.

Figura N° 05: Modelo de Router de 2 antenas

El enrutador realiza dos funciones básicas:

[1] White papers sobre Switchs y Ruteadores. http://www.redes-linux.com/manuales/Tecnologia_redes/switchesyruteadores.pdf (Acceso 10 Julio 2010)

1. El enrutador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente.
   De esta manera el enrutador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

2. La inteligencia de un enrutador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un enrutador puede incrementar el tiempo de espera o reducir el desempeño del enrutador cuando se compara con una simple arquitectura de Switch (Cisco 2009).

2.2.1.7. Pérdida de Señal WiFi.

Una de las dudas que tiene el usuario al momento de realizar la instalación WiFi y a la vez uno de los factores que se debe tener en cuenta es la interferencia que va tener la WLAN, a continuación se les presenta una tabla resumen con esos datos (Panda 2005).

Material	Pérdida adicional (db)	Rango efectivo
Espacio en abierto	0	100%
Ventana (no metal)	3	70%
Ventana (metal)	5-8	50%
Pared 5 cm espesor	5-8	50%
Pared 10 cm espesor	10	30%
Pared +10 cm espesor	15-20	15%
Hormigón	20-25	10%
Techo/suelo	15-20	15%
Techo/suelo (amplio)	20-25	10%

Tabla N° 03: Materiales que producen pérdida de señal.

2.2.1.8. Interferencia y Atenuación.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección nos ayudará a identificar los elementos

que afecten negativamente a la señal inalámbrica, algunos elementos y su grado de interferencia se muestra en la Tabla N° 07

Material	Ejemplo	Interferencia
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia	Alta
Papel	Rollos de papel	Alta
Vidrio con plomo	Ventanas	Alta
Metal	Vigas, armarios	Muy Alta

Tabla N° 04: Interferencia y Atenuación.

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que pueden afectar negativamente al rendimiento. Las tecnologías que pueden producir interferencias son las siguientes (Panda 2005):

- Bluetooth.
- Hornos Microondas.
- Algunos teléfonos DECT inalámbricos.
- Otras redes WLAN.

2.2.2. Seguridad en Redes Inalámbricas.

2.2.2.1. Redes Abiertas

✓ **Ataque Denegación de Servicio (DoS)**

El objetivo de este ataque implementado en una red inalámbrica consiste en impedir una comunicación entre el terminal y un punto de acceso. Para lograr esto sólo hemos de hacernos pasar por el punto de acceso poniéndonos su dirección MAC (obtenida mediante un simple Sniffer) y negarle la comunicación al terminal o terminales elegidos mediante el envío continuado de notificaciones de desasociación.

✓ **Descubrir ESSID ocultos**

En casi todos los puntos de acceso podemos encontrar la opción de deshabilitar el envío del ESSID en los paquetes o desactivar BEASON

FRAMES. Ante esta medida de seguridad, un presunto atacante tendría dos opciones:

- Esnifar la red durante un tiempo indeterminado a la espera de una nueva conexión a la red con el objetivo de conseguir el ESSID presente en las tramas PROVE REQUEST del cliente (en ausencia de BEASON FRAMES) o en las tramas PROVE RESPONSE.
- Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque DoS pero sin mantener al cliente desconectado.

✓ **Ataque Man in the middle**

Este ataque apareció en escena a raíz de la aparición de los Switchs, que dificultaban el empleo de Sniffers para obtener los datos que viajan por la red. Mediante el ataque Man in the middle se hace creer al cliente victima que el atacante es el punto de acceso y, al mismo tiempo convencer al punto de acceso que el atacante es el cliente.
Para llevar a cabo un ataque de este tipo es necesario obtener los siguientes datos mediante el uso de un Sniffers:

- El ESSID de la red.
- La dirección MAC del punto de acceso.
- La dirección MAC de la victima

Una vez obtenidas estos datos emplearíamos la misma metodología que en el ataque de tipo DoS para romper la conexión entre el cliente y el punto de acceso. Tras esta ruptura la tarjeta del cliente comenzará a buscar un nuevo punto de acceso en los diferentes canales, momento que aprovechará el atacante para suplantar al punto de acceso empleando su MAC y ESSID en un canal distinto. Para ello el atacante habrá de poner su propia tarjeta en modo máster.

De forma paralela el atacante ha de suplantar la identidad el cliente con el punto de acceso real empleando para ello la dirección MAC del cliente, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente (Panda 2005).

2.2.2.2. WEP – Privacidad Equivalente al Cable

2.2.2.2.1. Principios de Funcionamiento

Es el algoritmo de seguridad empleado para brindar protección a las redes inalámbricas incluido en la primera versión del estándar IEEE 802.11 y mantenido sin cambios en 802.11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. Este sistema emplea el algoritmo RC4, proporcionado por RSA Security, para el cifrado de las llaves que

pueden ser de 64 o 128 bits teóricos, puesto que en realidad son 40 o 104 y el resto (24 bits) se emplean para el vector de inicialización.

La seguridad ofrecida por WEP tiene como pilar central una clave secreta compartida por todos los comunicadores y que se emplea para cifrar los datos enviados. Pese a no estar así establecido, en la actualidad todas las estaciones y punto de acceso comparten una misma clave, lo que reduce el nivel de seguridad que puede ofrecer este sistema (Panda 2005).

2.2.2.3. WPA

En el estándar 802.11se definen unos mecanismos de seguridad que se han demostrado insuficientes e ineficientes:

- La confidencialidad se basa en el sistema denominado WEP (Wired Equivalent Privacy) que consiste en un sistema de cifrado simétrico RC4, utilizando una clave estática que comparten estaciones clientes y el punto de acceso. WEP usa vectores de inicialización para generar claves diferentes para cada trama. No obstante, WEP es un sistema muy débil ya que se puede conseguir la clave de cifrado monitorizando las tramas y procesándolas.
- La integridad se consigue utilizando técnicas de detección de errores (CRC) que no son eficientes para garantizar la integridad.
- La autenticación es inexistente ya que incluso permite hallar la clave usada por WEP de forma muy sencilla. Algunos fabricantes proporcionan autenticación del equipo a partir de la dirección MAC de la estación, pero es un método muy poco flexible.

Wi-Fi Alliance, como organización responsable de garantizar la interoperabilidad entre productos para redes inalámbricas de fabricantes diversos, ha definido una especificación de mercado basado en las directrices marcadas por el grupo de trabajo 802.11i denominada Wi-Fi Protected Access (WPA), junto con la correspondiente certificación de productos (Panda 2005).

2.2.2.3.1. Privacidad e Integridad con TKIP

Temporal Key Integrity Protocol (TKIP) es el protocolo elegido con el objetivo de sustituir a WEP y solucionar los problemas de seguridad que éste plantea. Como características mejoradas destacar la ampliación (Panda 2005).

2.2.2.3.2. Autenticación mediante 802.1X/EAP

El cometido principal del estándar 802.11x es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos y permite emplear el protocolo de autenticación extensible (EAP) para autentificar al usuario de varias maneras.

IEEE 802.1x define 3 entidades:

- ✓ El solicitante (suplicant), reside en la estación inalámbrica.
- ✓ El autenticador (authenticator), reside en el AP.
- ✓ El servidor de autenticación, reside en un servidor AAA (Authentication, Authoization, Accounting) como RADIUS.

EAP comprende 4 tipos de mensajes:

- ✓ Petición: empleado para enviar mensajes desde el AP al cliente.
- ✓ Respuesta: empleado para enviar mensajes desde el cliente al AP.
- ✓ Éxito: emitido por el AP, significa que el acceso está permitido.
- ✓ Fallo: enviado por el AP cuando para indicarle al Suplicante que se deniega la conexión.

Proceso de Autenticación, tras la asociación:

Se envía el AP-Request/Identity desde el Autenticador al Suplicante.

- ✓ El suplicante responde con EAP-Response/Identity al Autenticador, el cual lo pasa al Servidor de Autenticación.
- ✓ Se tuneliza el Challenge/Response y si resulta acertado el Autenticador permite al Suplicante acceso a la red condicionando por las directrices del Servidor de Autenticación

El funcionamiento base del estándar 802.11x se centra en la denegación de cualquier tráfico que no sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ellos el autenticador crea un puerto por cliente que define dos caminos, uno autorizado y otro no; manteniendo el primero cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso al camino autorizado.

El solicitante, cuando pasa a estar activo en el medio, selecciona y se asocia a un AP. El autenticador (situado en el AP) detecta la asociación del cliente y habilita un puerto para ese solicitante, permitiendo únicamente el trafico 802.1x, el resto de trafico se bloquea. El cliente envía un mensaje "EAP Stara". El autenticador responde con un mensaje "EAP Request Indetity" para obtener la identidad del cliente, la respuesta del solicitante "EAP Response" contiene su identificador y es retransmitido por el autenticador hacia el servidor de autenticación. A partir de ese momento el solicitante y el servidor de autenticación se comunicarán directamente, utilizando un cierto algoritmo de autenticación que pueden negociar. Si el servidor de autenticación acepta la autentificación, el autenticador pasa el puerto del cliente a un estado autorizado y el tráfico será permitido (Panda 2005).

2.2.2.3.3. EAP. TLS

Requiere de la posesión de certificados digitales por parte del cliente y el servidor de autenticación; el proceso de autenticación comienza con el envío de su identificación (nombre de usuario) por parte del solicitante hacia el servidor de autenticación, tras esto el servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo propio. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la generación de la clave de cifrado, la cual es enviada al AP por el servidor de autenticación para que pueda comenzar la comunicación segura (Panda 2005).

2.2.2.3.4. Vulnerabilidades en EAP – TLS

En la fase de identificación el cliente manda el mensaje EAP – Identity sin cifrar, permitiendo a un atacante ver la identidad del cliente que está tratando de conectarse.

2.2.2.3.5. PEAP Y EAP – TTLS

El mayor inconveniente que tiene el uso de EAP – TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número ellos puede ser difícil y costosa. Para corregir este defecto se crearon PEAP (Protected EAP) Y EAP -Tunneled TLS que únicamente requieren certificado en el servidor.

La idea base de estos sistemas es que, empleando el certificado del servidor previamente validado, el cliente pueda enviar sus datos de autenticación cifrados a través de un túnel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden generar una clave de sesión (Panda 2005).

2.2.2.3.6. Ataque WPA – PSK

El único ataque conocido contra WPA – PSK es del tipo fuerza bruta o diccionario; pese a la existencia de ese ataque la realidad es que el rendimiento del ataque es tan bajo y la longitud de la passphrase puede ser tan larga, que implementarlo de forma efectiva es prácticamente imposible. Los requisitos para llevar a cabo el ataque son:

- ✓ Un archivo con la captura del establecimiento de conexión entre el cliente y el AP.
- ✓ El nombre de ESSID.
- ✓ Un archivo de diccionario.

Se puede auditar la fortaleza de las contraseñas empleadas en un sistema realizando ataques de diccionario o de fuerza bruta, en este último caso

empleando herramientas al uso para crear todas las combinaciones de caracteres posibles (Panda 2005).

2.2.2.4. Portales cautivos

Sistema creado para permitir la validación de usuarios en nodos Wireless, Ampliamente empleado para proporcionar conexión regulada a los usuarios de establecimientos públicos, hoteles, aeropuertos, etc.
En un sistema con portal cautivo se definen dos partes diferenciadas: la zona pública y la privada.

La zona pública se compone, normalmente, de nodos Wireless que posibilitan la conexión de cualquier Terminal; en cambio el acceso la zona privada, normalmente Internet, se encuentra regulado por un sistema de autenticación que impide la navegación hasta que el usuario se valida.

El sistema de portales cautivos se compone en líneas generales, de una serie de APs conectados a un GATEWAY colocado antes de la zona privada, un servidor web donde colocar el portal y una base de datos donde almacenar los usuarios y el servicio de autenticación.
En el momento de en que un usuario no autenticado decide conectarse a la zona privada el Gateway comprueba si dicho usuario está autenticado; para ello se basa en la posesión de tokens temporales gestionados por http. Si dicho usuario no posee un token válido, el Gateway redirecciona la conexión hacia el portal donde al usuario se le solicitarán un usuario y contraseña válidos para asignarle un token, Una vez obtenido un token el Gateway permitirá la conexión hacia la zona privada (Panda 2005).

2.2.2.4.1. Vulnerabilidades en portales cautivos

Debido a las características de la zona abierta de los sistemas que implantan este sistema de portales, se permite la asociación con el AP a cualquier cliente y el tráfico entre los clientes y el AP no va; por este motivo se puede capturar el tráfico de las conexiones con la zona privada.
Por otra parte es posible implementar ataques de tipo spoofing o hijacking mientras el token que emplea el usuario legítimo sea válido.

2.2.2.5. Rogue AP

Punto de acceso no autorizado. Este tipo de ataques consiste, a nivel básico en colocar un punto de acceso bajo nuestro control cerca de las instalaciones de la víctima de forma que los clientes asociados o por asociar a esa red se conecten a nuestro AP en lugar de uno legítimo de la víctima debido a la mayor señal que recibe del nuestro.

Una vez conseguida la asociación al Rogue AP, el atacante puede provocar ataques de tipo DoS, robar datos de los clientes como usuarios y contraseñas de diversos sitios Web o monitorizar las acciones del cliente.

Este tipo de ataques se ha empleado tradicionalmente para:

- ✓ Crear puertas traseras corporativas.
- ✓ Espionaje industrial

2.2.2.5.1. Rogue AP Básico

El ROGUE AP puede consistir en un AP modificado o un portátil con el software adecuado instalado y configurado. Este software ha de consistir en: Servidor http, servidor DNS, servidor DHCP y un portal cautivo con sus correspondientes reglas para redirigir el tráfico al portal. Todo este proceso de instalación y configuración se puede simplificar bastante mediante Airsnarf, herramienta que automatiza el proceso de configuración y arranque de un Rogue AP.

Sin embargo hace falta algo más para poder montar un Rogue AP, se requiere que la tarjeta Wireless sea compatible con HostAP, un driver específico que permite colocar la tarjeta en modo máster, necesario para que nuestro terminal pueda comportase como si fuese un AP. Si queremos montar un Rogue AP sobre un Windows deberemos encontrar una tarjeta compatible con SoftAP para poder cambiar el modo a máster, y emplear Airsnarf para configurar los distintos servicios.
El proceso de configuración que lleva a cabo Airsnarf consiste en colocar el portal cautivo y arrancar el servidor http, configurar el servidor DHCP para que proporciones IP, Gateway y DNS al cliente; evidentemente el Gateway y el servidor DNS será el terminal del atacante convertido en Rogue AP. Por último se configura el servidor DNS para que resuelva todas las peticiones con la IP del atacante, de forma que se puedan redireccionar todas hacia el portal cautivo del Rogue AP.

Una vez el usuario introduce su usuario y contraseña en el portal cautivo, el atacante ya las tiene en su poder. Lo normal es cambiar la apariencia del portal cautivo para que sea igual a la del portal del sistema al que se está suplantando.

Otra opción es dejar navegar al usuario normalmente pero redirigir determinadas páginas a otras copias locales con el fin de obtener usuarios y contraseñas. Para ello se puede modificar el servidor DNS para resolver aquellas páginas que nos convengan a nuestra dirección local donde tendremos preparada una copia falsa de la página (Panda 2005).

2.2.2.5.2. Rogue RADIUS

Por este nombre se conocen aquellos montajes que, aparte del Rogue AP clásico, incorporan un servidor RADIUS en el terminal del atacante. Para este fin se emplea comúnmente un servidor Free RADIUS adecuadamente configurado para responder a las peticiones de los usuarios legítimos.

Este tipo de montaje se emplea contra sistemas que cuentan con servidores de autenticación y redes securizadas mediante EAP de forma que el atacante pueda suplantar todos los dispositivos y servidores presentes en el sistema legítimo de forma convincente, autenticador y servidor de autenticación (Panda 2005).

2.2.2.5.3. Rogue RADIUS VS EAP

EAP - TLS pretende mejorar la seguridad de EAP mediante la implantación de certificados digitales instalados en todos los clientes y servidores. De esta manera se añade la necesidad de poseer un certificado válido para completar la autenticación. Tras el intercambio de certificados entre el suplicante y el servidor de autenticación, estos negocian un secreto común que se emplea para cifrar el resto de las comunicaciones a partir de ese momento.

EAP- TTLS (EAP- Tunneled - TLS) añade a las características de seguridad de EAP- TLS el establecimiento de un canal de comunicación seguro para el intercambio de las credenciales de usuario. De esta forma se incrementa la seguridad frente a ataques de sniffing que pretendan hacerse con estos datos.

Por otra parte elimina la necesidad de contar con certificados en todos los clientes, que conlleva un proceso de distribución y mantenimiento engorroso y caro.

De esta forma, el proceso de autenticación pasa por una primera fase de asociación del suplicante con el autenticador y una segunda en la que el servidor de autenticación envía su certificado al suplicante que, una vez validado, emplea para crear un túnel de comunicación seguro por donde enviar las credenciales y finalizar la autenticación.

Tras montar un Rogue AP con un Rogue RADIUS el atacante puede desasociar a un cliente y cuando este cliente se intenta conectar, se asociará al Rogue AP por ofrecer esta mayor intensidad de señal. Una vez asociado se repetirá el proceso de autenticación mediante EAP – TLS/ TTLS - PEAP pero contra el Rogue RADIUS bajo nuestro control. De esta forma podremos (Panda 2005):

- ✓ Desasociar usuarios
- ✓ Recolectar usuarios y contraseñas
- ✓ Recolectar las credenciales de los usuarios
- ✓ Suplantar a otros usuarios en la red legítima

2.2.2.5.4. Defensa frente a Rogue APs

En la tarea de defender nuestros sistemas frente a este tipo de ataques nos encontramos con dos frentes a defender: el cliente y la infraestructura.

Comencemos por el cliente. El peligro al que se enfrenta el usuario de un terminal móvil es la asociación a un Rogue AP de forma voluntaria o no. Es de sobra conocida la habilidad de Windows XP para manejar las conexiones inalámbricas por sí mismo, y es precisamente esta característica la más apreciada por los atacantes pues el sistema operativo se basa sólo en la intensidad de la señal y el SSID para asociarse a un AP u a otro. Es por ello que los terminales así configurados son presa fácil de los Rogue AP.

El grupo Shmoo, creador entre otros de AIRSNARF, ha desarrollado una herramienta que monitoriza la conexión Wireless del terminal donde está instalado para detectar ataques mediante Rogue APs.

Para ello vigila:

- ✓ Autenticaciones/Desautenticaciones y operaciones masivas.
- ✓ Firma de Rogue APs conocidas
- ✓ Aumento repentino de la intensidad de la señal junto a un cambio de AP.

Estas técnicas no son definitivas pero aumentan sensiblemente la seguridad frente a este tipo de ataques.

2.2.2.6. WPA2

WPA2 (Wi-Fi Protected Access 2), es compatible con su antecesor WPA, proporciona a los administradores de red un alto nivel de fiabilidad que sólo los usuarios autorizados pueden acceder.

Está basado en el estándar IEEE 802.11i ratificado, WPA2, proporciona seguridad a escala mediante la aplicación del Instituto Nacional de Estándares y Tecnología (NIST) FIPS 140-2 algoritmo de encriptación AES. WPA2 se puede activar en dos versiones: WPA2- Personal y WPA2- Enterprise.

La primera protege el acceso no autorizado de la red mediante la utilización de una contraseña, y la segunda verifica los usuarios de la red a través de un servidor respectivamente.

Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA, así mismo está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. El estándar 802.11i fue ratificado en junio de 2004.

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad que la tecnología cumple con estándares de interoperatividad" declaró Frank HazlikManaging Director de la WiFi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i (Panda 2005).

2.2.3. Metodología COBIT 4.1.

2.2.3.1. Estructura de la Metodología COBIT 4.1.

COBIT 4.1 define las actividades de Tecnologías de Información (TI) en un modelo genérico de procesos, estos son cuatro dominios fundamentales de la metodología y tiene distribuidos treinta y cuatro procesos y doscientos catorce objetivos de control generales (IT Governance Institute 2007).

- Planear y Organizar.
- Adquirir e Implementar.
- Entregar y Dar Soporte.
- Monitorear y Evaluar.

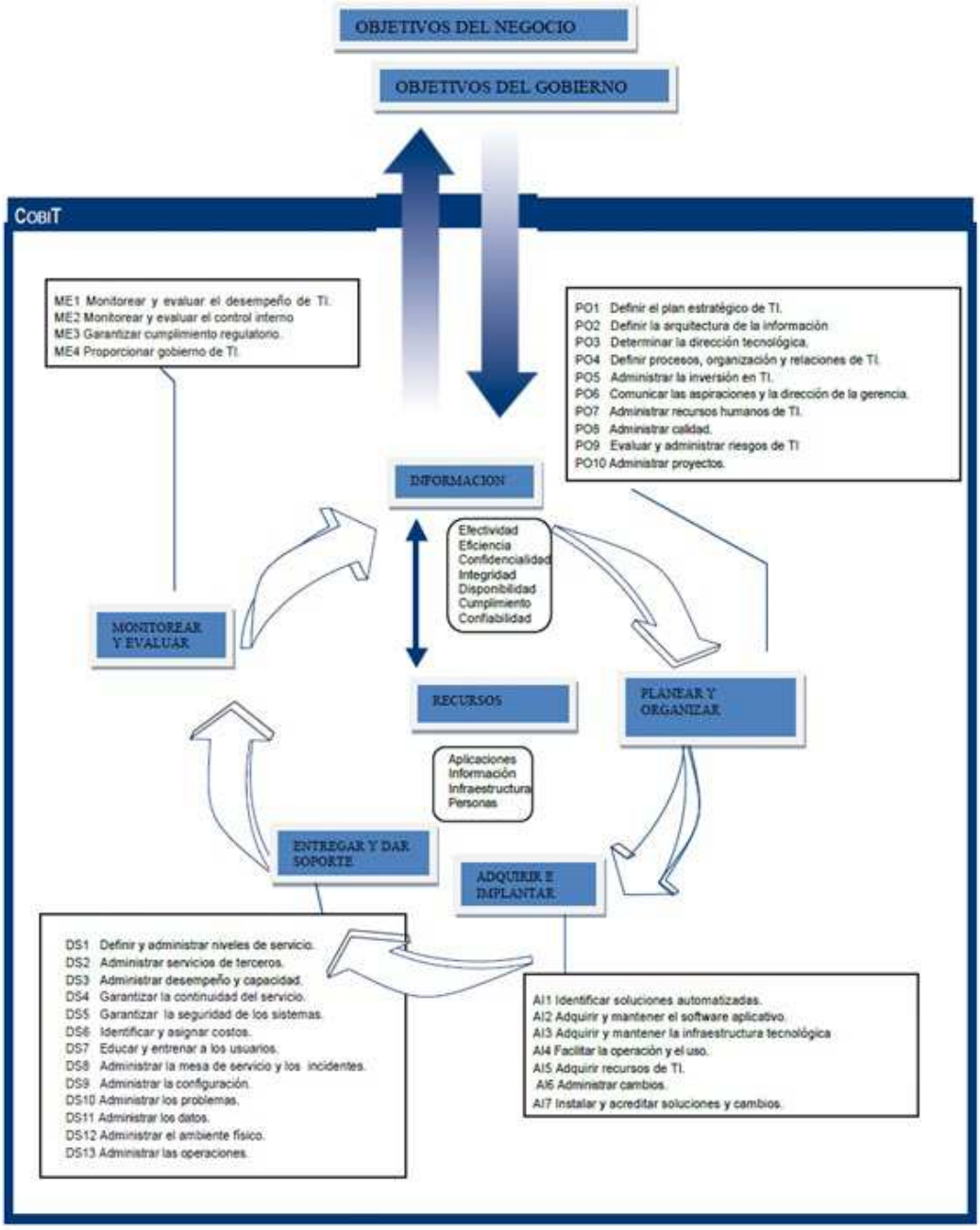

Figura N° 06 Marco de Trabajo de COBIT 4.1
FUENTE: (IT GOVERNANCE INSTITUTE 2007)

Los objetivos principales de estos dominios son:

Planear y Organizar (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.
Los objetivos de control de este dominio son:

PO1 Definir un Plan Estratégico de TI
PO2 Definir la Arquitectura de la Información
PO3 Determinar la Dirección Tecnológica
PO4 Definir los Procesos, Organización y Relaciones de TI
PO5 Administrar la Inversión en TI
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia
PO7 Administrar Recursos Humanos de TI
PO8 Administrar la Calidad
PO9 Evaluar y Administrar los Riesgos de TI
PO10 Administrar Proyectos

Adquirir e Implementar (AI)

Las soluciones de Tecnologías de Información necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones satisfacen los objetivos del negocio.
Los objetivos de control de este dominio son:

AI1 Identificar soluciones automatizadas
AI2 Adquirir y mantener software aplicativo
AI3 Adquirir y mantener infraestructura tecnológica
AI4 Facilitar la operación y el uso
AI5 Adquirir recursos de TI
AI6 Administrar cambios
AI7 Instalar y acreditar soluciones y cambios

Entregar Y Dar Soporte (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.
Los objetivos de control de este dominio son:

DS1 Definir y administrar los niveles de servicio
DS2 Administrar los servicios de terceros
DS3 Administrar el desempeño y la capacidad
DS4 Garantizar la continuidad del servicio
DS5 Garantizar la seguridad de los sistemas
DS6 Identificar y asignar costos
DS7 Educar y entrenar a los usuarios
DS8 Administrar la mesa de servicio y los incidentes
DS9 Administrar la configuración
DS10 Administrar los problemas

DS11 Administrar los datos
DS12 Administrar el ambiente físico
DS13 Administrar las operaciones

Monitorear Y Evaluar (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.
Los objetivos de control de este dominio son:

ME1 Monitorear y Evaluar el Desempeño de TI.
ME2 Monitorear y Evaluar el Control Interno.
ME3 Garantizar el Cumplimiento Regulatorio.
ME4 Proporcionar Gobierno de TI (IT Governance Institute 2007).

2.2.4. Auditoría.

2.2.4.1. Definición

El término de Auditoría empleada en el área financiera, con frecuencia sólo se la consideraba como una evaluación, cuyo único fin era detectar errores y señalar fallas.
Pero la auditoría y el control van más allá de detectar fallas.
La auditoría no sólo detecta errores: "es un examen crítico que se realiza con objetivo de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar acciones alternativas para mejorar la organización y lograr los objetivos propuestos" (Defliese y AICPA 1997).
Algo importante de la auditoría es que "se evalúa para mejorar lo existente, corregir y proponer alternativas de solución" (CGRP 2005).
Por lo que la auditoría no se reduce a la simple evaluación y señalamiento de errores, actualmente la auditoría se realiza a distintas áreas y desde distintos puntos de vista.

2.2.4.2. Clases de auditoría

2.2.4.2.1. Por su amplitud son:

- Auditoría Total: Afecta a todos los elementos de la empresa.
- Auditoría Parcial: Se concentra en determinados elementos de la empresa.

2.2.4.2.2. Por su frecuencia es:

- Auditoría Permanente: Se realiza periódicamente a lo largo del ejercicio económico.

- Auditoría Ocasional: Se realiza de forma esporádica.

2.2.4.2.3. Según el sujeto que la efectúa es:

- Auditoría Interna: Está a cargo de empleados de la propia empresa, encuadrados en un departamento directamente dependiente de la dirección general.
- Auditoría Externa: Está a cargo de auditores profesionales, ajenos a la empresa y totalmente independientes.

2.2.4.2.4. Por su contenido y fines es:

- Auditoría de Gestión: Afecta a la situación global de la empresa.
- Auditoría Financiera: Examen y verificación de los estados financieros de la empresa, para emitir una opinión fundada sobre el grado de fiabilidad de dichos estados.
- Auditoría Contable: Analiza la adecuación de los criterios empleados para recoger los hechos derivados de la actividad de la empresa y su representación, mediante apuntes contables, en los estados financieros.
- Auditoría Operacional: Determina hasta qué punto una organización, unidad o función dentro de una organización, cumple los objetivos establecidos por la gerencia, así como identificar las condiciones que necesiten mejora.

Se extiende a todas las áreas o campos de trabajo como ser:

- Auditoría Organizativa: analiza así la estructura organizativa de la empresa es la adecuada, según las necesidades y problemas de la misma.
- Auditoría Informática: Examen y verificación del correcto funcionamiento y control del sistema informático de la empresa.

En otras palabras, se acepta el término de auditoría para cualquier actividad que implique revisión, evaluación, análisis, estudio, exposición de deficiencias y propuesta de medidas para solucionar o eliminar las mismas, en muchos casos, las fronteras entre los tipos de auditoría no están bien definidas (CGRP 2005).

2.2.5. Auditoría Informática.

Según Ron Weber en Auditing Conceptual Foundations and Practice, la auditoría informática "es la revisión y evaluación de los controles, sistemas y procedimientos de la información de los equipos de computo, su utilización, eficiencia y seguridad de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente confiable y segura de la información que sirva para una adecuada toma de decisiones" (Echenique 2001).

"La Auditoría Informática es una función que ah sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente" (Echenique 2001).

2.2.5.1. Tipos de Auditoría Dentro De La Auditoría Informática.

Dentro de la Auditoría Informática existen varios tipos de auditoría, entre ellas la auditoría física, auditoría de dirección, auditoría del desarrollo, auditoría de mantenimiento, auditoría de seguridad y otros.

- ✓ Auditoría Física: verifica, evalúa y comprueba la funcionalidad, racionalidad y seguridad de los medios físicos.

- ✓ Auditoría de Dirección: el auditor examina el proceso de planificación de sistemas de información y evalúa si es razonablemente.

- ✓ Auditoría del Desarrollo: verifica y evalúa todo el ciclo de vida del software excepto: la explotación, el mantenimiento y el retiro del servicio o aplicación cuando esta tenga lugar.

- ✓ Auditoría de Seguridad, Evalúa las medidas de protección de datos y de los sistemas computarizados, involucrando en forma global Hardware y Software, las medidas de protección a ser utilizadas y los planes de contingencia preparados para enfrentar problemas con o sin conocimiento de causa.

Al finalizar el trabajo de auditoría se obtiene un informe del estado de la institución o unidad auditada, en el desarrollo de la auditoría el auditor obtiene los papeles de trabajo o documentación, que son parte de la evidencia que ayuda a sustentar su opinión (Echenique 2001).

2.2.5.2. Informe de Auditoría.

En todos los casos en que un auditor realiza una revisión, debe expresar una opinión. La opinión, diagnostico o dictamen es la expresión emitida acerca del resultado del proceso de auditoría (Echenique 2001).
Existen cuatro formas de dictaminar:

Dictamen favorable o limpio.

La opinión calificada como favorable, sin salvedades o limpia debe manifestarse de forma clara y precisa, es el resultado de un trabajo realizado sin limitación de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.
Si existen circunstancias que afecten de alguna manera, y no son lo suficientemente importantes como para generar una opinión adversa, se debe incluir un párrafo explicativo y establecer una opinión con salvedades.

Opinión con salvedades.

Se reitera lo dicho en la opinión favorable, al respecto de las salvedades cuando sean significativas en relación con los objetivos de auditoría, describiéndose con precisión la naturaleza y razones, se realiza según las circunstancias siguientes.

- ✓ Limitaciones al alcance del trabajo realizado, restricciones por parte del auditado.
- ✓ Incertidumbre cuyo resultado no permita una previsión razonable.
- ✓ Irregularidades significativas.
- ✓ No hay suficiente evidencia comprobatoria.
- ✓ No hay notas aclaratorias.

Opinión desfavorable o advera.

Establece que no presenta razonablemente los resultados de las operaciones de la entidad, de conformidad con principios generalmente aceptados.
Las excepciones son tan importantes que no le permite emitir una opinión con salvedades, por lo que se incluye los motivos o razones técnicas que le orienten a emitir este tipo de dictamen y los efectos que significan.
La opinión desfavorable o adversa es aplicable en el caso de:

- ✓ Identificación de irregularidades.
- ✓ Incumplimiento de la normativa legal y profesional que afecten significativamente a los objetivos de la auditoría informática estipulados, incluso con incertidumbre; todo ello en la evaluación

de conjunto y reseñando detalladamente las razones correspondientes.

Opinión denegada o abstención de opinión.

Establece que el auditor no expresa una opinión, normalmente por los siguientes motivos:

- ✓ Incertidumbre significativa de un modo tal que impida al auditor formarse una opinión.
- ✓ Irregularidades.
- ✓ Limitación en el alcance de la auditoría.
- ✓ La existencia de incertidumbre cuando su importancia es significativa.
- ✓ La trascendencia que tiene el riesgo de que la empresa no pueda seguir en operación.
- ✓ Falta de información.
- ✓ Incumplimiento de normativa legal y profesional.

2.2.5.3. Hallazgo.

Son las presuntas deficiencias o irregularidades identificadas como resultado de la aplicación de los procedimientos de auditoría, los mismos que con criterios de materialidad o significación económica debidamente desarrollados, referenciados y documentados constarán en los papeles de trabajo.
En la redacción de los hallazgos de auditoría, se debe utilizar lenguaje sencillo y fácilmente entendible, tratando los asuntos en forma objetiva, concreta y concisa.
La comunicación se efectúa por escrito en forma personal y reservada, a la persona directamente vinculada con el hallazgo, debiendo acreditarse su recepción (CGRP 1998).
Los elementos son:

a) Sumilla
Es el título o encabezamiento que resume la observación.

b) Condición
Este término se refiere al hecho irregular o deficiencia determinada, cuyo grado de desviación debe ser demostrada y sustentada con evidencias.

c) Criterio
Es la norma o estándar técnico–profesional, alcanzable en el contexto evaluado, que permiten al auditor tener la convicción de que es necesario superar una determinada acción u omisión de la entidad, en procura de mejorar la gestión. Los más comunes criterios a ser empleados en la auditoría son: las normas jurídicas vigentes, las normas técnicas o estándares profesionales, las opiniones de expertos, indicadores de gestión,

índices de desempeño de años anteriores o de entidades comparables bajo circunstancias iguales, los elementos de la estructura de control interno, recomendaciones de las normas técnicas de control interno para el sector público y los criterios de probidad administrativa.

d) Causa
Es la razón fundamental por la cual ocurrió la condición, o el motivo por el que no se cumplió el criterio o norma. Su identificación requiere de la habilidad y juicio profesional del auditor y es necesaria para el desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición.

e) Efecto
Es la consecuencia real o potencial cuantitativo o cualitativo, que ocasiona la observación, indispensable para establecer su importancia y recomendar a la Administración que tome las acciones requeridas para corregir la condición. Siempre y cuando sea posible, el auditor debe revelar en su informe la cuantificación del efecto (CGRP 1999).

2.2.5.4. Técnicas De Auditoría.

Los mecanismos mediante los cuales los auditores recopilan la evidencia de auditoría. Las técnicas de auditoría consisten en: comparación, cálculo, confirmación, indagación, inspección, observación y examen físico (CGRP 1998).

2.2.5.5. Técnicas De Verificación Física

Inspección, es el examen físico ocular de activos, obras, documentos y valores, con el objeto de establecer su existencia y autenticidad. La aplicación de esta técnica es de mucha utilidad, especialmente en cuanto a la constatación de efectivo, valores, activo fijo y otros equivalentes. Generalmente, se acostumbra a calificarla como una técnica combinada, dado que en su aplicación utiliza la indagación, observación, comparación, rastreo, tabulación y comprobación (CGRP 1998).

2.2.5.6. Técnicas De Verificación Ocular

Comparación, es el acto de observar la similitud o diferencia existente entre dos o más elementos. Dentro de la fase de ejecución de la auditoría se efectúa la comparación de resultados, contra criterios aceptables, facilitando de esa forma la evaluación por el auditor y la elaboración de observaciones, conclusiones y recomendaciones.

Observación, es el examen ocular realizado para cerciorarse cómo se ejecutan las operaciones. Esta técnica es de utilidad en todas las fases de la auditoría, por cuyo intermedio el auditor se cerciora de ciertos hechos y circunstancias, en especial las relacionadas con la forma de ejecución de

las operaciones, apreciando personalmente, de manera abierta o discreta, cómo el personal de la entidad ejecuta las operaciones.

Indagación, es el acto de obtener información verbal sobre un asunto mediante averiguaciones directas o conversaciones con los funcionarios responsables de la entidad. La respuesta a una pregunta formulada por el auditor comprende una porción insignificante de elementos de juicio en los que puede confiarse, pero las respuestas a muchas preguntas que se relacionan entre sí pueden suministrar un elemento de juicio satisfactorio si todas son razonables y consistentes. Es de especial utilidad la indagación en la auditoría de gestión cuando se examinan áreas específicas no documentadas; sin embargo, sus resultados por sí solos no constituyen evidencia suficiente y competente.

Entrevistas, pueden ser efectuadas al personal de la entidad auditada o personas beneficiarias de los programas o actividades a su cargo. Para obtener buenos resultados debe prepararse apropiadamente, especificar quiénes serán entrevistados, definir las preguntas a formular, alertar al entrevistado acerca del propósito y puntos a ser abordados. Asimismo, los aspectos considerados relevantes deben ser documentados y/o confirmados por otras fuentes y su utilización aceptada por la persona entrevistada.

Las Encuestas, pueden ser útiles para recopilar información de un gran universo de datos o grupos de personas. Pueden ser enviadas por correo u otro método a las personas, firmas privadas y otros que conocen del programa o el área a examinar. Su ventaja principal radica en la economía en términos de costo y tiempo; sin embargo, su desventaja se manifiesta en su inflexibilidad, al no obtenerse más de lo que se pide, lo cual en ciertos casos puede ser muy costoso. La información obtenida por medio de encuestas es poco confiable, bastante menos que la información verbal recolectada en base a entrevistas efectuadas por los auditores. Por lo tanto, debe ser utilizada con mucho cuidado a no ser que se cuente con evidencia que la corrobore (CGRP 1998).

2.2.5.7. ISO 27001.

Este estándar internacional fue preparado para proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización (ISO/IEC 2005).

III. MATERIALES Y MÉTODOS

3.1. Tipo y Diseño de la Investigación.

La investigación por ser de carácter aplicativa, se utilizó para la contrastación de la hipótesis correspondiente, el diseño en sucesión o línea (Tabla N° 05) donde se tuvo la participación de un grupo: el experimental, el cual fue evaluado y analizado antes y después de aplicado el estimulo (Buenas prácticas para auditar redes inalámbricas en el rubro hotelero de la ciudad de Chiclayo).

Las conclusiones fueron establecidas por comparación entre la situación antes de la aplicación de la variable estimulo, y la situación después de la aplicación de esta variable.

(Antes) Auditoría de redes inalámbricas basadas en la experiencia demoraba 3 semanas.	--------->	(Estímulo) Buenas prácticas para auditar redes inalámbricas	---------->	(Después) Auditoría de redes inalámbricas utilizando Buenas prácticas demora 2 semanas.

Tabla N° 05: Diseño de la Investigación.

Sin embargo actualmente no se cuenta con una guía de buenas prácticas que sirva de ayuda al auditor con experiencia y sin las herramientas necesarias para la auditoría en redes inalámbricas, en la cual los encargados del control la tomen de apoyo para realizar sus labores, realizándose el proceso de auditoría basados en la experiencia y de la mano con herramientas de monitoreo WLAN, realizándose sólo el monitoreo de canales de emisión, nivel de señal y tipos de claves, tomando más tiempo del que debería al no tener una guía de apoyo en la auditoría a la red inalámbrica.

3.2. Población, Muestra de Estudio y Muestreo.

Población:

La población objeto esta dado por las empresas hoteleras que cuentan con red inalámbrica en la Ciudad de Chiclayo, la cual hacen un total de 10 hoteles, comprobando su existencia y funcionamiento con visitas a las instalaciones de forma personal.

Muestreo:

5 empresas hoteleras aceptaron la aplicación de la encuesta, mas sólo una aceptó la aplicación de la investigación, El Gran Hotel Chiclayo.

NOMBRE	HOTEL	CARGO	Dirección
Elvis Obando	Garza Hotel	Jefe de Sistemas	Bolognesi 756
Juan Carlos Medina	Hotel Costal del Sol	Jefe de Sistemas	Av. Balta 399
Miguel Casusol	Gran Hotel Chiclayo	Systems Manager	Av. Federico Villareal 115
Carlos Sebastiani	Hotel Las Musas	Administrador Externo	Los Faiques No. 101 Urb. Santa Victoria
Roberto Bolívar Zapata	Hotel América	Jefe de Sistemas	Luis Gonzales 943

Tabla N° 06: Población de Hoteles.

Objeto de estudio: empresas hoteleras con redes inalámbricas de la ciudad de Chiclayo.

Muestra: Debido del temor al cambio, la pequeña cantidad de hoteles que cuentan con redes inalámbricas y al compromiso que se pudo llegar con el único hotel, El Gran Hotel Chiclayo, se consideró la misma que aceptó la aplicación de la investigación.

3.3. Hipótesis.

La elaboración de buenas prácticas para auditar redes inalámbricas permitirá mejorar la ejecución de los procesos de auditoría a redes inalámbricas.

3.4. Variables.

Variables Independientes:

- ✓ Buenas prácticas para auditar redes inalámbricas.

Variables Dependientes:

- ✓ Ejecución de los procesos de auditoría a redes inalámbricas.

3.5. Indicadores.

La Tabla N°07 muestra los indicadores que se utilizarán para validar la hipótesis y determinar el cumplimiento de los objetivos de la tesis.

Indicador	Descripción	Unidad de medida
Tiempo de auditoría a la red inalámbrica del	Tiempo dedicado a la auditoría de la red	Entero: Número de semanas.

hotel.	inalámbrica del hotel.	
Número de metodologías, manuales y/o buenas prácticas aplicadas para auditar redes inalámbricas.	Nos indicará la cantidad de metodologías, manuales y/o buenas prácticas utilizadas en la auditoría a la red inalámbrica.	Entero: Cantidad
Número de herramientas aplicadas para auditar la red inalámbrica.	Nos indicará la cantidad de herramientas utilizadas en la auditoría a la red inalámbrica.	Entero: Cantidad
Nivel de experiencia del personal en auditoría de redes inalámbricas.	Nos indicará el nivel de experiencia del personal en auditoría a redes inalámbricas.	Alto Medio Bajo

Tabla N° 07: Indicadores de la Investigación.

3.6. Métodos, Técnicas e Instrumentos de Recolección de datos.

✓ Métodos

Los métodos utilizados en la tesis fueron el análisis, la encuesta y la entrevista, la cual permitieron establecer una relación con el objeto de estudio. El análisis nos permitió hacer una revisión de metodologías, normas y buenas prácticas para auditar redes inalámbricas del territorio nacional e internacional. La entrevista y la encuesta han sido de gran utilidad para recoger información sobre aspectos muy específicos, acerca del nivel de experiencia del personal y las buenas prácticas implementadas en las redes inalámbricas de las empresas hoteleras de la ciudad de Chiclayo.

✓ Técnicas empleadas

Las técnicas empleadas han sido la entrevista, dirigidas a los encargados del área de telecomunicaciones.

✓ Instrumentos

Después de seleccionar los métodos que fueron empleados para las buenas prácticas para auditar redes inalámbricas en las empresas hoteleras, se elaboraron instrumentos para la aplicación e implementación del trabajo, los cuales consisten en **checklist y cuestionarios** (estos constituyen la

herramienta propuesta que ayuda a profesionales interesados en aplicar el presente trabajo), así como también la entrevista y la encuesta, que nos permitió recoger información adicional del área de telecomunicaciones.

3.7. Plan de Procesamiento para Análisis de Datos

Para medir la variable independiente: Buenas prácticas para auditar redes inalámbricas, se hizo uso de la entrevista y el análisis comparativo entre las metodologías, estándares, normas y modelos existentes en el medio nacional e internacional con empresas hoteleras que presentaban red inalámbrica implementada.

Para medir la variable dependiente: Ejecución de los procesos de auditoría a redes inalámbricas, se hizo uso de la encuesta y la entrevista, haciendo el estudio con los 5 hoteles, basándose en frecuencias de auditorías a la red inalámbrica, estándares, metodologías y herramientas basados para realizar dichas auditorías.

3.8. Procesamiento de la Información

Se recopiló la siguiente información para este punto con ayuda de las encuestas y entrevistas aplicadas al responsable del área de telecomunicaciones del Gran Hotel Chiclayo, el cual manifestó los siguientes problemas que ha tenido desde la fecha que se instaló la red inalámbrica hasta el presente.

Problemas más frecuentes dados desde la instalación de la red inalámbrica hasta el momento:

1. Diseño de la red inalámbrica, generación de tiempo y dinero adicional en su modificación o rediseño, debido a que no se basaron en una guía, norma, metodología o buenas prácticas para realizar el diseño de la red inalámbrica acorde a sus necesidades.
2. Escalabilidad, en el 2004 ante la llegada de la fiesta del futbol de la Copa América a Chiclayo, el hotel no imagino la numerosa llegada de equipos de futbol, periodistas y turistas. Lo cual le provoco un gran problema para solucionar la escalabilidad de la red inalámbrica.
3. Alcance y cobertura de la señal débil, en la totalidad de las habitaciones, para ser más precisos en el piso 7 es muy débil, y fuga de señal fuera de los límites del hotel, esto es debido a la falta de medidas preventivas respecto a la infraestructura (muros, columnas, etc.) que actúan como obstáculos, mala ubicación de la mayoría de los equipos que conforman la red, el no haber tenido en cuenta las interferencias y distancias que perturban el buen funcionamiento de la señal inalámbrica, además debido a que no se basaron en una guía, norma, metodología o buenas prácticas para la implementación de la red inalámbrica.

4. El ancho de banda, que les proporciona su proveedor de Internet es de 1 MB, permite trabajar con normalidad a sus pasajeros, trabajando con aplicaciones VPNs, descargas de música y video, chat, etc, pero el problema surge al momento de conexiones simultáneas de pasajeros y personas ajenas al hotel, con un aproximado de 100 – 120 conexiones al día.
5. Con respecto a la seguridad, los mecanismos no cubren en su totalidad, debido a que tienen problemas con conexiones de fuera de los límites del hotel, además debido a que no se basaron en una guía, norma, metodología o buenas prácticas para la seguridad de la red inalámbrica.
6. Los estándares de red que utilizan son 802.11b y 802.11g.
7. La mayoría de equipos que utilizan para la seguridad de su WLAN son de las marcas Linksys y 3com en la calidad del cable UTP CAT 6.

Después de haber revisado y analizado los problemas, recolectados tanto de las entrevistas como también de las encuestas se llegó a las siguientes conclusiones:

- ✓ El hotel requiere una mayor cobertura en sus instalaciones de la red inalámbrica, por lo que es necesario rediseñar la actual red inalámbrica en función del alcance y cobertura, a su vez con la infraestructura del hotel.
- ✓ Ante un crecimiento de la red inalámbrica, se debe prever a futuro un crecimiento.
- ✓ Los estándares 802.11b y 802.11g son más utilizados por la velocidad máxima de transmisión que utiliza, esto hace que sea suficiente para la mayoría de las aplicaciones.
- ✓ La seguridad es muy importante, debido a que se debe tener un mejor control sobre los usuarios, ancho de banda, procesos, etc.

3.9. Metodologías.

3.9.1. Metodologías para la elaboración de la Buenas Prácticas.

Para el desarrollo del presente trabajo de investigación, utilicé diferentes métodos y técnicas según la etapa.
El método utilizado en el presente trabajo de investigación, está basado en el método científico.
Se hizo un estudio a 5 hoteles de la región, entrevistando a los encargados de las respectivas áreas de telecomunicaciones y sistemas, teniendo como resultado un nivel alto de experiencia.
Revisé diferentes metodologías, normas y buenas prácticas para auditar WLAN's, que describo en el marco teórico para elaborar las buenas prácticas.

Dichas metodologías y normas son las siguientes:

- ISO 27002 - (anteriormente denominada ISO17799).

- COBIT 4.1
- Metodología para administrar redes – Sergio Untiveros.
- Seguridad en redes inalámbricas - Geannina Jackeline Aguirre Briones.
- Estudio, diseño e implementación de una red inalámbrica en el instituto tecnológico superior aeronáutico. – Patricio Espín
- Lista de verificación de datos del centro de seguridad física. – The SANS Institute
- Las diez mejores prácticas de ENISA en el campo de la conciencia de seguridad de la información.
- Consultoría estratégica inalámbrica – Red-M
- Plan de cinco pasos para la seguridad de su empresa Wlan" - Core Competence
- Osstmm 2.3 WIRELESS – ISECOM Pete Herzog
- Information Networks Planning and Design (INPD).

De cada de una de las 11 metodologías y normas se describe sus objetivos y como me han servido en la definición de la mejores prácticas para una auditoría de redes inalámbricas.

El modelo ISO – IEC 27002 es la norma dedicada a la seguridad de la información, lo que permite alinear de mejor manera las mejores prácticas, la cláusula fundamental para garantizar la seguridad física es: Seguridad física y ambiental, pero no se debe dejar de lado aspectos organizacionales que ayuden con esta cláusula. En consecuencia para el Dominio de Seguridad se selecciona 9 de las 11 cláusulas que tiene la norma ISO – IEC 27002, se excluye 2 cláusulas completas y los objetivos de control y sub controles que están dirigidos a la parte de seguridad lógica, teniendo así cláusulas y controles exclusivamente para el apoyo de la seguridad física de los recursos de información.

Del modelo internacional COBIT 4.1, se utilizó debido a que hace un análisis y selección de objetivos de control, controles detallados que contemplan aspectos de seguridad física. Cabe aclarar que varios aspectos de COBIT ya son contemplados en el modelo ISO – IEC 27002, pero existen aspectos que no son tomados en cuenta, las cuales se adicionan a las cláusulas y objetivos de control del modelo ISO – IEC 27002.

Del modelo "Metodología para Administrar Redes" – Sergio Untiveros, se utilizó debido a que presenta como objetivo, una visión global para diseñar y administrar redes inalámbricas sin dejar de lado la seguridad, familiarizándose con la terminología utilizada y los diferentes riesgos y tipos de ataques informáticos a los cuales está expuesta, así como también introduce niveles básicos y avanzados de seguridad en la implementación de una red inalámbrica.

Del modelo "Seguridad en redes inalámbricas" - Geannina Jackeline Aguirre Briones, se utilizó debido a que hace un análisis de la visión global del estado de seguridad en las redes inalámbricas, familiarizándose con la terminología utilizada y los diferentes riegos y tipos de ataques informáticos a los cuales está

expuesta la red inalámbrica, introduciendo niveles básicos y avanzados de seguridad en la implementación de la red inalámbrica. Describiendo así los elementos que participan en la solución como los protocolos de red y funcionalidades necesarias para garantizar la seguridad de la red inalámbrica.

Del modelo "Estudio Diseño e Implementación de una red inalámbrica en el Instituto Tecnológico Superior Aeronáutico." – Patricio Espin. Se utilizó debido al propósito fundamental que es el de diseñar e implementar una red inalámbrica paso a paso, con el fin de que poder hacer uso el servicio de Internet e ingresar a la red administrativa del instituto.

Del modelo "Lista De Verificación De Datos Del Centro De Seguridad Física". – The SANS Institute, el presente documento se utilizó debido al portafolio que presenta como lista de verificación informal compilados para crear conciencia sobre los problemas de seguridad física en el entorno del centro de datos. Siendo de vital importancia al momento de auditar los Especialistas en Seguridad de la Información utilicen esta lista para determinar las debilidades en la seguridad física de los centros de datos que su organización utiliza. Abarca aspectos como la penetración física ofreciendo al hacker el acceso a los datos sensibles, la ingeniería social y el acceso físico a los puertos de la consola se facilitan (118-119).

Del modelo "Las Diez Mejores Prácticas De Enisa En El Campo De La Conciencia De Seguridad De La Información.", se utilizó en base a que hace un análisis de los aspectos clave en el campo de la conciencia de la seguridad de la información y la comunicación (TIC) en las empresas. Para ello, las mejores prácticas pueden ser utilizadas para seguridad de la información como una guía para las medidas básicas y para sensibilizar al personal de los riesgos en la seguridad de la información y explicar las diez reglas de oro.

Del modelo "Consultoría estratégica inalámbrica" de Red-M., mediante este documento se propone definir exactamente cómo, cuándo y dónde se utiliza Wireless en la organización, para asegurarse de alinear totalmente la estrategia Wireless con la estrategia de negocio. Permitió consolidar los objetivos de control para el Dominio de Diseño.

Del modelo "Plan De Cinco Pasos Para La Seguridad De Su Empresa Wlan" de Core Competence, se utilizó en base a que hace un análisis de cinco pasos esenciales para la salvaguardia de los clientes inalámbricos y de datos para la auditoría y el control de conexiones Wi-Fi, recomendando las mejores prácticas para garantizar la seguridad y la integridad de las redes empresariales.

Del modelo "OSSTMM 2.9 WIRELESS" de ISCOM Pete Herzog. Se utilizó este manual debido a que es un estándar profesional para pruebas de seguridad en cualquier medio de afuera hacia adentro, y un conjunto entendible de test. Como pruebas de seguridad continuarán desarrollándose para ser una válida y respetada profesión. Estos son una seria de pasos que deben estar en observación y revisados durante la realización de una prueba completa. El cuadro metodológico que es el camino optimo de dirección de esto con parejas de probadores.

Del modelo "Information Networks Planning and Design" for David Etheridge Errol Simón se utilizó debido a que presenta objetivos ambiciosos como: explicar el proceso y proponer una metodología para el análisis de información de la red y el diseño de una visión de sistemas orientados. La metodología es precedida y apoyada por una discusión a fondo de las necesidades de comunicación y las tecnologías de redes. Los autores también abordan cuestiones de organización y gestión que están influenciados por las redes de información.

De acuerdo a estas consideraciones, las buenas prácticas propuestas evalúan de forma completa los dominios de Diseño, Administración y Seguridad de la red inalámbrica de acuerdo a los conceptos ya mencionados de las metodologías, estándares y normas nacionales e internacionales.

Para cada buena práctica definida se propone su objetivo o propósito de la buena práctica, actividades o tareas a desarrollar, herramientas y un Checklist que estén de acuerdo a los conceptos que maneja, para esto se realiza lo siguiente:

- El diseño y construcción de dominios diseño, administración y seguridad de las buenas prácticas para auditar redes inalámbricas.
- El diseño y construcción de las buenas prácticas para auditar WLAN por cada dominio.
- El diseño y construcción del objetivo de la buena práctica para auditar WLAN.
- El diseño y construcción de las actividades o tareas de la buena práctica.
- El diseño y construcción de las herramientas que apoyará la labor de la auditoría.
- El diseño y construcción del Checklist de la buena práctica para apoyar la labor del auditor.

3.9.2. Metodologías para la aplicación de la auditoría.

Para la aplicación de la auditoría, hojas de trabajo e informe de auditoría se basó en el estándar de International Standards for the Profesional Practice of Internal Auditing Copyright © 2001 by The Institute of Internal Auditors, tales como:

- En cuanto a la fase de planificación de la auditoría me basé en NAGU 2.10. (Planificación General) y NAGU 2.20. (Planeamiento de la Auditoría),
- En cuanto a la fase de ejecución e informe, me basé en NAGU 4.10. (Elaboración del Informe) y NAGU 4.40. (Estructura del Informe)

Entre las técnicas de auditoría se utilizaron técnicas de verificación ocular como la observación, técnicas de verificación oral como indagación, entrevistas y encuestas, técnicas de verificación física como inspección, además de la utilización de herramientas asistidas por el computador como: InSSIDer y Xirrus.

A continuación una breve explicación de las metodologías utilizadas para la aplicación de la auditoría:

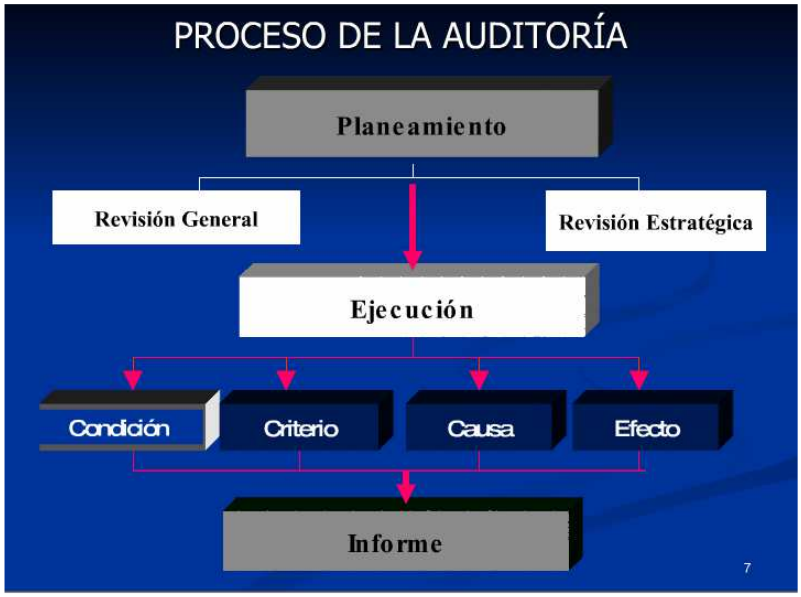

Figura N° 07: Proceso de la auditoría
FUENTE: [CONTRERAS LLALLICO, 2010]

A) PLANEAMIENTO: Plan de auditoría. Programa de auditoría.

NAGU 2.10: PLANIFICACIÓN GENERAL

- ✓ Objetivos:
- ✓ Alcance:
- ✓ Metodología a utilizar:

NAGU 2.20: PLANEAMIENTO DE LA AUDITORÍA

- ✓ Objetivos del examen. Son los resultados que se esperan alcanzar
- ✓ Alcance del examen. Grado de extensión de las labores de auditoría.
- ✓ Descripciones de las actividades de la entidad.
- ✓ Normas aplicables a la entidad.
- ✓ Informes a emitir y fecha de entrega
- ✓ Identificación de las áreas críticas.
- ✓ Personal nombre y categoría de los auditores.
- ✓ Funcionarios de la entidad a examinar.
- ✓ Presupuesto de tiempo.
- ✓ Participación de otros profesionales.
- ✓ Papeles de trabajo,

B) EJECUCIÓN: Comunicación de hallazgos. Borrador de informe.

HALLAZGO: Condición, criterio, causa, efecto

C) FORMULACION DEL INFORME

NAGU 4.10: ELABORACIÓN DEL INFORME:
Informe: Emisión del informe

- ✓ Supervisión de la estructura y contenido del borrador del informe administrativo y debido respaldo en papeles de trabajo.
- ✓ Evaluación de los comentarios de la entidad y supervisión del informe administrativo final.
- ✓ Supervisión de las observaciones, conclusiones, recomendaciones y el proceso de determinación de las responsabilidades, administrativas, civiles o penales.
- ✓ Supervisión del informe especial de ser el caso.
- ✓ Revisión final y suscripción de los informes.
- ✓ Trámite de aprobación y remisión del Informe a la entidad.

NAGU 4.40: CONTENIDO DEL INFORME.

ESTRUCTURA DEL INFORME
I. INTRODUCCIÓN
1. Origen del examen
2. Naturaleza y objetivos del examen
3. Alcance del examen
4. Antecedentes, base legal de la entidad
5. Comunicación de hallazgos
6. Memorándum de control interno
7. Otros aspectos de importancia.
II. OBSERVACIONES.
III. CONCLUSIONES (observaciones)
IV. RECOMEDACIONES (Conclusiones)
V. ANEXOS
Firma
Síntesis Gerencial

3.10. Dominios y/o escenarios de las Buenas Prácticas.

En esta sección veremos los escenarios que contemplan las buenas prácticas para auditar redes inalámbricas.
Basándome en la encuesta realizada a los 5 hoteles de la ciudad de Chiclayo y la entrevista que se tuvo con el encargado del área de telecomunicaciones, se pudo analizar la información, y se determinó tres dominios que cubran en su totalidad la red inalámbrica, que son el diseño, la administración y la seguridad de la red inalámbrica de la empresa.
En cada dominio describo su finalidad y qué aspectos contempla, como se puede mostrar a continuación:

1. Dominio Diseño.
Para este dominio se realizó el análisis de metodologías orientadas al diseño, infraestructura y hardware de las WLAN's, alineadas a la verificación de planes, normas, fuentes de diseño, implementación, migración de una WLAN; infraestructura, examinar la ubicación, temperatura, infraestructura, limites de señal de la red y equipos de comunicación sean adecuadas permitiendo un funcionamiento óptimo de la red empresarial; Hardware, examinar que los equipos de la WLAN soportadas en la empresa sean los adecuados para el funcionamiento de la misma, y sean acordes con las necesidades de la empresa, y finalmente se obtuvo un marco de trabajo de auditoría de diseño de las WLAN's. Se determinaron objetivos de control orientados a:

1. Análisis de la empresa.
2. Análisis tecnológico de la empresa.
3. Diseño Físico de la Red
4. Diseño Lógico de la Red.
5. Planes de Implementación.

2. Dominio Administración de la Red.
Para este dominio se realizó el análisis de metodologías orientadas a la administración de las WLAN's, alineadas a verificar, comprobar, analizar, examinar la continuidad de la operación constante de la WLAN soportadas en la empresa; obteniendo finalmente un marco de trabajo de auditoría de administración de WLAN's. Se determinaron objetivos de control orientados a:

1. La administración de recursos informáticos.
2. La administración de recursos humanos.
3. La administración de comunicaciones y operaciones.
4. La administración de control de accesos.

3. Dominio Seguridad.
Para este dominio se realizó el análisis de metodologías orientadas a la seguridad de las WLAN's, alineadas a verificar, comprobar, analizar, examinar la seguridad de las operaciones, transacciones de información constante de la WLAN, abarcando pruebas de seguridad externa, que va de un ambiente no privilegiado a uno privilegiado, asimismo examinar que existan controles, procedimientos y políticas de seguridad que permitan monitorear las operaciones, transacciones de información constante de la WLAN, obteniendo finalmente un marco de trabajo de auditoría de hardware de WLAN's.
Se determinaron objetivos de control orientados a:

1. Política de seguridad de la información en la WLAN.

2. Organización de la seguridad de la información en la WLAN.
3. Seguridad WLAN.
4. Gestión de incidentes de seguridad de información en la WLAN.

IV. RESULTADOS

4.1. Diseño y construcción de las buenas prácticas para auditar redes inalámbricas.

A continuación se muestra el diseño y construcción de las buenas prácticas para auditar redes inalámbricas siguiendo la metodología vista en el punto 3.9.1.

4.1.1 Características de las buenas prácticas para auditar redes inalámbricas.

Las buenas prácticas propuestas tienen tres características que se detallan a continuación.

- Los requisitos establecidos en las Buenas Prácticas para auditar redes inalámbricas son genéricas y están previstos a ser aplicables en toda institución hotelera o independiente del tipo, tamaño o su naturaleza.
- Está enfocada a los dominios de diseño, administración y seguridad de la red inalámbrica.
- Adecuado a nuestra realidad, ya que las buenas prácticas considera las recomendaciones de metodologías, normas y documentos nacionales e internacionales en Auditoría WLAN.

De acuerdo a estas consideraciones, las buenas prácticas propuestas evalúan de forma completa los dominios de diseño, administración y seguridad de la red inalámbrica de acuerdo a los conceptos ya mencionados de las metodologías, estándares y normas nacionales e internacionales.

Para cada buena práctica definida se propone su objetivo o propósito de la buena práctica, actividades o tareas a desarrollar, herramientas y un checklist que estén de acuerdo a los conceptos que maneja, para esto se realiza lo siguiente:

- El diseño y construcción de dominios diseño, administración y seguridad de las buenas prácticas para auditar redes inalámbricas.
- El diseño y construcción de las buenas prácticas para auditar WLAN por cada dominio.
- El diseño y construcción del objetivo de la buena práctica para auditar WLAN.
- El diseño y construcción de las actividades o tareas de la buena práctica.
- El diseño y construcción de las herramientas que apoyará la labor de la auditoría.
- El diseño y construcción del Checklist de la buena práctica para apoyar la labor del auditor.

4.1.2 Definición de las buenas prácticas para auditar redes inalámbricas.

En este punto se van a mostrar y detallar los dominios diseño, administración y seguridad, y por cada dominio las buenas prácticas para auditar redes inalámbricas basándome en las metodologías, normas y documentos existentes en el medio nacional e internacional.
Para más detalle de los estándares, buenas prácticas, metodologías y guías tomadas en cuenta para la definición de las buenas prácticas para auditar redes inalámbricas ver Anexo N°04.

4.1.2.1 Dominio Diseño.

Buena Práctica Dis001: Análisis de la Empresa

Objetivo: Verificar información general y relevante que permita tener una perspectiva general de la empresa respecto a su modelo de negocio.

Actividades:
- Analizar información general como giro de la empresa, ubicación geográfica, estructura orgánica, distribución física actual (plano arquitectónico).
- Revisar objetivos de las empresas como: Misión, visión, análisis FODA.
- Analizar la arquitectura del sistema, su descomposición funcional (áreas de la empresa), arquitectura del proceso de la información, análisis de los problemas encontrados.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Formato De Análisis De La Empresa	Anexo N° 05	Físico	Plantilla que permitirá hacer un levantamiento de información propia de la organización.

Tabla N° 08: Formato de Análisis de la empresa.

Checklist

	Buena Práctica DIS001: Análisis de la Empresa	SI	NO	N/A
1	¿La empresa ha definido formalmente su misión y visión?			
2	¿Cuentan con un análisis FODA?			
3	¿Cuentan con un manual de organización y funciones?			
4	¿La empresa tiene en claro sus objetivos?			
5	¿Cuenta con un plan estratégico?			
6	¿Los cambios tecnológicos están acordes con el plan estratégico?			
7	¿La empresa cuenta con el plano arquitectónico actualizado de la distribución física actual?			
	TOTAL			

Tabla N° 09: Checklist de Buena Práctica DIS001

Buena Práctica DIS002: Análisis tecnológico de la empresa.

Objetivo: Verificar información general y relevante que permita tener una perspectiva tecnológica de la empresa.

Actividades:
- Verificar si se cuentan con un inventario de los equipos existentes y aplicaciones de escritorio, etc.
- Verificar si los componentes de red y equipos de conexión son acorde a las necesidades de la organización y satisfacen a los usuarios.
- Verificar si los elementos de la red están trabajando sin problemas.
- Verificar cobertura, interferencia, canal y ancho de banda de la señal inalámbrica.
- Verificar si presentan saturación los canales de la red inalámbrica.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
MSIA 5.1 Analizador de inventario de software	http://www.microsoft.com/spain/softlegal/msia/default.aspx	Software Gratuito	Herramienta diseñada para realizar un inventario de software.
Total network inventory 2.0.1	http://www.softinventive.com/es/products/total-network-inventory/	Software Gratuito	Solución de escaneo de redes, inventario de software y hardware y auditoría de PC.
Inventario de estaciones	ANEXO N° 06	Físico	Plantilla que permitirá hacer un levantamiento de información de estaciones de trabajo.
Inventario de dispositivos inalámbricos	ANEXO N° 06	Físico	Plantilla que permitirá hacer un levantamiento de información de los dispositivos inalámbricos.
Cuestionario para el análisis tecnológico de la organización	ANEXO N° 07	Físico	Cuestionario que permitirá realizar un análisis tecnológico básico de telecomunicaciones.

Tabla N° 10: Herramientas de Buena Práctica DIS002

Checklist

	Buena Práctica DIS002: Análisis tecnológico de la empresa		SI	NO	N/A
1	¿Cuentan con un inventario de los equipos existentes?				
2	¿Se cuenta con una lista de las aplicaciones de escritorio, proceso, etc.?				
3	¿El ancho de banda es acorde con las necesidades de la organización?				
4	¿La topología definida es acorde con las necesidades de la organización?				
5	¿El estándar con el que está trabajando es acorde con las necesidades de la organización?				
6	¿El cifrado de la red inalámbrica es la adecuada?				
7	¿La autenticación de la red inalámbrica es la adecuada?				
8	¿La red inalámbrica trabaja con más de un canal?				
9	¿Presenta problemas con la cobertura de los puntos de acceso en las áreas con mayor concentración de usuarios?				
10	¿Presenta fuentes de interferencia en la señal inalámbrica?				
11	¿La red inalámbrica presenta problemas de saturación con sus canales?				
12	¿Las cantidades de ancho de banda utilizada por cada uno de los enlaces es la óptima?				
13	Los equipos de conexión son los óptimos, tales como:	Servidor Principal: Controlador De Dominio Y DNS?			
14		Servidor Secundario: Proxy, Firewall, Radius, Enrutamiento, Vlan?			
15		Servidor Base Datos?			
16		Servidor De Archivos E Impresión?			
17		Router?			
18		Switch Principal?			
19		Switch Secundario?			
20		Puntos de acceso?			
21		Adaptadores De Red?			
22	¿Los componentes de red que más solicitudes hacen y atienden están trabajando sin problemas, como estaciones de trabajo, puertos y servicios?				
23	¿Los Puntos de acceso implementados cubren con su señal inalámbrica todas las áreas de la organización?				
	TOTAL				

Tabla N° 11: Checklist de Buena Práctica DIS002

Buena Práctica DIS003: Diseño físico de la red

Objetivo: Verificar información general y relevante que permita tener una perspectiva del diseño físico de la red de la empresa.

Actividades:

- Verificar si la ubicación de los equipos de red es la adecuada.
- Revisar el nivel de saturación de los canales.
- Verificar los canales de emisión son los adecuados.
- Verificar la topología de la red, estándar inalámbrico, las frecuencias y los protocolos son las adecuadas.
- Verificar la configuración de los equipos de red es la adecuada.
- Verificar que se realicen pruebas de conectividad física.
- Verificar si el número de puntos de acceso cubren toda la red.
- Verificar el alcance de la red inalámbrica dentro y fuera de las instalaciones.
- Verificar si la sala de equipos de comunicación presenta un ambiente adecuado.
- Verificar si se aplicó alguna norma, documento o buenas prácticas para la implementación de la sala de servidores.
- Verificar la interconexión de la red inalámbrica a la red cableada o Internet.
- Verificar la compatibilidad de los equipos de red.
- Verificar la correcta administración de los equipos de red y comunicación.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
AirWave VisualRF Report	http://www.arubanetworks.com/products/management-security-software-2/airwave/visualrf/	Software Licenciado	Herramienta para el auditor que da una visión precisa de toda la red sin tener que abandonar su escritorio.
Network Event Viewer	http://network-event-viewer.softonic.com/descargar	Software Gratuito	Controlador de AP's que permite gestionar eventos de red como alarmas, cobertura, localización de usuarios, etc.
AirWave Wireless Site Plan	http://www.moonblinkwifi.com/airwavetech.cfm	Software Licenciado	Herramienta de monitorización.

Tabla N° 12: Herramientas de Buena Práctica DIS003

Checklist

	Buena Práctica DIS003: Diseño físico de la red		SI	NO	N/A
1	¿La ubicación de los equipos de comunicación es la adecuada?				
2	¿Los canales de emisión de la señal es la adecuada?				
3	¿El nivel de saturación de los canales?				
4	¿La topología definida es acorde con las necesidades de la empresa?				
5	¿La topología existente satisface las necesidades de los usuarios?				
6	¿El estándar inalámbrico propuesto satisface las necesidades de ancho de banda actual?				
7	¿Los protocolos inalámbricos propuestos satisfacen las necesidades de la empresa?				
8	¿La configuración de seguridad de los equipos de red es la adecuada?				
9	¿La red presenta puntos muertos de señal?				
10	¿El número de Puntos de acceso cubren toda la red?				
11	¿Están ubicados correctamente los puntos de acceso?				
12	¿La configuración de los equipos, contraseñas, autenticación es la adecuada?				
13	¿El alcance de la red inalámbrica dentro y fuera de las instalaciones es la adecuada?				
14	¿La sala de equipos de comunicación presenta un ambiente adecuado?				
15	¿Se diseño la sala de servidores con:	Sistema de aire acondicionado?			
16		Sistema eléctrico y de respaldo de energía – UPS?			
17		Sistema de detección y extinción contra incendios?			
18		Sistema de cámaras de seguridad?			
19	¿Se aplicó alguna norma, documento o buenas prácticas para la implementación de la sala de servidores?				
20	¿Se verificó la interconexión de la red inalámbrica a la red cableada es la adecuada?				
21	¿La red presenta problemas con la compatibilidad en los equipos de red y comunicación?				
22	¿Presenta un esquema de cobertura de la red?				
23	¿Frecuentemente los clientes inalámbricos pierden conexión con la red?				
24	¿En ocasiones al navegar por internet los clientes inalámbricos se han quejado de que las páginas cargan muy lentamente?				
25	¿Se realizan pruebas de envío y recibo de archivos para detectar fallos?				

26	¿Ante un problema de conexión o señal inalámbrica se revisa el número de usuarios conectados a la red inalámbrica?			
27	¿Presenta problemas de compatibilidad en los equipos de red?			
28	¿Los puntos de acceso están apagados durante parte del día cuando no esté en uso?			
29	¿La función "Reset" de los puntos de acceso es utilizado sólo por personal autorizado y sólo cuando sea absolutamente necesario?			
30	¿Los puntos de acceso se restauran con los ajustes de seguridad más recientes después de la función de reinicio?			
31	¿Las interfaces de gestión de los puntos de acceso tienen la autenticación de usuarios?			
32	¿Todos los puntos de acceso tienen fuertes contraseñas administrativas?			
33	¿Todas las contraseñas administrativas se cambian con regularidad y se almacena de forma segura?			
34	¿Los routers inalámbricos, Gateways y puntos de acceso no almacenan la contraseña de administrador en texto plano en la base de información de gestionada (MIB) por defecto?			
35	¿Los Puntos de acceso se encuentran ubicados en zonas seguras, de tal forma que se pueda evitar la sustracción por personas ajenas?			
36	¿Se realizó una inspección del lugar para medir y establecer la cobertura del punto de acceso para la organización luego de la instalación?			
37	¿Los puntos de acceso fueron implementados lejos de redes inalámbricas cercanas para evitar una posible denegación de servicio por causa problemas de interferencia?			
	TOTAL			

Tabla N° 13: Checklist de Buena Práctica DIS003

Buena Práctica DIS004: Diseño lógico de la red.

Objetivo: Verificar información general y relevante que permita tener una perspectiva del diseño lógico de la red de la empresa.

Actividades:

- Verificar si las cuentas de usuario por dominio y equipos es la adecuada.
- Verificar que se realicen pruebas de conectividad lógica.
- Verificar si la autenticación de los usuarios es la correcta.
- Verificar si los niveles de acceso a los recursos compartidos es la recomendada.
- Verificar la tasa de transferencia de la red inalámbrica.
- Verificar si se determinó el sistema operativo correcto de red para equipos de comunicación y estaciones de trabajo basado en las necesidades de la organización.
- Verificar si el protocolo de red es el adecuado.
- Verificar si se suministraron herramientas necesarias para poder implementar mecanismos para acceso remoto.
- Verificar la configuración, autenticación y cifrado de los equipos de comunicaciones.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Secure shell	http://openssh.softonic.com/ http://en.kioskea.net/download/download-1423-ssh-secure-shell	Software Gratuito	Herramienta para estaciones de trabajo es flexible cliente SSH que permite conectarse de forma segura a aplicaciones remotas.
Administración Remota EMCO	http://emcosoftware.com/remote-administration	Software Licenciado	Herramienta para la implementación remota que ayuda a los administradores del sistema para ejecutar los paquetes y scripts
Comandos "Ping" y "Traceroute".	Dispositivos de comunicación	Comandos	Comandos ayudarán a realizar pruebas de conectividad lógica.

Tabla N° 14: Herramientas de Buena Práctica DIS004

Checklist

	Buena Práctica DIS004: Diseño lógico de la red	SI	NO	N.A.
1	¿Los nombres de cuentas de usuario de dominio están estandarizados?			
2	¿Todos los usuarios tienen su cuenta de usuario?			
3	¿Se realizan pruebas punto a punto entre entidades finales?			
4	¿Se realizan pruebas salto por salto entre entidad origen y cada elemento intermedio?			
5	¿Los dispositivos de red inalámbrica interfieren con otros dispositivos electrónicos en las frecuencias similares, tales como teléfonos inalámbricos, microondas, etc.			
6	¿Los usuarios presentan restricciones para el acceso a la red inalámbrica?			
7	¿Los usuarios presentan problemas para reconocer la red inalámbrica?			
8	¿La empresa cuenta o utiliza un modelo basado en dominios?			
9	¿El sistema operativo de red para equipos de comunicación y estaciones de trabajo está basado en las necesidades de la empresa o es el adecuado?			
10	¿Se determinó como protocolo de red TCP/IP?			
11	¿Se da mantenimiento a las cuentas de usuario?			
12	¿Los usuarios son autenticados para poder acceder a los recursos compartidos?			
13	¿Se determinó los niveles de acceso a los recursos compartidos?			
14	¿Se suministraron herramientas necesarias para poder implementar mecanismos de integridad como MD5, entre otras?			
	Configuración, autenticación y cifrado de equipos inalámbricos			
15	¿El servicio set identifier (SSID) por defecto del punto de acceso ha sido cambiado?			
16	¿La cadena de caracteres SSID es fácil de adivinar y refleja información sobre la empresa (nombre, ubicación, función, productos...)?			
17	¿El router inalámbrico, punto de acceso o puerta de enlace utiliza el 'Nombre de red' o SSID por defecto?			
18	¿Las claves se almacena en texto plano?			
19	¿Los protocolos de gestión inseguros e innecesarios en los puntos de acceso han sido desactivados?			
20	¿Los parámetros por defecto han sido cambiados en los puntos de acceso?			
21	¿Los tamaños de clave de cifrado son de por lo menos 128 bits, o lo más grande posible?			

22	¿Las claves por defecto son reemplazadas por claves únicas más seguras?			
23	¿El firewall ha sido correctamente configurado y se ha instalado entre la infraestructura de la red cableada y la red inalámbrica?			
24	¿Mediante la red inalámbrica es posible acceder a la red cableada?			
25	¿Hay dispositivos en la red inalámbrica que están siempre en partes sensibles de la red cableada?			
26	¿Las tecnologías WLAN tienen los últimos parches de seguridad y actualizaciones?			
27	¿Los usuarios se autentican (RADIUS local, Kerberos...) con nombre de usuario y contraseña para la red WLAN?			
28	¿La autenticación de red es susceptible a la reproducción de autenticaciones anteriores para tener acceso a recursos de red?			
29	¿Se utiliza IPSec en lugar del predeterminado WEP como el protocolo de seguridad?			
30	¿Se utiliza el protocolo de autenticación 802.1x?			
31	¿Un algoritmo de cifrado más seguro que el algoritmo RC4 por defecto está en uso (3DES o AES)?			
32	¿La autenticación del usuario a la WLAN es obtenida a través de métodos más seguros (datos biométricos, tarjetas inteligentes, autenticación de dos factores, PKI, RSA...)?			
33	¿Si no es totalmente necesario el DHCP, está desactivado.			
34	¿El acceso se concede únicamente a las máquinas cliente con direcciones MAC registradas?			
35	¿Todas las funciones de seguridad posible que se proporcionan en la arquitectura están en uso?			
36	¿Todos los clientes inalámbricos tienen software antivirus instalado?			
37	¿Todos los clientes inalámbricos tienen firewall instalado?			
	TOTAL			

Tabla N° 15: Checklist de Buena Práctica DIS004

Buena Práctica DIS005: Planes de implementación.

Objetivo: Verificar información relevante sobre la implementación WLAN.

Actividades:

- Verificar si la organización cuenta con el suficiente recurso humano para implementar la red.
- Verificar si se desarrollaron, documentaron e informaron planes de contingencia y planes de implementación de red.
- Verificar si se hizo un estudio de compatibilidad de hardware y software existente con el instalado.
- Verificar si se documentan los cambios para futuras referencias.
- Verificar si existe un presupuesto asignado para la red inalámbrica.
- Verificar la calendarización de actividades en la implementación.
- Verificar las pruebas de implementación de la red diseñada.

Checklist

	Buena Práctica DIS005: Planes de implementación	SI	NO	N.A.
1	¿La implementación de la red inalámbrica fue realizada por personal calificado?			
2	¿Existe un plan o calendarización de implementación de red?			
3	¿Existe un plan de administración de red?			
4	¿Existe un plan de contingencia?			
5	¿Existe un plan financiero?			
6	¿Existe un estudio previo para asegurar que el software que será instalado es compatible con los componentes ya existentes?			
7	¿Se notificó anticipadamente a los usuarios sobre la implementación o algún cambio en la red?			
8	¿Se documenta todo cambio para futuras referencias?			
9	¿Se cumplió con los tiempos para cada actividad presentado en el calendario de actividades?			
10	¿Se realizaron pruebas de conectividad al culminar la implementación?			
11	¿El presupuesto asignado para la red inalámbrica fue suficiente?			
	TOTAL			

Tabla N° 16: Herramientas de Buena Práctica DIS005

4.1.2.2. Dominio: Administración

Buena Práctica ADM001: Administración de recursos informáticos.

Objetivo: Verificar la administración y protección apropiada de los recursos y asegurar que la información reciba un apropiado nivel de protección.

Actividades:

- Verificar la existencia de un inventario de los equipos inalámbricos.
- Verificar la existencia de procedimientos para el uso aceptable de los equipos inalámbricos.
- Verificar las actualizaciones de los equipos inalámbricos.
- Verificar la clasificación de la información en términos de su valor, sensibilidad, criticidad y modo de suministrarla a los empleados.
- Verificar el desarrollo e implementación de procedimientos de manejo de información en la red inalámbrica.

Herramientas

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Network Event Viewer	http://network-event-viewer.softonic.com/descargar	Software	Herramienta que le permite al auditor y usuario controlar los APs, para gestionar alarmas, cobertura, localización de usuarios, etc.
MSIA 5.1 Analizador de Inventario de Software	http://www.microsoft.com/spain/softlegal/msia/default.aspx	Software Gratuito	Herramienta diseñada para realizar un inventario de su software.
Total Network Inventory 2.0.1	http://www.softinventive.com/es/products/total-network-inventory/	Software Gratuito	Solución de escaneo de redes, inventario de software y hardware y auditoría de PC.
Inventario de estaciones de trabajo.	ANEXO N° 06	Físico	Plantillas que le permite al auditor realizar un inventario de las estaciones de trabajo.
Inventario de equipos inalámbricos	ANEXO N° 06	Físico	Plantillas que le permite al auditor realizar un inventario de los equipos inalámbricos.

Tabla N° 17: Herramientas de Buena Práctica ADM001

Checklist

	Buena Práctica ADM001: Administración de recursos informáticos.	SI	NO	N/A
	RESPONSABILIDAD POR LOS RECURSOS.			
	INVENTARIO DE RECURSOS			
1	¿Todos los equipos inalámbricos son claramente identificados?			
2	¿Se realiza y mantiene un inventario de los equipos inalámbricos?			
3	¿El inventario de los recursos incluye toda la información necesaria para la recuperación ante un desastre?			
	USO ACEPTABLE DE LOS EQUIPOS INALÁMBRICOS			
4	¿Son documentados e implementadas políticas de uso de los equipos inalámbricos?			
5	¿Se informa al personal sobre las políticas de uso de los equipos inalámbricos?			
7	¿El personal cumple con las políticas de uso de los equipos inalámbricos?			
8	¿Se aplican las últimas actualizaciones a todos los equipos inalámbricos que la soporten?			
10	¿Las actualizaciones para los equipos inalámbricos se despliegan sobre una base regular?			
11	¿Todos los dispositivos inalámbricos se han configurado correctamente de forma que no hay dispositivos no autorizados en la red?			
13	¿Los registros de acceso contienen dispositivos no autorizados con acceso a la red inalámbrica?			
	ADMINISTRACIÓN DE LOS EQUIPOS INALÁMBRICOS			
14	¿Los puntos de acceso están apagados durante parte del día cuando no esté en uso?			
15	¿La función "Reset" de los puntos de acceso es utilizado sólo por personal autorizado y sólo cuando sea absolutamente necesario?			
16	¿Los puntos de acceso se restauran con los ajustes de seguridad más recientes después de la función de reinicio?			
17	¿Las interfaces de gestión de los puntos de acceso tienen la autenticación de usuarios?			
18	¿Todos los puntos de acceso tienen fuertes contraseñas administrativas?			
19	¿Todas las contraseñas administrativas se cambian con regularidad y se almacena de forma segura?			
20	¿Los routers inalámbricos y puntos de acceso no almacenan la contraseña de administrador en texto plano en la base de información gestionada (MIB) por defecto?			
21	¿Se tiene configurado VPN para usuarios de red remotos?			
23	¿Toda configuración vía web impulsada por el router o punto			

	de acceso está desactivada?			
24	¿La configuración de puntos de acceso y routers inalámbricos sólo pueden realizarse a través de acceso al puerto serial?			
25	¿La gestión del tráfico de puntos de acceso está en una subred dedicada?			
26	¿La configuración SNMP en los puntos de acceso ha sido configurada con los menores privilegios (sólo lectura)?			
27	¿Si no se utiliza SNMP[2] se desactiva?			
28	¿El punto de acceso gestiona el tráfico protegido con SNMPv3 o criptografía equivalente?			
	TOTAL			

Tabla N° 18: Checklist de Buena Práctica ADM001

[2] El Protocolo Simple de Administración de Red

Buena Práctica ADM002: Administración de recursos humanos.

Objetivo: Verificar que los empleados tengan claro sus responsabilidades y obligaciones sobre la red inalámbrica y poder reducir el riesgo de robo, fraude o mal uso de los equipos inalámbricos, a su vez estén conscientes de amenazas e inquietudes de la seguridad inalámbrica, y caso tengan que dejar el empleo salgan de manera ordenada.

Actividades:
- Verificar que se hallan definido y documentado los roles y responsabilidades de los empleados para la red inalámbrica.
- Comprobar que se halla firmado los términos y condiciones de su contrato de empleo, estableciendo sus roles y responsabilidades y las de la organización concerniente a la red inalámbrica.
- Verificar la aplicación de la seguridad inalámbrica por parte de los empleados.
- Comprobar la capacitación de los empleados en políticas y procedimientos de seguridad inalámbrica.
- Verificar el establecimiento de un procedimiento disciplinario formal para empleados que han cometido una falta o violación a la seguridad inalámbrica.
- Verificar la asignación y definición clara de las responsabilidades del empleado al finalizar o cambiar el empleo ante la red inalámbrica.
- Verificar la devolución de los equipos inalámbricos en posesión por parte de los empleados al finalizar su empleo.
- Verificar el retiro de los derechos de acceso a la red inalámbrica a los empleados al finalizar su empleo.

CHECK LIST

	Buena Práctica ADM002: Administración de recursos humanos.	SI	NO	N/A
	PREVIO A LA CONTRATACIÓN			
	ROLES Y RESPONSABILIDADES			
1	¿Son definidos los roles y responsabilidades de los empleados sobre la red inalámbrica?			
2	¿Son documentados los roles y responsabilidades de los empleados sobre la red inalámbrica?			
3	¿Estos roles y responsabilidades de los empleados están de acuerdo a las necesidades de la organización?			
	TÉRMINOS Y CONDICIONES DE EMPLEO			
4	¿Los empleados acuerdan y firman los términos y condiciones del contrato de empleo?			
5	¿El contrato de empleo establece las responsabilidades del empleado y las de la organización concerniente a la red inalámbrica?			
6	¿Se aclara, establece y firman acuerdos de confidencialidad o no divulgación aquellos que tendrán acceso a la red inalámbrica?			

	DURANTE EL EMPLEO			
	DURANTE EL EMPLEO			
7	¿Se verifica y solicita que los empleados apliquen seguridad inalámbrica de acuerdo con las políticas y procedimientos de seguridad?			
8	¿Todos los empleados son capacitados para el desempeño de sus funciones sobre la WLAN?			
9	¿Se motiva a los empleados para cumplir con políticas de seguridad inalámbrica?			
	TOMA DE CONCIENCIA, EDUCACIÓN Y ENTRENAMIENTO SOBRE SEGURIDAD WLAN			
10	¿Todos los empleados son capacitados regularmente en concientización y actualización de políticas y procedimientos de seguridad inalámbrica relevantes para su función?			
11	¿Se realizan capacitaciones a los empleados de modo que le permita reconocer problemas e incidentes en la red inalámbrica?			
	PROCESO DISCIPLINARIO			
12	¿Se sigue un proceso disciplinario formal para empleados que han cometido una falta en la red inalámbrica?			
13	¿Se inicia el proceso disciplinario después de una previa verificación de que ah ocurrido una falta en la red inalámbrica?			
14	¿El proceso disciplinario asegura un tratamiento correcto y justo para los empleados sospechosos?			
15	¿En casos de mala conducta los procesos permiten el retiro inmediato de sus derechos y obligaciones?			
	PERSONAL DE LIMPIEZA			
16	¿El equipo de limpieza es restringido a la sala de telecomunicaciones para evitar algún sabotaje?			
17	¿Si el personal de limpieza debe tener acceso a la sala de telecomunicaciones es acompañado por personal de la misma área?			
18	¿Se permite el acceso a los visitantes a la sala de telecomunicaciones sin aprobación escrita?			
	FINALIZACIÓN O CAMBIOS DE EMPLEADO			
	FINALIZACIÓN DE RESPONSABILIDADES			
19	¿Están claramente definidas y asignadas las responsabilidades para llevar a cabo la finalización o cambio del empleo?			
	RETORNO DE RECURSOS			
20	¿Todos los empleados devuelven todos los equipos inalámbricos de la organización que están a su cargo al finalizar su empleo?			
21	¿En caso de que los empleados compran o usan su propio equipamiento se asegura que la información es transferida a la organización?			
	ELIMINACIÓN DE DERECHOS DE ACCESO			
22	¿Los derechos de acceso a la red inalámbrica son retirados, anulados o se ajustan al finalizar su empleo?			

23	¿Los derechos de acceso a la red inalámbrica e instalaciones son reducidos o eliminados antes de terminar o cambiar el empleo?			
24	¿Se cambian todas las contraseñas de cuentas que siguen activas a la finalización o cambio de empleados?			
	TOTAL			

Tabla N° 19: Checklist de Buena Práctica ADM002

Buena Práctica ADM003: Administración de comunicaciones y operaciones inalámbricas.

Objetivo: Verificar la correcta y segura operación de la red inalámbrica, para mantener la integridad y disponibilidad de la información a los usuarios, previniendo la divulgación no autorizada, modificación o interrupción de las comunicaciones y operaciones inalámbricas.

Actividades:
- Verificar el registro de todos los cambios a la red inalámbrica.
- Verificar la documentación, mantenimiento y disponibilidad de procedimientos de operación inalámbrica a los usuarios.
- Verificar la asignación y distribución de roles y responsabilidades a los usuarios, para reducir las oportunidades de modificación no autorizada o no intencional o mal uso de la red inalámbrica.
- Verificar la existencia de copias de respaldo de configuración de los equipos inalámbricos.

CHECK LIST

	Buena Práctica ADM003: Administración de comunicaciones y operaciones inalámbricas.	SI	NO	N/A
	PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIÓNALES			
	GESTIÓN DE CAMBIOS			
1	¿Los cambios en la WLAN están controlados?			
2	¿Se establecen responsabilidades de gestión para asegurar el control de manipulación de equipos inalámbricos?			
	DISTRIBUCIÓN DE OBLIGACIONES			
3	¿Los roles y responsabilidades son asignados y distribuidos para reducir las oportunidades de modificaciones no autorizadas, no intencionales o mal uso de la red inalámbrica?			
4	¿Se controla que ninguna persona pueda acceder, modificar o utilizar los recursos WLAN sin autorización o sin ser detectado?			
	RESPALDO			
	RESPALDO DE INFORMACIÓN			
5	¿Se hacen copias de respaldo de configuración de equipos inalámbricos y se pone a prueba?			
6	¿Se realizan registros exactos y completos de las copias de respaldo de equipos inalámbricos?			
7	¿Presenta procedimientos documentados de restauración de copias de respaldo?			
8	¿Las copias de respaldo de configuración de equipos inalámbricos se almacenan fuera del edificio o a una distancia suficiente para evitar daños o desastre que ocurra en la organización?			
9	¿Las copias de respaldo de configuración de equipos			

	inalámbricos se almacenan en un ambiente seguro y vigilado?			
10	¿Las copias de respaldo de configuración de equipos inalámbricos se eliminan de forma segura y sin riesgo usando procedimientos cuando ya no son requeridos?			
	TOTAL			

Tabla N° 20: Checklist de Buena Práctica ADM003

Buena Práctica ADM004: Administración de control de accesos

OBJETIVO: Verificar el acceso de usuarios autorizados y no autorizado a la red inalámbrica.

ACTIVIDADES:
- Comprobar la existencia de políticas de control de acceso.
- Comprobar la existencia de procedimientos formales para el registro y cancelación de usuarios.
- Verificar la asignación, uso y restricción de privilegios a la red inalámbrica.
- Comprobar la existencia de un proceso formal y documentado de seguridad para la selección, asignación, uso y control de contraseñas.
- Comprobar el uso de buenas prácticas de seguridad,
- Verificar que las estaciones de trabajo desatendidas tengan protección apropiada.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Recomendaciones en relación a la gestión y establecimiento de contraseñas.	ANEXO N° 08	Físico	Recomendaciones para el usuario, que le van ayudar en la selección de contraseñas seguras.
MaxPassword	http://www.max2k.com/	Software	Aplicación disponible para el usuario, diseñada para generar passwords seguros al azar.
Password Generator	http://gratis.portalprogramas.com/Password-Generator.html	Software	Aplicación disponible para el usuario, permite generar contraseñas aleatorias muy seguras y muy difíciles de romper combinando diferentes caracteres.
Password Strength Analyser and Generator	http://password-strength-analyser-and-generator.softonic.com/	Software	Aplicación disponible para el auditor y usuario, permite comprobar la seguridad de las contraseñas, si no queda satisfecho, crear nuevas contraseñas.

Tabla N° 21: Herramientas de Buena Práctica ADM004

Checklist

	Buena Práctica ADM004: Administración de control de accesos	SI	NO	N/A
	CONTROL DE ACCESOS			
	POLÍTICAS DE CONTROL DE ACCESO A LA RED INALÁMBRICAS			
1	¿Se establece, documenta y revisa políticas de seguridad de control de acceso a la red inalámbrica?			
2	¿Las reglas de control acceso a la red inalámbrica consideran reglas aplicables y opcionales?			
3	¿Las reglas de control de acceso a la red inalámbrica son apoyadas por procedimientos formales y responsabilidades claramente definidas?			
	GESTIÓN DE ACCESOS A USUARIOS A LA RED INALÁMBRICAS			
	REGISTRO DE USUARIOS A LA RED INALÁMBRICA			
4	¿Existe un procedimiento formal para registrar y suprimir el acceso de usuarios a la red inalámbrica?			
5	¿Se comprueba que el nivel de acceso a la red inalámbrica concedido es apropiado y acorde con el cargo que tiene el empleado en la organización?			
6	¿Se proporciona a los usuarios una declaración escrita de sus derechos de acceso a la red inalámbrica?			
7	¿Se remueve o bloquea inmediatamente los derechos de acceso a la red inalámbrica de usuarios que han cambiado roles o trabajos, o dejan la organización?			
	REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS			
8	¿Se revisa los derechos de acceso a la red inalámbrica de usuarios en intervalos regulares usando un proceso formal?			
9	¿Las asignaciones de privilegios a la red inalámbrica son comprobadas al momento de iniciar su primera sesión y a intervalos regulares para asegurar que los privilegios no autorizados no son obtenidos?			
	RESPONSABILIDADES DE LOS USUARIOS			
	USO DE CONTRASEÑAS			
10	¿Se exige a los usuarios que sigan buenas prácticas de seguridad en la selección y empleo de contraseñas?			
11	¿Cuando el usuario tiene acceso a múltiples servicios o sistemas y tiene una sola contraseña de calidad se asegura el nivel de protección?			
12	¿Se cambia las contraseñas en intervalos regulares de tiempo y se asegura de no reutilizar las contraseñas?			
	EQUIPOS DE USUARIOS DESATENDIDOS			
13	¿Los usuarios aseguran que el equipamiento desatendido tiene la protección apropiada?			
14	¿Se aconseja a los usuarios a finalizar su sesión activa cuando			

	han terminado de usar el servicio y hacer uso de una contraseña o llave para bloquearlo?			
15	¿La información sensible o crítica está protegida cuando el computador está desocupado?			
16	¿Los computadores y terminales están apagados o protegidos mediante mecanismos de cierre de pantallas y bloqueo de teclado?			
	TOTAL			

Tabla N° 22: Checklist de Buena Práctica ADM004

4.1.2.3. Dominio: Seguridad

Buena Práctica SEG001: Política de seguridad de las TICs.

Objetivo: Verificar el apoyo y dirección de las políticas de seguridad en la red inalámbrica de acuerdo a los requisitos de la organización.

Actividades:
- Verificar la existencia de un documento de política de seguridad en la red inalámbrica.
- Verificar que se haya comunicado las políticas de seguridad a los usuarios de la red inalámbrica.
- Verificar que se revise y actualice las políticas de seguridad en la red inalámbrica en intervalos planificados o cuando exista cambios significativos para asegurar su continuidad, actualización adecuada y eficacia.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Recomendaciones para la concientización en seguridad de información	Anexo N° 09	FISICO	Formato disponible para el usuario, es una guía de recomendaciones para la seguridad en la red inalámbrica.

Tabla N° 23: Herramientas de Buena Práctica SEG001

Checklist:

	Buena Práctica SEG001: Política de seguridad de la TICs	SI	NO	N/A
	DOCUMENTOS DE POLÍTICA DE SEGURIDAD DE LAS TIC'S			
1	¿Presenta políticas de seguridad para la red inalámbrica?			
2	¿Se han implementado dichas políticas de seguridad para la red inalámbrica?			
3	¿La Política de Seguridad sobre la red inalámbrica es aprobada por la dirección, publicada y comunicada?			
4	¿Se puntualiza dentro de la organización los objetivos, alcance e importancia de la seguridad en la red inalámbrica?			
5	¿Se asignan roles y responsabilidades para cada una de las actividades de las políticas de seguridad?			
6	¿Se monitorea la correcta ejecución de las políticas de seguridad?			
7	¿Se asegura que las políticas de seguridad son accesibles, correctas, entendidos y actualizados?			
8	¿Las políticas de seguridad están estandarizadas e integradas			

	para permitir una administración y mejora?				
9	¿Se asegura de que las políticas de seguridad se implementan y comunican a todo el personal relevante?				
10	¿Se lleva un control del porcentaje del personal que entiende las políticas de seguridad?				
11	¿Se lleva un control del porcentaje del personal que cumple con las políticas de seguridad?				
12	¿Las políticas de seguridad incluyen el monitoreo, detección y reporte de las vulnerabilidades e incidentes de seguridad?				
13	¿El documento de Política de seguridad en la red inalámbrica	Tiene el propósito de apoyar a los objetivos y principios de seguridad en la red inalámbrica de acuerdo con la estrategia del negocio y los objetivos de la empresa?			
14		Incluye controles de seguridad para la red inalámbrica?			
15		Presenta una breve explicación de los principios, normas y el cumplimiento de requisitos de importancia?			
16		Define responsabilidades generales y especificas de seguridad en la red inalámbrica para el reporte de incidentes de seguridad?			
17		Presenta documentos de referencia adicionales que apoyan al documento de política de seguridad en la red inalámbrica?			
	REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD EN LAS TIC's				
18	¿Existe un responsable encargado de realizar el mantenimiento y revisión del documento de política de seguridad en la red inalámbrica?				
19	¿Se programan revisiones periódicas del documento de política de seguridad en la red inalámbrica?				
20	¿La dirección conserva un registro de las revisiones hechas al documento de política de seguridad en la red inalámbrica?				
	TOTAL				

Tabla N° 24: Checklist de Buena Práctica SEG001

Buena Práctica SEG002: Organización de la seguridad inalámbrica.

Objetivo: Verificar la gestión de seguridad inalámbrica dentro de la organización.

Actividades:
- Verificar la coordinación de las actividades de seguridad inalámbrica.
- Verificar la definición clara de todas las responsabilidades de la seguridad inalámbrica.
- Verificar la identificación y revisión de los acuerdos de confidencialidad o no divulgación para la protección de la información en la WLAN.
- Verificar la identificación de riesgos en la red inalámbrica.
- Verificar los requisitos de seguridad inalámbrica identificados, antes de dar acceso a la información y a recursos de la organización.
- Verificar la gestión de todos los acuerdos con los empleados que involucran acceso, proceso, comunicación o gestión de la información de la organización mediante la WLAN.

Checklist:

	Buena Práctica SEG002: Organización de la seguridad inalámbrica.	SI	NO	N/A
	COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD INALÁMBRICA			
1	¿La dirección apoya activamente la seguridad inalámbrica dentro de la organización?			
2	¿Se proporciona recursos necesarios para la seguridad inalámbrica?			
3	¿Las actividades de seguridad inalámbrica son coordinadas por representantes de la organización de diferentes áreas?			
4	¿Se aprueban buenas prácticas y procesos de seguridad inalámbrica?			
5	¿Se define claramente todas las responsabilidades para la seguridad inalámbrica?			
6	¿Los niveles de autorización están claramente definidos y documentados?			
7	¿Los acuerdos de confidencialidad y/o no divulgación para la protección de la información de la organización, son identificados y revisados regularmente?			
8	¿Se tiene un proceso establecido para la notificación e informe de divulgación no autorizada?			
9	¿Se mantiene contacto con grupos u empresas especializadas en seguridad inalámbrica?			
10	¿Se tiene acuerdos para compartir información a fin de mejorar la cooperación y coordinación en los asuntos de seguridad inalámbrica?			
	IDENTIFICACIÓN DE RIESGOS			
11	¿Son identificados los riesgos de la información en la WLAN			

	que provengan de personas ajenas a la organización?			
12	¿Se manejan prácticas y procedimientos para manejar incidentes de seguridad inalámbrica?			
	Dirigiendo la seguridad			
13	¿Se implementa adecuados controles de seguridad inalámbrica en relación al acceso para clientes inalámbricos de la organización?			
	TRATANDO LA SEGURIDAD			
14	¿Se toman las medidas de seguridad inalámbrica necesarias antes de conceder acceso a la información y a los recursos?			
	TOTAL			

Tabla N° 25: Checklist de Buena Práctica SEG002

Buena Práctica SEG003: Implementación de la seguridad inalámbrica

Objetivo: Verificar el acceso físico y lógico no autorizado, daños e interferencias a los dispositivos inalámbricos de la organización, a su vez la pérdida, daño, robo o compromiso de los mismos.

Actividades:

- Verificar el perímetro de seguridad WLAN, comprobando que la señal no es alcanzada fuera de la organización.
- Verificar que existan controles físicos de entrada
- Verificar la protección y ubicación de los dispositivos inalámbricos en una zona segura
- Verificar el control de acceso y habilidad para interceptar o interferir con la comunicación inalámbrica.
- Verificar que no existan interferencias con otros dispositivos inalámbricos.
- Verificar la posibilidad de capturar y obtener información desde los dispositivos inalámbricos.
- Verificar el cifrado en uso.
- Verificar que protocolos de autenticación utiliza la red inalámbrica.
- Verificar que protocolos de encriptación utiliza a red inalámbrica.
- Verificar que tipos de protección utiliza la red inalámbrica.

Herramientas:

HERRAMIENTA	DISPONIBILIDAD	TIPO	DESCRIPCIÓN
Backtrack	http://www.remote-exploit.org/BackTrack/	Software	Herramienta que le permite al auditor realizar pruebas de penetración y seguridad, permitiendo descubrir vulnerabilidades.
Insider	http://inssider.softonic.com/descargar	Software	Es una herramienta que permite al auditor monitorizar la calidad de la señal de redes inalámbricas, y controlar de un modo gráfico la intensidad de la señal.
Herramienta completa de cálculo de pérdida de señal WIFI	http://www.paramowifix.net/antenas/calculoenlacewlan.html	Software	Cálculo de pérdida de potencia, propagación, recepción, en espacio abierto a 2.45Ghz, propagación difracción
Xirrus Wifi Inspector	http://xirrus-wi-fi-	Software	Función de localización con sonidos. Gráfico con historial de

	inspector.softonic.com/		potencia de la señal. Exportación de redes a archivos CSV. Atajos a pruebas de calidad de la conexión
Calcula pérdida de señal y potencia	http://hwagm.elhacker.net/calculo/calcularalcance.htm	Software	Herramienta que le permite al auditor realizar un cálculo de la pérdida de señal y potencia.
Datos de pérdidas de señal	http://camyna.com/2006/05/31/pérdida-de-senal-wifi/	Software	Herramienta que le permite al auditor realizar un cálculo de la pérdida de señal y potencia.
WPA PSK (Raw Key) Generator	http://www.wireshark.org/tools/wpa-psk.html	Software	El Wireshark WPA pre compartida Key Generator es una herramienta útil para el usuario, ofrece una manera fácil de convertir una frase de contraseña WPA y SSID a la de 256-bit pre-compartida ("raw") clave que se utiliza para la derivación de claves

Tabla N° 26: Cuadro de herramientas de Buena Práctica SEG003

Checklist:

	Buena Práctica SEG003: Implementación de la seguridad inalámbrica.		SI	NO	N/A
	PERIMETRO DE SEGURIDAD WLAN				
1	¿Son definidos y usados perímetros de seguridad WLAN para proteger la señal inalámbrica y los dispositivos inalámbricos?				
2	¿Los perímetros del edificio son físicamente sólidos que no permiten la fuga de señal?				
3	¿El personal de servicio ajeno la sala de telecomunicaciones tiene restringido la manipulación o configuración de los dispositivos inalámbricos?				
4	¿Los derechos de configuración de los dispositivos inalámbricos son revisados y actualizados regularmente o revocados cuando es necesario?				
5	¿Los equipos inalámbricos están ubicados en zonas estratégicas que permitan cubrir el área con la señal inalámbrica?				
6	¿La sala de telecomunicaciones.	Está situada en un lugar que evita el acceso del público?			
7		Está en un lugar cerrado?			
8		Cuenta con sensores o alarmas que avisen a la oficina de soporte informático la ocurrencia de alguna eventualidad?			
9		Cuenta con cámaras que avisen a la oficina de informática de algún sabotaje?			
10		Presenta materiales o paredes inflamables en su			

		interior?			
11		Está diseñada contra el daño proveniente de fuego, inundaciones, terremoto, explosión, convulsión civil, y otras formas de desastre natural u ocasionadas por el hombre?			
12		Se supervisa las actividades en su interior?			
	SEGURIDAD DE LOS EQUIPOS DE COMUNICACIÓN				
	UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS DE COMUNICACIÓN				
13	¿Los dispositivos inalámbricos son ubicados y protegidos estratégicamente para reducir los riesgos de amenaza, ambientales y las oportunidades para el acceso no autorizado?				
14	¿Los dispositivos inalámbricos están protegidos de fallas de energía?				
15	¿Los dispositivos inalámbricos cuentan con UPS?				
	CONTROL DE ACCESO Y HABILIDAD PARA INTERCEPTAR O INTERFERIR CON LA WLAN				
16	¿El nivel de control de acceso físico (cámaras, etc.) a los dispositivos inalámbricos es la recomendable?				
17	¿Los lugares donde la comunicación inalámbrica se extiende más allá de los límites físicos de la organización y la distancia que se extiende, presentan clientes inalámbricos potencialmente peligrosos?				
18	¿Se puede acceder a la red inalámbrica utilizando antenas comunes de alta ganancia en los límites de las instalaciones?				
19	¿Las medidas de seguridad que se encuentran en el lugar donde la comunicación inalámbrica sea superior a los límites físicos (cámaras, detección de movimiento...) son las adecuadas?				
20	¿Se determina qué tipo de información puede o no ser enviado a través de enlaces inalámbricos?				
	DISPOSITIVOS INALÁMBRICOS DE MANO (PDA, POCKET PC, PALM, ETC)				
21	¿Los usuarios intercambian datos en forma cifrada?				
22	¿Los dispositivos inalámbricos de mano utilizan métodos de autenticación robustas?				
23	¿Los dispositivos inalámbricos de mano tienen contraseña activada para proteger los datos si el dispositivo se pierde o es robada?				
24	¿Todos los dispositivos inalámbricos de mano tienen mecanismo que automáticamente le pide al usuario una contraseña después de un período de inactividad?				
25	¿El software antivirus está instalado en dispositivos inalámbricos de mano?				
26	¿Existen interferencias con otros dispositivos inalámbricos o electrónicos en las frecuencias en las que operan?				
27	¿El cifrado que está en uso actualmente en los dispositivos				

	inalámbricos considera que es el más robusto?					
28	¿La red utiliza protocolos de autenticación como:	Kerbeos?				
29		Radius?				
30		Diameter?				
31		Tacas?				
32		Tacas +?				
33		NTML?				
34		WPA/PSK?				
35	¿La red utiliza protocolos de encriptación como:	SSH?				
36		TLS?				
37		SSL?				
38		3DES?				
39		CCMP?				
40		PSK?				
41	¿La red está protegida a través de:	Firewall o IDS?				
42		WEP?				
43		WPA?				
44		WPA2?				
45		VPN?				
46	¿Se han implementado herramientas de:	Monitoreo	Inssider?			
47						
48			Xirrus Inspector?			
49		Seguridad	BackTrack?			
50			AirCrack?			
			WifiSlax?			
51			WifiWay?			
	TOTAL					

Tabla N° 27: Checklist de Buena Práctica SEG003

Buena Práctica SEG004: Gestión de incidentes de seguridad inalámbrica.

Objetivo: Verificar que sean comunicados de manera que permita tomar una acción correctiva oportuna a los eventos y debilidades de seguridad inalámbrica.

Actividades:
- Verificar la existencia de informes de eventos de seguridad inalámbrica a través de canales de gestión apropiados lo más rápido posible.
- Verificar que los empleados anoten y reporten cualquier debilidad de seguridad inalámbrica observada o sospechada.
- Verificar la existencia de responsabilidades y procedimientos para asegurar una respuesta rápida, eficiente, y ordenada a los incidentes de seguridad inalámbrica.
- Verificar la recolección, retención y presentación de evidencia cuando se ha dado una acción de seguimiento contra un empleado después de un incidente de seguridad inalámbrica.

Checklist

	Buena Práctica SEG004: Gestión de incidentes de seguridad de la información en la WLAN	SI	NO	N/A
	REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN			
1	¿Los eventos de seguridad inalámbrica son reportados tan pronto es posible?			
2	¿Los empleados son conscientes y reportan los eventos de seguridad inalámbrica?			
3	¿Se tiene establecido un encargado a quien se reporte los eventos de seguridad inalámbrica?			
	INFORME DE DEBILIDADES DE SEGURIDAD INALÁMBRICAS			
4	¿Los empleados saben identificar y comunicar cualquier debilidad de seguridad inalámbrica observada o sospechada en la organización?			
5	¿El mecanismo de reporte es fácil, accesible y está disponible?			
6	¿Se advierte a los empleados que será responsabilidad legal para quien realice pruebas a fin de demostrar la existencia de debilidades de seguridad inalámbrica?			
7	¿Se prohíbe la realización de pruebas a fin de demostrar la existencia de debilidades de seguridad inalámbrica?			
8	¿Se hace un seguimiento a un empleado recolectando y presentando evidencia después de un incidente de seguridad inalámbrica.			
	TOTAL			

Tabla N° 28: Checklist de Buena Práctica SEG004

4.2. Caso de aplicación Gran Hotel Chiclayo

4.2.1. EJECUCIÓN. Comunicación de hallazgos. Borrador de informe.

Se ejecutó en el periodo quincena Noviembre 2011 – finales Noviembre 2011, con el respaldo del personal del hotel, el Ing. Miguel Casusol – Gerente de sistemas de la organización. Se realizaron entrevistas con diferentes objetivos cada una, en la primera y segunda fue un bosquejo general de la situación actual del hotel, haciendo preguntas abiertas en las que el gerente de sistemas explicaba como inicio la implementación de la red inalámbrica, su migración y crecimiento, los inconvenientes que tuvo en el transcurso de la implementación. Sin dejar de lado habló de los equipos de comunicación con los que inició la red inalámbrica, su crecimiento a los equipos que actualmente cuentan y la ubicación de los mismos.

En las entrevistas siguientes se aplicaron las buenas prácticas, se dividió en tres partes, diseño, administración y seguridad, en cada parte se utilizó aproximado de 1 a máximo 2 días en aplicación por módulo, en esos dos días se desarrollaban las actividades de cada módulo Diseño, Administración y Seguridad, se aplicaban los checklist y herramientas de monitoreo de red en caso sea necesario.

Respecto al dominio diseño se verificó los planes, normas, fuentes de diseño, implementación, se examinó la ubicación, temperatura, infraestructura, límites de señal de la red y equipos de telecomunicación del Gran Hotel Chiclayo.

Respecto al dominio administración se verificó, comprobó, analizó y examinó la continuidad de las operaciones constantes basadas en la administración de los recursos informáticos, humanos, de comunicaciones y operaciones y los controles de accesos en la WLAN.

Respecto al dominio de seguridad se verificó las operaciones, transacciones de información constante de la WLAN, asimismo se examinó que existan controles, procedimientos y políticas de seguridad que permitan monitorear las operaciones, transacciones de información constante de la WLAN.

Al finalizar el desarrollo de la auditoría se presenta el resultado que fueron 04 hallazgos, los cuales son falta de seguridad en la señal inalámbrica del hotel, contraseñas de los equipos de comunicación no son cambiadas periódicamente y no son almacenadas en lugar seguro, puntos de acceso no adecuados para la red inalámbrica y el limitado ancho de banda; de los cuales se detalla su titulo del hallazgo, condición, criterio, causa, efecto y recomendación (ANEXO N°03).

4.3. Informe: Emisión del informe

El caso de aplicación fue realizado en el periodo quincena Noviembre 2011 – finales Noviembre 2011 en el Gran Hotel Chiclayo, con el respaldo del personal del hotel, el Ing. Miguel Casusol – Gerente de sistemas de la organización.

En la presente auditoría se realizaron cuatro etapas, la 1ra Etapa de planificación general basada en NAGU 2.10, la 2da Etapa de planeamiento de la auditoría basada en NAGU 2.20, la 3ra Etapa de ejecución y la 4ta Etapa de contenido del informe basada en NAGU 4.40

Al principio como primer punto se realizó la planificación general (Anexo n°01), luego se identificó objetivos, alcance y metodología a utilizar.

Como segundo punto el planeamiento de la auditoría (Anexo n°02), donde se identificó los objetivos del examen, alcance del examen, descripciones de las actividades de la entidad, informes a emitir y fecha de entrega, personal nombre, funcionarios de la entidad a examinar, presupuesto de tiempo y papeles de trabajo.

Como tercer punto tenemos a la ejecución de la auditoría (Anexo n°03), donde se identificaron los hallazgos, comunicación de los mismos con su respectiva condición, criterio, causa y efecto.

Para luego pasar al 4to y último punto que es el informe (Anexo n°03), identificando origen del examen, naturaleza y objetivos del examen, alcance del examen, antecedentes, base legal de la entidad, comunicación de hallazgos, observaciones, conclusiones (observaciones), recomendaciones (Conclusiones), ANEXOS y Firma.

V. DISCUSION

Las soluciones de una red inalámbrica otorgan una serie de beneficios y posibilidades hoy en día. Estas deben ser bien conocidas por las empresas para identificar con suficiente anticipación las oportunidades que les brindan, tanto para crear productos mejores, más competitivos y de mayor valor, como para explorar nuevas rutas de gestión en los negocios, para que sean competitivos en costes, más innovadores o se adapten mejor a las nuevas condiciones del entorno o del mercado. La conectividad, la localización o la identificación a distancia son las funciones básicas que los sistemas inalámbricos brindan.

Sin embargo, a todas estas bondades también aparecen problemas como es el de diseño, administración y seguridad en la red inalámbrica, los cuales son elementos que han sido inconveniente para que en la actualidad grandes empresas tengan problemas con el uso de esta tecnología, y a su vez materia de investigacion en la presente tesis.

En este capítulo se hará un análisis de los resultados de la aplicación de las buenas prácticas para auditar redes inalámbricas, en Gran Hotel Chiclayo. El análisis estará enfocado a evaluar los indicadores planteados en el capítulo III. Estos indicadores son:

- Tiempo de auditoría a la red inalámbrica del hotel.
- Número de metodologías, manuales y/o buenas prácticas aplicadas para auditar redes inalámbricas.
- Número de herramientas aplicadas para auditar la red inalámbrica.
- Nivel de experiencia del personal en auditoría de redes inalámbricas.

5.1 Casos analizados

En el presente trabajo de investigación se obtuvo una guía de buenas prácticas que incluyen los dominios de diseño, administración y seguridad, una solución segura para la red inalámbrica, en base buenas prácticas con sus respectivas actividades o tareas a desarrollar acompañado de herramientas de auditoría, un cuestionario y un checklist de forma que se podrá así desarrollar una auditoría Wlan, basándome en marcos, metodologías y buenas prácticas adicionales como "Information Networks Planning and Design (INPD), Osstmm Wireless 2.9, Metodología Para Administrar Redes, Instituto Superior Aeronáutico, ISO 27002, COBIT 4.1, RED – M, LVD Centro seguridad física. Tras revisar los siguientes casos se obtuvo que:

CASO N° 01: Wi-Fi RF AUDIT

Wi-Fi RF AUDIT se centra sólo en "responder a los problemas de acceso del usuario, rendimiento y servicio, tratar con los problemas de seguridad, planificación para el crecimiento, integración de nuevas tecnologías, comprobación de una red nueva o existente y establecer una línea de base de diseño para la instalación de nuevas redes Wi-Fi" no ayudando en

mucho al desarrollo de las buenas prácticas y limitándose sólo a la parte de administración WLAN.

En base que las buenas prácticas desarrolladas tienen un campo más amplio, y para complementar las mismas, se recurrió de marcos adicionales.

CASO N° 02: Plan de cinco pasos para la seguridad del Enterprise WLAN

Plan de cinco pasos para la seguridad del enterprise WLAN se centra sólo en "diseñar una infraestructura para garantizar la seguridad e integridad de una WLAN en cinco pasos esenciales, que consistió en la salvaguardia de los clientes inalámbricos, control de conexiones Wi-Fi, auditoría de la actividad inalámbrica y la aplicación y cumplimiento de las políticas inalámbricas" no ayudando en mucho al desarrollo de las buenas prácticas y limitándose sólo a la parte de seguridad WLAN.

En base que las buenas prácticas desarrolladas tienen un campo más amplio, y para complementar las mismas, se recurrió de marcos adicionales.

CASO N° 03: Wi-Fi Wireless LAN de Auditoría de Seguridad.

Wi-Fi Wireless LAN de auditoría de seguridad se centra sólo en "garantizar la seguridad WLAN, que consistió en la revisión de cuentas de seguridad Wi-Fi conteniendo una variedad de pruebas, encontrando debilidades en sus puntos de acceso haciendo uso de las últimas herramientas de gestión de WLAN para averiguar si la WLAN está transmitiendo fuera de las paredes de la organización de manera incontrolada e insegura, conocidas como redes de los puntos de acceso deshonestos (Networks Rogue)" no ayudando en mucho al desarrollo de las buenas prácticas y limitándose sólo a la parte de Seguridad WLAN.

En base que las buenas prácticas desarrolladas tienen un campo más amplio, y para complementar las mismas, se recurrió de marcos adicionales.

CASO N° 04: Audit Briefing

Audit Briefing se centra sólo en "auditoría de información, dicha información reunida tenía por objetivo proporcionar el conocimiento de problemas de seguridad de los clientes, que se deben tener en cuenta en la planificación para su uso" no ayudando en mucho al desarrollo de las buenas prácticas.

En base que las buenas prácticas desarrolladas tienen un campo más amplio, y para complementar las mismas, se recurrió de marcos adicionales.

CASO N° 05: OSSTMM Wireless 2.9

OSSTMM Wireless 2.9 se centra sólo en "método aceptado para la realización de pruebas de seguridad completa, siendo un conjunto de reglas y normas. Este manual es un estándar profesional que consiste en pruebas de seguridad aplicadas a cualquier medio de afuera hacia adentro, incluyendo reglas de contrato, la ética para el probador profesional, las legalidades de la seguridad de pruebas, y un conjunto de test de seguridad;

las pruebas de seguridad externas van de un ambiente no privilegiado a uno privilegiado, para evitar/vulnerar los componentes de seguridad, procesos, y alarmas para ganar acceso privilegiado" ayudando y aportando un gran porcentaje al desarrollo de las buenas prácticas, abarcando la parte de Seguridad WLAN.
En base que las buenas prácticas desarrolladas tienen un campo más amplio, y para complementar las mismas, se recurrió de marcos adicionales.

5.2 Análisis comparativo (indicadores)

En la Tabla N° 30 y N° 31 se puede observar un resumen, caso por caso de los dominios de las buenas prácticas.

CASO	Sin Buenas Prácticas			**Total**
	Diseño	**Administración**	**Seguridad**	
1	X	✓	X	1
2	X	✓	X	1
3	X	X	✓	1
4	X	X	X	0
5	X	X	✓	1
Total	**0**	**2**	**2**	4

Tabla N° 30. Resumen comparativo de los casos

CASO	Con Buenas Prácticas			**Total**
	Diseño	**Administración**	**Seguridad**	
Buenas Prácticas	✓	✓	✓	3
Total	1	1	1	3

Tabla N° 31. Resumen comparativo de Buenas Prácticas

CASO	**Tipo de Auditoria**	**Aplicación de Auditoria**	**Tiempo**	**Reducción de Tiempo**
Personal del Hotel	Auditoria a la red inalámbrica.	Auditoría a la red inalámbrica del Gran Hotel Chiclayo	3 semanas	0
Buenas Prácticas	Auditoria a la red inalámbrica.	Buenas prácticas para auditar la red inalámbrica del Gran Hotel Chiclayo	2 semanas	**1 SEMANA**

Tabla N° 32. Resumen comparativo de reducción de tiempo entre Auditoria del personal del hotel y Buenas Prácticas.

Respecto al indicador tiempo de desarrollo de auditoría, actualmente una auditoría WLAN variar de 3 a mas semanas, aplicando las buenas prácticas esto se

puede reducir a 2 semanas, como fue el caso de aplicación del Gran Hotel Chiclayo.

Respecto al indicador número de metodologías, manuales y/o buenas prácticas aplicadas para auditar redes inalámbricas, el 10% de empresas hoteleras de Chiclayo que presentan WLAN utilizan alguna buena práctica, y ya con el desarrollo de las buenas prácticas las empresas están interesadas en utilizarlas, teniendo como objetivo aumentar a un 70% - 80% de empresas hoteleras en utilizar buenas prácticas.

Respecto al indicador número de herramientas aplicadas para auditar la red inalámbrica, en la actualidad sólo el 20% de hoteles que son el Gran Hotel Chiclayo y Costa del Sol son los únicos que utilizan herramientas para el monitoreo de la WLAN, y ante el desarrollo de las buenas prácticas los hoteles crecerá la necesidad de la utilización de las mismas para administrarlas, Diseño y Seguridad WLAN.

Respecto al indicador nivel de experiencia del auditor, en base al estudio realizado a los 5 hoteles de la región, actualmente el nivel de experiencia es alto, porque realizan auditorías habituales, y el propósito de la tesis es que las empresas realicen auditorías frecuentes respaldandose en las buenas prácticas desarrolladas.

Por lo tanto en base a esto se logró facilitar el trabajo a los auditores, apoyar la labor de la auditoría y reducir el tiempo de la misma.

VI. PROPUESTA

Para llegar al producto final de la investigación, la cual engloba mi propuesta para El Gran Hotel Chiclayo (Caso de estudio para aplicación real) se siguió una serie de etapas.

Inicialmente se encuestó a cinco empresas hoteleras, en las cuáles se pudo hacer la aplicación de una encuesta y entrevista, para saber la situación de la red inalámbrica, periodo de auditorías y si se basaron en buenas prácticas, y así como también de información de nuestro interés para la elaboración de la guía de buenas prácticas para auditar redes inalámbricas.

Se realizó la revisión de las metodologías, normas y buenas prácticas nacionales e internaciones para auditar WLAN's que son utilizadas en la actualidad.

De acuerdo a los conceptos ya mencionados de las metodologías, estándares y normas nacionales e internacionales, las buenas prácticas propuestas, se proponen dominios como dominios de diseño, administración y seguridad de la red inalámbrica, que evalúan de forma completa cada uno de ellos. Para cada dominio se determinaron buenas prácticas, proponiendo para cada una su objetivo o propósito de la buena práctica, actividades o tareas a desarrollar, apoyadas de herramientas de software y físicas, cuestionarios y checklist, teniendo como resultado la propuesta siguiente:

En la parte del dominio diseño se propone 5 buenas prácticas, cada una con su respectivo checklist, incluidos herramientas de apoyo, con un total de 11 herramientas.

	Dominio Diseño	Checklist	Herramientas
1	Buena Práctica Dis001: Análisis de la empresa	✓	• Formato De Análisis De La Empresa
2	Buena Práctica Dis002: Análisis tecnológico de la empresa.	✓	• MSIA 5.1 Analizador de Inventario de Software • Total Network Inventory 2.0.1 • Inventario de dispositivos inalámbricos • Inventario de estaciones.
3	Buena Práctica DIS003: Diseño físico de la red	✓	• AirWave VisualRF Report • Network Event Viewer • AirWave Wireless Site Plan
4	Buena Práctica DIS004: Diseño lógico de la red	✓	• Secure Shell • Administración Remota EMCO • Comandos "Ping" y "Traceroute"
5	Buena Práctica DIS005: Planes de implementación	✓	

Tabla N° 33. Dominio Diseño y Buenas Prácticas.

En la parte del dominio administración se propone 4 buenas prácticas, cada una con su respectivo Checklist, incluidos herramientas de apoyo, con un total de 9 herramientas.

	Dominio Administración	Checklist	Herramientas
1	Buena Práctica ADM001: Administración de recursos informáticos	✓	• Network Event Viewer • MSIA 5.1 Analizador de Inventario de Software • Total Network Inventory 2.0.1 • Inventario de dispositivos inalámbricos • Inventario de estaciones de trabajo.
2	Buena Práctica ADM002: Administración de recursos humanos	✓	
3	Buena Práctica ADM003: Administración de comunicaciones y operaciones inalámbricas	✓	
4	Buena Práctica ADM004: Administración de control de accesos	✓	• Recomendaciones en relación a la gestión y establecimiento de contraseñas • MaxPassword • Password Generator • Password Strength Analyser and Generator

Tabla N° 34. Dominio Administración y Buenas Prácticas.

En la parte del dominio seguridad se propone 4 buenas prácticas, cada una con su respectivo checklist, incluidos herramientas de apoyo, con un total de 4 herramientas.

	Dominio Seguridad	Checklist	Herramientas
1	Buena Práctica SEG001: Política de seguridad de las TIC's	✓	• Recomendaciones Para La Concientización En Seguridad De Información
2	Buena Práctica SEG002: Organización de la seguridad inalámbrica	✓	
3	Buena Práctica SEG003: Implementación de la seguridad Inalámbrica	✓	• BackTrack • InSSIDER • Xirrus Wifi Inspector
4	Buena Práctica SEG004: Gestión de incidentes de seguridad inalámbrica	✓	

Tabla N° 35. Dominio Seguridad y Buenas Prácticas.

Por lo tanto mi tesis desarrolló tres dominios: Dominio diseño, dominio administración y dominio seguridad, en total 13 buenas prácticas, habiendo revisado un número de 11 marcos entre Metodologías, guías, frameworks, etc. proponiendo además 20 herramientas para apoyar la ejecución de los procesos de auditoría de una red inalámbrica en las empresas del rubro hotelero.

Para el caso real de aplicación se realizaron visitas a el Gran Hotel Chiclayo, entrevistando al gerente de sistemas, y aplicando los checklist, herramientas de apoyo, como InSSIDer, Xirrus Wi-Fi Monitor y Backtrack para monitorear los canales, SSID, tipo de red, tipo de seguridad, inspeccionando la infraestructura de red, hardware y software en general. Asimismo, se realizó la aplicación de cada módulo por día aplicando el checklist y herramientas de apoyo, y al finalizar la aplicación de los tres módulos se paso al procesamiento de información y elaboración de informe preliminar, la cual presentó cuatro hallazgos, y en cada uno se detallan las normas trasgredidas, efecto, causa, y recomendaciones o acciones a tomar, para más detalle revisar Anexo 03 – Informe de Auditoría.

Como resultado del caso real de aplicación de las buenas prácticas se determinaron 04 hallazgos, las cuales se centran en el SSID irradiado presentaba información del hotel, bajo número de conexiones soportadas por los puntos de acceso, saturación de canales de emisión, bajo ancho de banda e incompatibilidad de equipos de telecomunicación.

La auditoría resultó *favorable con salvedades*, porque parte de las situaciones encontradas transgredieron las normas aquí utilizadas. Además el gerente de sistemas mantiene actualizada el inventario de los equipos de comunicación, mantiene la cobertura de la red en un 70% del hotel, mantiene un ambiente adecuado para los equipos de comunicación, presenta planes de contingencia, se realizan copias de seguridad de los equipos de comunicación, mantiene políticas de seguridad para los equipos de comunicación, monitorea frecuentemente la red inalámbrica para detectar así intrusos y canales que estén interfiriendo con los de los puntos de acceso en funcionamiento. Por parte del personal están definidos los roles y responsabilidades para cada uno de ellos, recibiendo capacitación constante en seguridad inalámbrica, y verificando que apliquen esta. Respecto a la seguridad los controles de acceso están monitoreados, asignando roles y responsabilidades para cada actividad, proporcionando recursos necesarias para la seguridad inalámbrica, y ante un problema de seguridad, es reportado tan pronto sea posible mediante mecanismos fáciles, accesibles y fácil de usar.

Finalmente, con la guía propuesta de buenas prácticas para auditar la red inalámbrica, los auditores podrán realizar auditorías sin problema alguno, basándose en los dominios propuestos, desarrollando cada buena práctica, realizando las actividades de cada una de estas, aplicando las herramientas de apoyo, y desarrollando el checklist, para asi finalmente poder detectar problemas, deficiencias y debilidades de la WLAN.

VII. CONCLUSIONES

Las conclusiones presentadas en este apartado se basan en las teorías formuladas en la discusión de esta investigación, las cuales al concretarse enmarcarían la solución de los problemas descritos en los resultados de esta investigación, logrando por tanto mejorar la auditoría WLAN. Por tanto se concluye que la guía propuesta de buenas prácticas para auditar redes inalámbricas permitirá:

- Al realizar un estudio de las empresas del rubro hotelero de la ciudad de Chiclayo, se pudo aplicar las buenas prácticas al hotel en estudio, logrando hacer un análisis de las redes inalámbricas actuales, encontrando una sobre posición de canales en un 36% y en el mismo canal un 15% de los canales en el espectro de emisión e insuficiente ancho de banda, en la cual dieron sugerencias y controles que permitieron reducirla a un 10% cada una de ellas permitiendo mejorar la disponibilidad, confiabilidad e integridad de la información, facilitando que las personas vuelvan a seguir con sus actividades.
- Cotejando las metodologías, manuales y buenas prácticas nacionales e internacionales, tales como; ISO 27001, ISO 27002, NAGU, Metodología para Administrar Redes, Seguridad en Redes Inalámbricas, Consultoría estratégica inalámbrica y OSSTMM 2.9 WIRELESS, se pudo identificar 8 buenas prácticas en promedio, logrando desarrollar 5 nuevas prácticas para así obtener finalmente 13 buenas prácticas agrupadas en tres dominios: Diseño, administración y seguridad, haciendo posible aplicar y lograr mayor eficiencia y eficacia en el proceso de auditoría a las redes inalámbricas en el rubro hotelero.
- Las herramientas estuvieron hay, pero al momento de complementarlas dieron resultados que sirvieron del uno para el otro, y poder seguir avanzando en las mejoras que se dieron como monitoreo de canales, tipo de encriptación y nombre del SSID, detallando así en cada buena práctica herramientas como InSSIDER, Xirrus Wi-Fi Monitor, formatos y checklist ayudando al auditor en la ejecución de la auditoría a la red inalámbrica.
- Con el desarrollo de las buenas prácticas se pudo mejorar el proceso de auditoría a la red inalámbrica, facilitando y apoyando la labor del auditor con experiencia y sin las herramientas necesarias para el desarrollo de auditorías a redes inalámbricas, además de reducir el tiempo de ejecución de una auditoría que bajo de 3 a 2 semanas, logrando una importante disminución de tiempo y por ende en consecuencia de dinero y personal.
- Con el desarrollo de las buenas prácticas para auditar redes inalámbricas se aplicó a una entidad hotelera de la ciudad de Chiclayo, siendo el resultado favorable con salvedades, recomendando mejoras en su red inalámbrica.

Finalmente el cumplimiento de las conclusiones enunciadas como beneficios que superan los problemas descritos en esta investigación permitió establecer la siguiente conclusión general: logra facilitar la labor del auditor con experiencia en el desarrollo de auditorías a redes inalámbricas en el rubro hotelero y

optimizar ampliamente el tiempo en el desarrollo de una auditoría WLAN en el rubro hotelero.

VIII. REFERENCIAS BIBLIOGRÁFICAS

(Arteaga 2009)	Arteaga, M. 2009. Metodologías de control interno, seguridad y auditoría informática. Articulo. Colombia
(Red M 2002)	Red M 2002. Wi-Fi RF Audit. . http://www.red-m.com/wp-content/uploads/2009/10/Wi-Fi_RF_Audit1.pdf (último acceso: 29 de Marzo de 2009).
(CORE 2006)	Core Competence Inc. 2006. Plan de cinco pasos para la seguridad del Enterprise WLAN. http://fiercemarkets.tradepub.com/free/w_ai05/pf/w_ai05.pdf (último acceso: 2 de Julio de 2009).
(Cypress 2008)	Cypress Solution. 2008. Wi-Fi Wireless LAN de Auditoría de Seguridad. http://www.cypress-india.com/case-study/Wi-Fi%20Wireless%20LAN%20Security%20Audit.pdf (último acceso: 28 de Octubre de 2009).
(AuditNet 2005)	AuditNet. 2005. Audit Briefing. www.auditnet.org/docs/WLANAuditBriefing.doc (último acceso: 04 de Abril de 2009).
(ISECOM y Herzog 2003)	ISECOM, y Peter Herzog. 2003. OSSTMM Wireless 2.9. http://isecom.securenetltd.com/osstmm.en.2.9.wireless.pdf (último acceso: 02 de Marzo de 2009).
(Oliver y Escudero 1999)	Miquel Oliver y IEEE. 1999. Redes de área local inalámbricas según el estándar IEEE 802.11. Cataluña: BURAN.
(34 TELECOM 2005)	34TELECOM. 2005. Normalización IEEE para WLAN. http://www.34t.com/box-docs.asp?doc=639 (último acceso: 23 de Febrero de 2009).
(Cisco 2009)	Cisco. 2009. CCNA 1 and CCNA2 - Wireless LANs V1.2. CHICLAYO: USS Inc.
(Briones y Geannina 2005)	Briones, A., y J. Geannina. 2005. Seguridad en redes inalámbricas. TESIS. Guayaquil - Ecuador: Escuela Superior Politécnica Del Litoral.
(Panda 2005)	PANDA, SOFTWARE. 2005. Seguridad en redes inalámbricas. Unites States of America: Panda Software International S.L.,
(IT	IT Governance Institute. 2007. Cobit 4.1. Estados Unidos de

Governance Institute 2007)	América: Suite.
(Defliese y AICPA 1997)	Philip L. Defliese y AICPA.1997. Auditoría Montgomery. México: Limusa.
(CGRP 2005)	Contraloría General de la Republica del Perú. 2005. Normas Generales de Auditoría Gubernamentales. Perú.
(Echenique 2001)	Echenique, J. A. 2001. Auditoría en Informática. MADRID: KARMA.
(CGRP 1998)	Contraloría General de la República. 1998. Manual De Auditoría Gubernamental MAGU. Perú.
(ISO/IEC 2005)	ISO/IEC 27001. 2005. Tecnología de la Información – Técnicas de Seguridad – Sistema de Gestión de Seguridad – Requerimientos.
(CGRP 1999)	Contraloría General de la Republica del Perú. 1999. RESOLUCION DE CONTRALORIA N° 141-99-CG. El Peruano, Noviembre 29.

IX. ANEXOS

ANEXO N° 01

Planeamiento de la auditoría - Planificación general

Planificación General.

A) Objetivos:
Verificar y auditar la red inalámbrica del Gran Hotel Chiclayo, en cuanto a su diseño, administración y seguridad.

B) Alcance:
Se auditará sólo la red inalámbrica del Gran Hotel Chiclayo.

C) Metodología a utilizar:
Se realizarán entrevistas al gerente de sistemas del Gran Hotel, así mismo se aplicará cuestionarios y checklist para el levantamiento de información relevante para la auditoría de la red inalámbrica.
Además se realizará la verificación e inspección de la ubicación y estado de los equipos de telecomunicación en las instalaciones del hotel.
Por último se utilizarán las buenas prácticas para auditar redes inalámbricas.

ANEXO N° 02

Planeamiento De La Auditoría

Planeamiento de la Auditoría.

A) Objetivos del examen.

Ante el desarrollo de la auditoría obtendremos un enfoque de la situación actual de la red inalámbrica del hotel, en lo que respecta a la parte del diseño, administración y seguridad de la red inalámbrica, y así plantear las recomendaciones del caso.

B) Alcance del examen.

Se realizarán entrevistas al gerente de sistemas del Gran Hotel, dando un alcance de la situación actual de la red y los equipos de red de forma narrativa que se encontraban al alcance. Luego se pasará a realizar un Checklist que abarcarán los dominios de Diseño, Administración y Seguridad de la red inalámbrica del hotel.

En cuanto al Diseño se auditará:

- Análisis de la empresa.
- Análisis tecnológico de la empresa.
- Diseño físico de la red.
- Diseño lógico de la red.
- Planes de implementación.

En cuanto a la Administración se auditará:

- Administración de recursos informáticos.
- Administración de recursos humanos.
- Administración de comunicaciones y operaciones inalámbricas.
- Administración de control de accesos.

En cuanto a la Seguridad se auditará:

- Política de seguridad de las Tics.
- Organización de la Seguridad Inalámbrica.
- Implementación de la Seguridad Inalámbrica.
- Gestión de incidentes de seguridad inalámbrica.

C) Descripciones de las actividades de la entidad.

El Gran Hotel Chiclayo, es un hotel cómodo y sofisticado se encuentra en una amplia avenida, a sólo minutos del centro de Chiclayo y del aeropuerto. Su ubicación céntrica es ideal para los viajeros de negocios así como para aquellas personas que vienen a experimentar los excepcionales

museos y sitios arqueológicos de la costa desértica del norte, todo queda muy cerca.

El gran hotel cuenta con 129 habitaciones, cada habitación cuentan con Acceso a internet Wi-Fi de alta velocidad gratis, Aire acondicionado, Televisión por cable, Teléfono, Secadora de pelo, Caja de seguridad, TV con cable con pantalla LCD, Caja de seguridad y Minibar. Es ideal tanto para los viajeros de negocios como de placer. Las habitaciones serán completamente rediseñadas para el año 2012, y hay Wi-Fi de alta velocidad en todo el hotel, como 7 salas de reuniones / eventos y un centro de negocios totalmente equipado para clientes corporativos. La piscina al aire libre, spa y el sauna lo convierten en un lugar ideal que lo invita a relajarse en una ciudad transitada.

Presenta como misión ser una empresa dedicada a brindar servicios y productos de primera calidad que satisfagan las necesidades a sus diferentes tipos de clientes, contando con personal altamente calificado, infraestructura adecuada para proporcionarles una estadía excelente.

Presenta como visión ser una empresa reconocida en el mundo del Turismo, proyectándose hacia la consolidación en el mercado hotelero regional, a través de la construcción de una infraestructura de calidad, convenios con instituciones nacionales e internacionales que le permitan proporcionar mejores servicios a clientes cada vez más exigentes contando para esto con tecnología de punta y con sistemas de información integrados y estratégicos.

D) Informes a emitir y fecha de entrega.

Se emitirá un informe final a la entidad, incluyendo los hallazgos más representativos y las recomendaciones respectivas.

E) Personal nombre.

Franck Jhonathan Santa María Becerra.

F) Funcionarios de la entidad a examinar.

Gerente de Sistemas del Gran Hotel Chiclayo.

G) Presupuesto de tiempo.

N°	ACTIVIDAD	DIAS HOMBRE
1	Planificación General	2

2	Planeamiento de la auditoría	2
3	Ejecución de Auditoría (Auditoria de diseño, administración y seguridad de la red inalámbrica)	6
4	Comunicación de Hallazgos	2
5	Elaboración del Informe de Auditoría	3
	TOTAL	**15**

Tabla N° 32. Presupuesto de Tiempo.

H) Papeles de trabajo

N	PAPEL DE TRABAJO	CODIGO P/T	FORMULÓ	REVISOR	UBICACIÓN
1	Encuesta a Hoteles: Garza Hotel, Hotel Las Musas, Hotel América, Gran Hotel y Costa del Sol.	1.1.1	FJSB	JLBJ	Anexo N°01
2	Checklist aplicadas al gerente de sistemas.	1.1.2.	FJSB	JLBJ	Anexo N°02
3	Análisis de la situación actual en base a las encuestas y entrevistas.	1.1.3.	FJSB	JLBJ	Anexo N°03
4	Aplicación de Checklist del Dominio Diseño, Administración y Seguridad al gerente de sistemas.	1.1.4.	FJSB	JLBJ	Anexo N°04
5	Falta de seguridad en la señal inalámbrica del hotel.	1.1.5.	FJSB	JLBJ	Anexo N°05
6	Canales de emisión de la red inalámbrica	1.1.6.	FJSB	JLBJ	Anexo N°06
7	Bajo ancho de banda de la red inalámbrica	1.1.7.	FJSB	JLBJ	Anexo N°07

Tabla N° 33. Papeles de Trabajo.

ANEXO N° 03

Informe de Auditoría.

I. INTRODUCCIÓN

1. Origen del examen

La presente auditoría denominada "Buenas prácticas para auditar redes inalámbricas" en el Gran Hotel Chiclayo, se realiza en cumplimiento al plan de auditoría en el marco de aplicación de Tesis de Pregrado (Anexo N° 01).

Como resultado de la auditoría se evidenciaron indicios razonables de deficiencias en la red inalámbrica, por lo que en cautela de los intereses de el Gran Hotel Chiclayo y en cumplimiento a la NAGU 4.40 Emisión del Informe, se está emitiendo el presente Informe, el mismo que constituye prueba pre constituida para el inicio de las acciones correctivas.

2. Naturaleza y objetivos del examen

La auditoría realizada esta orientada a la red inalámbrica del hotel, presentando como objetivo enfocarse a parte de diseño, administración y seguridad de la Wlan, teniendo en cuenta que la correcta funcionalidad de estas tres conllevan al buen funcionamiento de la red inalámbrica, y en consecuencia tener a sus clientes contentos con el servicio del hotel.

3. Alcance del examen

La auditoría, se desarrolló de conformidad a las normas de auditoría gubernamental, OSSTMM Wireless 2.9., ISO/IEC 27002:2005 y COBIT 4.1, dentro del ámbito del Gran Hotel Chiclayo, revisando en forma selectiva la documentación que obra en el área de sistemas, abarcando el periodo comprendido quincena Noviembre – finales de Noviembre 2011.

La evaluación abarca la revisión efectuada a la documentación de la red inalámbrica en sus dominios de diseño, administración y seguridad.

4. Antecedentes, base legal de la entidad

4.1. Antecedentes

El gran Hotel Chiclayo promueve el servicio a pasajeros nacionales y extranjeros, dándoles un servicio personalizado en hospedaje, fomentando el bienestar de los mismos desde que llegan hasta que se van.

4.2. Ubicación Geográfica

El Hotel abre sus puertas al público por primera vez el 7 de mayo de 1995, contando con una clientela menor. Conforme paso el tiempo se fue haciendo de un nombre conocido en la ciudad contando cada vez con clientes más selectos.

Localizándose en la Av. Federico Villarreal 115 – Chiclayo - Lambayeque – Perú.

4.3. Subsistemas de información actuales

MÓDULO HOTELERO

Este subsistema denominado por la empresa como Módulo Hotelero se encarga de manejar toda la parte hotelera como lo que son: Reservaciones, cuartelaría, restaurante, bar, lavandería.
Fue diseñado en Fox Pro 2.6 para D.O.S. y aún no se encuentra integrado con el resto de módulos.

MÓDULO DE ALMACÉN
En este módulo se ven todas las partes referentes a los inventarios de los productos que luego serán remitidos al módulo hotelero para su control en los sub almacenes.
En este módulo se controla lo que ingresa al hotel; pero el control aún es deficiente.

MÓDULO DE CONTABILIDAD
En este módulo se concentra toda la parte contable de la empresa, aquí se manejan todos los libros (Libro mayor, libro diario, etc.) para luego ser procesada y saber qué es lo que se va a cancelar en la SUNAT.

MÓDULO DE PLANILLAS
En este módulo se maneja toda la información de los pagos de los trabajadores de la empresa, así como descuentos, incentivos y otros que van a dar el sueldo total de los trabajadores.

5. Comunicación de hallazgos
Las observaciones determinadas fueron comunicadas por escrito en calidad de hallazgos al gerente de sistemas de la organización.

II. OBSERVACIONES. Todos los hallazgos, criterio y condición.

HALLAZGO N°01
FALTA DE SEGURIDAD EN LA SEÑAL INALÁMBRICA DEL HOTEL.

CONDICIÓN
Al realizar la auditoría se pudo apreciar que la señal inalámbrica del hotel mostraba información del hotel y no presenta ningún tipo de seguridad como son contraseñas o autenticación.

CRITERIO
Según el manual de buenas prácticas OSSTMM Wireless 2.9. En el apartado "2. Pruebas Inalámbricas 802.11"dice:

46. Verificar que el router inalámbrico, punto de acceso o Gateways no usa el 'Nombre de Red' o el SSID por defecto como Wired Equivalent Privacy (WEP) clave de cifrado. Ya que desde el SSID un atacante remoto podría determinar la llave WEP y descifrar el tráfico.
51. Verificar que todas las características de seguridad de los productos WLAN se han habilitado, incluyendo la autenticación criptográfica y características secretas WEP.

52. Verificar que la encriptación de las llaves son de tamaño al menos 128 bits o tan grande como posible.
54. Asegurar que un Firewall configurado correctamente haya sido instalado entre la infraestructura Cableada y la red inalámbrica.
58. Verificar que los usuarios son autenticados con Nombre de Usuario y Contraseña a WLANS y qué tipo de la autenticación es usado (RADIO, Kerberos.).
61. Para mejorar la seguridad en casos donde esta es apoyada, verificar que un protocolo de autenticación, como 802.1x, es usado en la parte superior de WEP.

CAUSA
Se opto por esto por motivos de que los pasajeros tenían problemas ante la conexión a la red inalámbrica, no ubicaban el SSID y/o ingresaban mal la clave, confundían los dígitos y números, es por eso que se opto por emitir la señal libre sin seguridad alguna.

EFECTO
Esto hace posible que cualquier usuario dentro o fuera de los límites del hotel se pueda conectar sin problema, aprovechando del ancho de banda y perjudicando a los pasajeros del hotel poniéndola lenta y en consecuencia quejas de los pasajeros.

HALLAZGO NRO 02
"CONTRASEÑAS DE LOS EQUIPOS DE COMUNICACIÓN NO SON CAMBIADAS PERIÓDICAMENTE Y NO SON ALMACENADAS EN LUGAR SEGURO"

CONDICIÓN
Al llevar a cabo la entrevista y el desarrollo del checklist, se pudo detectar las contraseñas no han sido cambiadas por un periodo largo, y las mismas que son almacenadas en un texto en la misma computadora del gerente de sistemas en la organización.

CRITERIO
Según el manual de buenas prácticas OSSTMM Wireless 2.3. En el apartado "2. Pruebas Inalámbricas 802.11"dice:

> 27. Verificar que los Puntos de Acceso (Access Point) sean restaurados a los últimos ajustes de seguridad después de la característica de RESET haya sido usada.
> 28. Verificar que el manejo de interfaces para los puntos de acceso tengan la autenticación de usuario.
> 29. Verificar que todos los puntos de acceso tienen contraseñas administrativas difíciles.
> 30. Verificar que todas las contraseñas administrativas son cambiadas con regularidad y seguramente almacenadas.
> 32. Si el router inalámbrico o el punto de acceso permiten configuración remota, verifique que este inhabilitado.
> 33. Si es posible, verifique que toda la configuración conducida por web del router o punto de acceso sea inhabilitado (inutilizado).

Respecto a la gestión y administración de claves el estándar ISO/IEC 27002:2005 – 11.3.1 Uso de Contraseñas que dice: "Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.". Sobre el uso de claves secretas dice:

> a) Mantener confidenciales las claves secretas;
> b) Evitar mantener un registro (por ejemplo, papel, archivo en software o dispositivo manual) de las claves secretas, a no ser que este se pueda mantener almacenado de manera segura y el método de almacenaje haya sido aprobado;
> c) Cambio de claves secretas cuando haya el menor indicio de un posible peligro en el sistema o la clave secreta;
> d) Seleccionar claves secretas de calidad con el largo mínimo suficiente que sean:
>
> > 1) Fáciles de recordar;
> > 2) No se basen en nada que otro pueda adivinar fácilmente u obtener utilizando la información relacionada con la persona; por ejemplo, nombres, números telefónicos y fechas de nacimiento, etc.

3) No sean vulnerables a los ataques de diccionarios (es decir, que no consista de palabras incluidas en los diccionarios);
4) Libre de caracteres consecutivos idénticos, todos numéricos o todos alfabéticos;

e) Cambio de las claves secretas a intervalos regulares o en base al número de accesos (las claves secretas para las cuentas privilegiadas se debieran cambiar con mayor frecuencia que las claves secretas normales), y evitar el re-uso de reciclaje de claves secretas antiguas;
f) Cambiar la clave secreta temporal en el primer registro de ingreso;
g) No incluir las claves secretas en ningún proceso de registro automatizado; por ejemplo, almacenado en un macro o función clave;
h) No compartir las claves secretas individuales;
i) No usar la misma clave personal para propósitos comerciales y no-comerciales

Si los usuarios necesitan tener acceso a múltiples servicios, sistemas o plataformas, y requieren mantener múltiples claves secretas separadas, se les debiera advertir que pueden utilizar una sola clave secreta de calidad (ver d) en el párrafo anterior) para todos los servicios donde se le asegura al usuario que se ha establecido un nivel de protección razonable para el almacenaje de la clave secreta dentro de cada servicio, sistema o plataforma.

CAUSA
Por motivos de uniformidad de claves y fácil acceso a los equipos de comunicación se opto por una sola clave para todos, pero la misma es almacenada en un archivo .txt en la misma computadora del gerente de sistemas.

EFECTO
Las claves corren el riesgo de ser captadas desde la misma computadora del usuario por personas inescrupulosas, y si esto se diera corren el riesgo todos los equipos de comunicación al tener acceso a los mismo y ser manipulados y reconfigurados.

HALLAZGO NRO 03
PUNTOS DE ACCESO NO ADECUADOS PARA LA RED INALÁMBRICA.

CONDICIÓN
Al desarrollar la auditoría se inicio con una entrevista al gerente de sistemas del Gran Hotel, la cual fue grabada en un audio, desarrollando el checklist indicándonos que actualmente los equipos no presentan uniformidad en marcas, provocando una incompatibilidad de configuraciones entre las mismas, limitaciones en la cantidad de conexiones, cobertura, canales de emisión, seguridad e implementar tecnología emergente con la actual.
Respecto a la cobertura, alcanza zonas de alto tránsito de pasajeros como el lobby, terraza, del 1ro - 6to piso, excepto en el 7mo piso, que la señal es muy débil o nula en ocasiones. La ubicación de los equipos se determinó a criterio propio con asesoría del proveedor de los equipos de comunicación, se colocaron 2 puntos de acceso por cada lado de la parte externa, siendo un total de 4 puntos de acceso en las afueras del hotel con línea de vista a las habitaciones, y en el interior se colocaron 8 puntos de acceso, presentando un total de 12 APs.
Número insuficientes de conexiones, soportando promedio de 60 conexiones simultáneas, provocando un Reset a los AP cada vez que llegan a su máximo. A nivel general en conexiones simultáneas diarias es de 50-80 conexiones en todo el hotel, y de 100-110 conexiones en todo el día, que generalmente se da de Martes – Viernes que son periodos de alta ocupabilidad y Sábado – Lunes de baja ocupabilidad.

CRITERIO
Respecto a la compatibilidad de equipos de comunicación hoy en día existen organizaciones que se dedican a la creación de protocolos y estándares para equipos de comunicación, que nos dice que la red inalámbrica debe estar disponible, basándose en equipos compatibles y puedan trabajar bien sin ningún problema al momento de realizar su trabajo, al no darse esto se estaría transgrediendo la norma:

- ISO/IEC 27002:2005 – 6.1.4. Proceso de Autorización de Recursos para el Tratamiento de la Información que dice: "Donde sea necesario, el hardware y el software debiera de ser chequeado para asegurar que son compatibles con otros componentes del sistema"
- Previamente al adquirir un equipo de comunicación se haga un estudio y análisis de las características y configuraciones, comparando con los equipos de otras marcas a adquirir o con los equipos que presenta la organización, y constatar que tienen características compatibles y configurables de las cuales se le pueda sacar el máximo provecho a los mismos.
- Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por la acción de materiales ambientales. La ubicación de los puntos de acceso debe ser libre de interferencias, ya que estos rayos no pueden atravesar los objetos sólidos.

Según el manual de buenas prácticas OSSTMM Wireless 2.3. En el apartado "2. Pruebas Inalámbricas 802.11" para los canales de emisión nos dice:

16. Verificar que todos puntos de acceso en la red inalámbrica están en menos de 5 canales el uno aparte del otro y desde puntos de acceso en redes inalámbricas vecinas para evitar posible problemas de negación de servicio causado por interferencia.

CAUSA

Motivo por el cual se dio la incompatibilidad de los equipos una fue los motivos económicos, otra fue por la falta de información exacta de sus características, de un previo estudio de los equipos actuales con los que se iban adquirir y si eran compatibles las características de importancia que se quería configurar en la red inalámbrica ya sea seguridad o cobertura. En lo que respecta a la cobertura el criterio principal es lo difícil de infraestructura del hotel, al presentar columnas de gran magnitud y falta de áreas abiertas.

EFEECTO

Los principales efectos que experimenta la red inalámbrica en estos momentos es:

- Incompatibilidad de equipos de comunicación.
- Cobertura mínima o nula en áreas con menor concentración de usuarios.
- Número de conexiones insuficientes soportadas por los Puntos de acceso.
- Riesgo de falta y/o pérdida de conexión de los pasajeros cuando requieran o estén utilizando la red inalámbrica, provocando descontento e incomodidad al interrumpir su conexión en momentos que estén trabajando con la misma.
- Inaplicabilidad de tecnología común a todos los equipos, como de Vlan's, QoS.

HALLAZGO NRO 04
LIMITADO ANCHO DE BANDA

CONDICIÓN
Al desarrollar el Checklist el gerente de sistemas nos transmitió esa incomodidad por parte de los pasajeros, y nos reforzó con una entrevista lo mismo, que al utilizar la red inalámbrica para Video y/o VPN, experimentan una baja en el ancho de banda, tomando en cuenta que presentan un contrato por 1Mbps.

El hotel actualmente cuenta con 129 habitaciones, llegando a un promedio de ocupabilidad de 70 habitaciones, en tiempo de alta ocupabilidad que son de martes – viernes, y sábado-lunes de baja ocupabilidad. Haciendo uso de la red inalámbrica un promedio de 50-60 pasajeros al mismo tiempo. En lo que respecta al café bar un aproximado de 15 pasajeros se conectan simultáneamente, y 40 conexiones al día, dando un promedio aproximado de 80-90 conexiones simultáneas y 100 conexiones en el día en todo el hotel. Generalmente las aplicaciones que utilizan los pasajeros son de acceso al correo, navegación en internet, videos, audio y VPN.

CRITERIO
La red inalámbrica debe trabajar con ancho de banda que cubra cualquier necesidad del pasajero, sea e-mail, Video o VPN, debido a que es un hotel 4 ESTRELLAS, se hospedan autoridades del estado, comitivas de futbol, profesionales, altos ejecutivos, etc, que tienen como necesidad primordial el VPN, Video, correo, etc, y debiendo el hotel cubrir esa necesidad sin mayor problema.

CAUSA
Por motivos económicos no se ha optado por un ancho de banda mayor, debido a que se cubre las principales necesidades de pasajeros como es de e-mail, carga y descarga de archivos.

EFECTO
Demora en la conexión VPN, carga de audio y video.

III. CONCLUSIONES (observaciones) las recomendaciones

Como resultado de la auditoría ejecutada en El Gran Hotel Chiclayo por el periodo 2011 se ah llegado a las conclusiones siguientes:

1. Se ah emitido el Informe de Auditoría el cual se presenta como favorable con salvedades de la red inalámbrica del Gran Hotel Chiclayo al 20 de Diciembre del 2011. Pues parte de las situaciones encontradas transgredieron las normas aquí utilizadas, además manteniendo el gerente de sistemas un inventario de los equipos de comunicación, manteniendo cobertura de la señal en mayor parte del hotel, adecuado ambiente para los equipos de comunicación, constante monitoreo de la señal inalámbrica,

2. De la revisión e inspección de la red inalámbrica se determino las siguientes conclusiones:

- Los equipos de comunicación no son los óptimos para el uso que el hotel necesita.
- Por parte del personal queda por documentar los roles y responsabilidades y recibir capacitación frecuente en seguridad inalámbrica.

IV. RECOMEDACIONES (Conclusiones) opinión general

En merito a las observaciones y conclusiones expuestas en el presente Informe se recomienda lo siguiente:

AL GERENTE DE SISTEMAS DEL GRAN HOTEL CHICLAYO:

- Durante el desarrollo de la auditoría al Gran Hotel Chiclayo, se pudo encontrar que se requería de la implementacion de un servidor controlado, para la autenticacion y accesso a la red de los usuarios.

- Para la puesta en marcha de la solución planteada ante la auditoría se recomienda que existan servidores de autenticación Radius con el estándar de autenticación 802.1x, que a modo de sugerencia para abaratar costos pueden ser FreeRADIUS pudiéndose observar que no requiere de un hardware de gama alta, o licenciados, y sean clientes del servidor.

- Recomendable que los puntos de acceso trabajen de modo cliente-servidor, que tengan un controlador Wireless, y que los mismos sean clientes del controlador.

- Para mejorar el ancho de banda se recomienda la implementación de un proxy-firewall transparente, de modo que se pueda facilitar y agilizar la implementación de la misma, sin necesidad de configurarlo en cada terminal usuario. A modo de sugerencia si se desea abaratar costos podría ser un Squid.

- Desarrollar auditorías periódicas, de manera prioritaria en el dominio diseño, donde se encontró la mayor cantidad de hallazgos, sin dejar de lado los dominios de administración y seguridad.

- Finalmente tomar en cuenta y/o hacer el levantamiento de las sugerencias en la presente auditoría asignando un persona responsable de vigilar y revisar las observaciones halladas.

V. ANEXOS

Anexo N°01

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: LISTA DE ENCUESTAS A HOTELES GARZA HOTEL, HOTEL LAS MUSAS, HOTEL AMERICA, GRAN HOTEL Y COSTA DEL SOL
Fecha o periodo cubierto: Abril 2010 – Mayo 2010

Detalles del trabajo realizado: Se realizó en el periodo detallado la encuesta a los hoteles de la ciudad de Chiclayo para poder determinar si presentaban una red inalámbrica en su organización, y de esa forma poder determinar con que hoteles trabajar.

Resultados del trabajo: Al concluir con la encuesta se pudo determinar que 5 hoteles contaban con una red inalámbrica en la organización.

Conclusiones: Se pudo determinar 5 hoteles de la ciudad contaban con una red inalámbrica en la organización, y que tenían un personal a su cargo.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Abril 2010
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Abril 2010

Índice o código del P/T: 1.1.1.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°02

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: CHECKLIST APLICADAS AL GERENTE DE SISTEMAS.
Fecha o periodo cubierto: Noviembre 2011 – Diciembre 2011

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, se hizo una entrevista al Gerente de sistemas en la cual se fue aplicando los checklist de los dominios diseño, administración y seguridad, en la cual cada checklist presentaba un apartado de observaciones si en caso quería hacer alguna aclaración o algún agregado en dicha parte, así en lo mismo en los siguientes dominios de administración y seguridad.

Resultados del trabajo: Al concluir con los Checklist de los dominios diseño, administración y seguridad, se pudo obtener un alcance mejor de la situación de la organización.

Conclusiones: La situación de la red inalámbrica presenta algunas deficiencias en las cuales se debe mejorar, las cuales serán detalladas en los apartados de resultados de la Tesis.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.2.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°03

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: ANÁLISIS DE LA SITUACIÓN ACTUAL EN BASE A LAS ENCUESTAS Y ENTREVISTAS.
Fecha o periodo cubierto: Noviembre 2011 – Diciembre 2011

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, se hizo una entrevista al Gerente de sistemas, la misma que fue grabada con su consentimiento en su oficina, en la que se le hizo pregunta abiertas para que pueda ir describiendo la situación actual del hotel.

Resultados del trabajo: Al concluir con la encuesta se pudo determinar que 5 hoteles contaban con una red inalámbrica en la organización.

Conclusiones: La situación de la red inalámbrica presenta algunas deficiencias en las cuales se debe mejorar, las cuales serán detalladas en los apartados de resultados de la Tesis.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.3.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°04

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: APLICACIÓN DE CHECKLIST DEL DOMINIO DISEÑO, ADMINISTRACIÓN Y SEGURIDAD AL GERENTE DE SISTEMAS.
Fecha o periodo cubierto: Abril 2010 – Mayo 2010

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, se hizo una entrevista al Gerente de sistemas, la misma que fue grabada con su consentimiento y en la cual se fue aplicando los Checklist de los dominios diseño, administración y seguridad, en la cual cada checklist presentaba un apartado de observaciones si en caso quería hacer alguna aclaración o algún agregado en dicha parte, así en lo mismo en los siguientes dominios de administración y seguridad.

Resultados del trabajo: Al concluir con el Checklist se pudo determinar que presenta algunas deficiencias que tomar en cuenta para mejorar la red inalámbrica en la organización.

Conclusiones: Se pudo determinar 5 hoteles de la ciudad contaban con una red inalámbrica en la organización, y que tenían un personal a su cargo.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.4.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°05

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: FALTA DE SEGURIDAD EN LA SEÑAL INALÁMBRICA DEL HOTEL.
Fecha o periodo cubierto: Noviembre 2011 – Diciembre 2011

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, se hizo una entrevista al Gerente de sistemas, en la cual con su coordinación también se hizo un escaneado a la señal inalámbrica, en la cual se pudo constatar que la misma no presentaba seguridad alguna, demostrándolo con los siguientes gráficos.

Resultados del trabajo: Al concluir el escaneado de la señal inalámbrica se pudo obtener las siguientes imágenes:

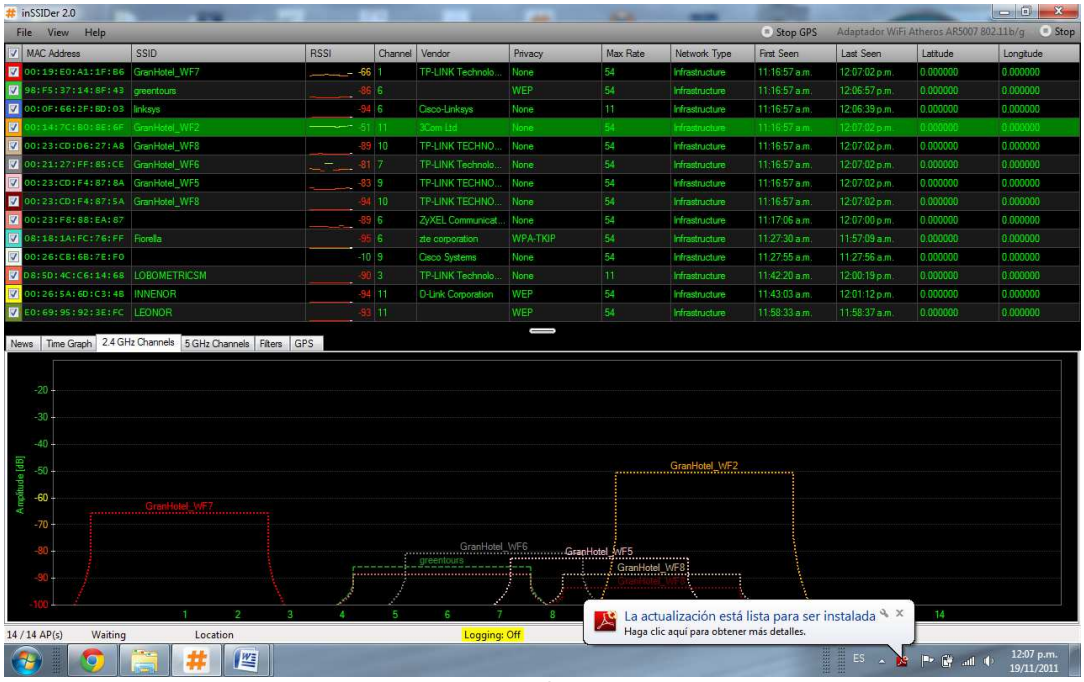

Figura N° 08: Monitoreo de la red Inalámbrica del Gran Hotel Chiclayo con la herramienta InSSIDER 2.0.
Fuente: Elaboración Propia.

El siguiente gráfico podemos apreciar que la red no presenta cifrado.

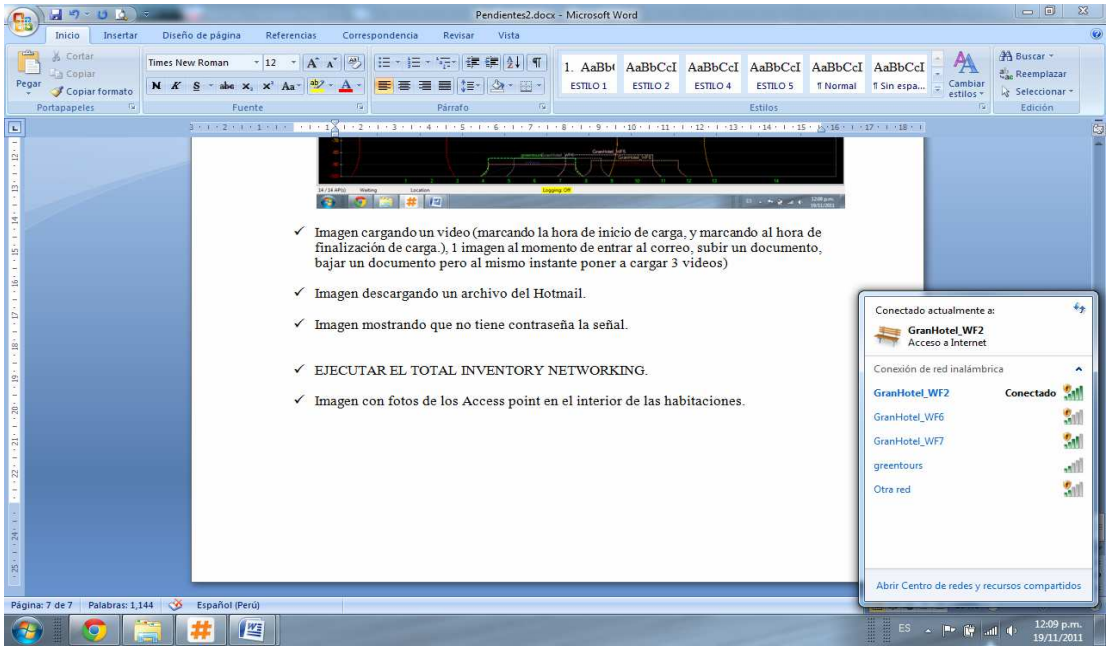

Figura N° 09: Monitoreo de las redes Inalámbricas del Gran Hotel Chiclayo con la herramienta de Windows y Conexión a "GranHotel_WF2"
Fuente: Elaboración Propia.

Ante tal caso de no presentar cifrado, se puedo apreciar que se puede hacer conexión a la red:

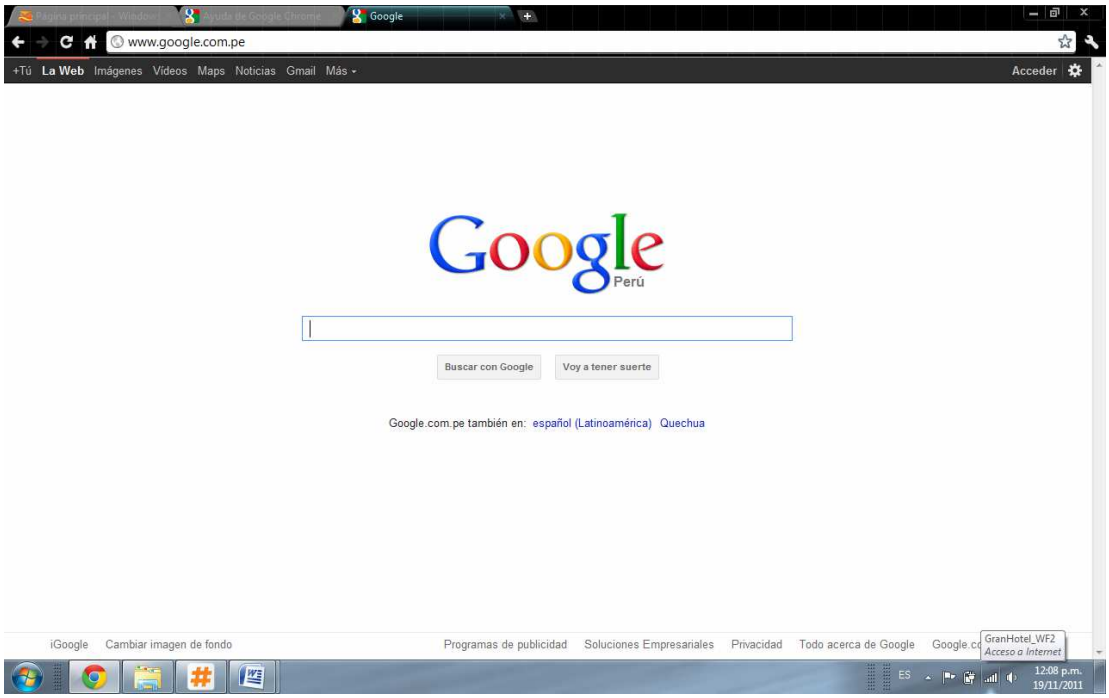

Figura N° 10: Navegación en la Red Inalámbrica "GranHotel_WF2".
Fuente: Elaboración Propia.

Conclusiones: Se pudo determinar que en la organización, la red inalámbrica no presenta ningún tipo de seguridad.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.5.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°06

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: CANALES DE EMISIÓN DE LA RED INALÁMBRICA.
Fecha o periodo cubierto: Noviembre 2011 – Diciembre 2011

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, se hizo un monitoreo a los canales de emisión de la señal inalámbrica, en la cual se pudo constatar que presenta superposición de canales, demostrándolo con los siguientes gráficos.

Resultados del trabajo: Al concluir el escaneado de la señal inalámbrica se pudo obtener las siguientes imágenes:

Al realizar la inspección del lugar, se constató que la señal inalámbrica trabaja con 5 canales, "1, 7, 9, 10 y 11", los mismos que son utilizados por redes vecinas, de la misma manera el gerente de sistemas realiza un monitoreo de la red para revisar los canales que se estén interfiriendo y los canales disponibles para migrar a esos libres.

Después del monitoreo de la red inalámbrica de la organización, se prueba que trabaja con los canales "1, 7, 9, 10 y 11", y que las redes vecinas también trabajan en canales similares y la superposición de los mismos con canales vecinos.

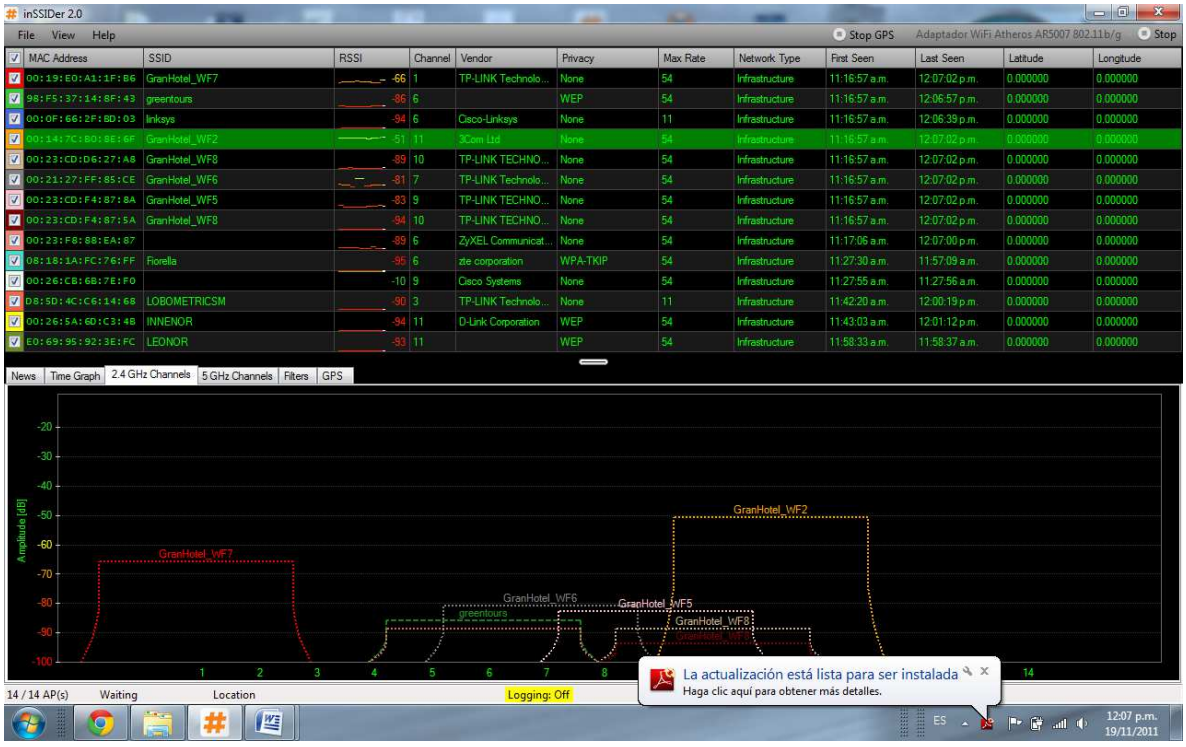

Figura N° 11: Monitoreo de los canales superpuestos y libres en el espectro del Hotel con herramienta InSSIDER.
Fuente: Elaboración Propia.

Conclusiones: Se pudo determinar que en la organización, la red inalámbrica no presenta ningún tipo de seguridad.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.6.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

Anexo N°07

Nombre de la entidad: GRAN HOTEL CHICLAYO
Título del P/T: BAJO ANCHO DE BANDA DE LA RED INALÁMBRICA.
Fecha o periodo cubierto: Noviembre 2011 – Diciembre 2011

Detalles del trabajo realizado: Se realizó en el Gran Hotel Chiclayo, después de hacer conexión con la red inalámbrica, se probó el ancho de banda, y efectivamente, al momento de hacer uso del servicio de Video, la red experimenta una baja en el ancho de banda, pero para servicio de correo al momento de descarga y subida de archivos no hay problemas.

Resultados del trabajo: Al concluir con la navegación de la señal inalámbrica se pudo obtener las siguientes imágenes:

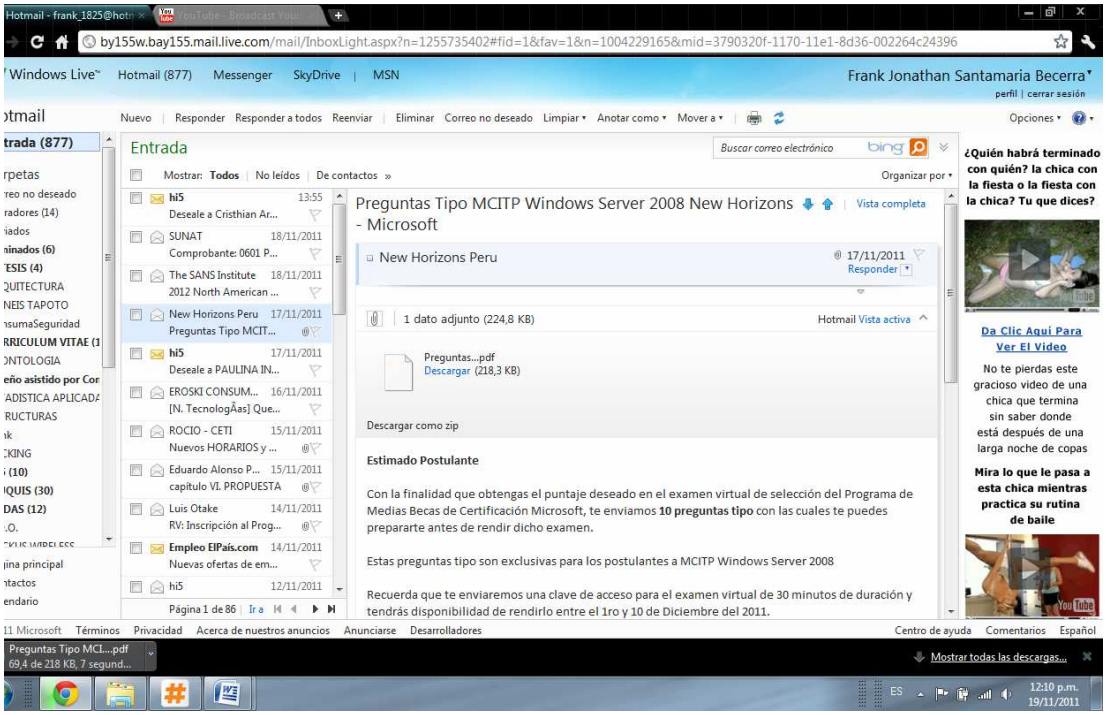

Figura N° 12: Probando el ancho de banda de la red con la descarga de un archivo.
Fuente: Elaboración Propia.

Conclusiones: Se pudo determinar que en la organización el ancho de banda de la red inalámbrica es bajo.

Hecho por:	Franck Jhonathan Santa María Becerra
Fecha:	Noviembre 2011
Revisado por:	MSc Ing. Jessie Leila Bravo Jaico
Fecha:	Diciembre 2011

Índice o código del P/T: 1.1.7.
Iniciales del que formuló: FJSB
Iniciales del revisor: JLBJ

ANEXO N° 04

OBJETIVOS DE CONTROL PROPUESTOS

N°	Objetivos de control propuestos.	Según los modelos, normas y/o metodologías
	DISEÑO	
1	1. ANÁLISIS DE MODELO DE NEGOCIO DE LA EMPRESA	Information Networks Planning and Design (INPD)
	A. Descripción de la Empresa.	INPD
	B. Revisión de objetivos de las empresas	INPD
	C. Paso de la información vital.	INPD
	D. Arquitectura del Sistema	INPD
2	2. ANÁLISIS TECNOLÓGICO DE LA EMPRESA.	INPD
	A. Localización de los equipos existentes en los hoteles.	INPD
	B. Listado de las aplicaciones	INPD
	C. Red actual.	INPD
	1.1. Planeación y Diseño de la red.	Met. Para Administrar Redes.
	2.2. Monitoreo del Rendimiento.	Met. Para Administrar Redes.
	2. Análisis previo	Instituto Superior Aeronáutico
3	3. DISEÑO FÍSICO DE LA RED.	INPD
	A. Objetivos y Metas	INPD
	B. Alcance de la Red	INPD
	C. Identificar el Modelo de Red y la función de los nodos de la red	INPD
	D. Diseño de la Red de Área Local	INPD
	E. Componentes de hardware de red y equipos de conexión	INPD
	F. Identificación de la seguridad física requerida por la red	INPD
	G. Esquema del diseño físico de la red WLAN	INPD
	2. Análisis previo	Instituto Superior Aeronáutico
4	4. DISEÑO LÓGICO DE LA RED.	INPD
	A. Sistema Operativo de Red	INPD
	B. Protocolos de Red	INPD
	C. Determinación del esquema de Red	INPD
	D. Configuración de los equipos de red	INPD
	E. Determinación de la organización de usuario y equipos	INPD
	F. Recursos Compartidos y niveles de acceso a los recursos compartidos	INPD
	G. Implementación de la Seguridad Lógica de la red	INPD
	H. Políticas de seguridad de la Red.	INPD
	3. Configurar el protocolo TCP/IP	Instituto Superior Aeronáutico
5	5. PLANES DE IMPLEMENTACIÓN.	INPD
	1.3. Instalaciones y Administración del Software y Hardware.	Met. Para Administrar Redes.
	A. Plan de Implementación.	INPD
	B. Plan de administración.	INPD
	C. Plan de Contingencia.	INPD
	D. Plan Financiero.	INPD
	E. Análisis De Beneficios	INPD

	2. Análisis previo (P. 6 y P.7)	Instituto Superior Aeronáutico
	5. Propiedades configurables en el punto de acceso	Instituto Superior Aeronáutico
	6. Conexión con la red local cableada e internet	Instituto Superior Aeronáutico
	Evaluar la configuración, autenticación y cifrado de redes inalámbricas	Osstmm Wireless – 2.Pruebas de Capa Física de WLAN 802.11
	Evaluar clientes inalámbricos	Osstmm Wireless – 2.Pruebas de Capa Física de WLAN 802.11
	ADMINISTRACIÓN	
1	**ADMINISTRACIÓN DE RECURSOS INFORMATICOS**	
	3.1. Responsabilidad por los recursos.	ISO 27002 – 7.1
	3.2. Clasificación de la información	ISO 27002 – 7.2 equivalente
	Definir la arquitectura de la información	a COBIT 4.1 – PO2
	Evaluar el acceso administrativo a los dispositivos inalámbricos	Osstmm Wireless – 2.Pruebas de Capa Física de WLAN 802.11
2	**ADMINISTRACIÓN DE RECURSOS HUMANOS**	
	4.1. Previo al empleo	ISO 27002 – 8.1 equivalente
	Administrar recursos humanos de TI	a COBIT 4.1 – PO7
	4.2 DURANTE EL EMPLEO	ISO 27002 – 8.2 equivalente
	Administrar recursos humanos de TI	a COBIT 4.1 – DS7 y se adiciona el
	Educar y entrenar a los usuarios	Sub control COBIT 4.1 – PO7.
	4.3. FINALIZACIÓN O CAMBIOS DE EMPLEADO	ISO 27002 – 8.2 equivalente
	Administrar recursos humanos de TI	a COBIT 4.1 – PO7
	2. SECCION DE PERSONAS.	LVD Centro seguridad física.
3	**ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIÓNES**	
	10.1. Procedimientos y responsabilidades operacionales	ISO 27002 – 10.1 se toma tal cual la norma lo presenta.
	10.5. Respaldo	ISO 27002 – 10.5 se adiciona sub controles de
	Administración de la información	COBIT 4.1 – DS11 casi equivalente.
	10.7. Manejo de medios.	ISO 27002 – 10.7 se toma tal cual la norma lo presenta.
4	**ADMINISTRACIÓN DE CONTROL DE ACCESOS**	
	11.1. Requisitos del negocio para el control de accesos	ISO 27002 – 11.1 excluyendo seguridad lógica.
	11.2. Gestión de accesos de usuarios	ISO 27002 – 11.2
	11.3. Responsabilidad de los usuarios.	ISO 27002 – 11.3
	SEGURIDAD	
1	**POLITICA DE SEGURIDAD INFORMACIÓN**	
	1.1. Política de Seguridad de la información	ISO 27002 – 5
	Comunicar las aspiraciones y la dirección de la gerencia.	COBIT 4.1 – PO6
	Definir un plan estratégico de TI	COBIT 4.1 – PO1
	Definir los procesos, organización y relaciones de TI.	COBIT 4.1 – PO4
	Las diez mejores prácticas de Seguridad de Información.	ENISA
	Evaluar el equipamiento, firmware y actualizaciones	Osstmm Wireless – 2.Pruebas de Capa Física de WLAN 802.11
2	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
	2.1. Organización Interna	ISO 27002 – 6.1 equivalente
	Definir y administrar los niveles de servicio	a COBIT 4.1 – DS1
	2.2. Partes externas	ISO 27002 – 6.2 equivalente
	Administrar los servicios de terceros.	a COBIT 4.1 – DS2
	PASO 1: Proteger los clientes inalámbricos	RED - M

	PASO 2: Transito seguro de datos	RED - M
	PASO 3: Controlar el uso de la red corporativa	RED - M
	PASO 4: Auditoría de actividad inalámbrica	RED - M
	PASO 5: Aplicar directiva inalámbrica	RED - M
3	**SEGURIDAD FÍSICA Y AMBIENTAL**	
	5.1. Áreas Seguras	ISO 27002 – 9.2 equivalente
	Administrar el ambiente físico	a COBIT 4.1 – DS12
	5.2. Seguridad del equipo	ISO 27002 – 9.2 se toma tal cual la norma lo presenta.
	1. SECCION DE LA PROPIEDAD	LVD Centro seguridad física.
4	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN**	
	13.1. Informe sobre los eventos y debilidades de seguridad de la información	ISO 27002 – 13.1 se adiciona el control COBIT 4.1 – DS8
	13.2. Gestión de los incidentes y mejoras de seguridad de la información, Administrar los problemas.	ISO 27002 – 13.2 se adiciona el control COBIT 4.1 – DS8
	CUMPLIMIENTO DE SEGURIDAD	
	15.1. Cumplimiento de requisitos legales (NO VA)	ISO 27002 – 15.1 equivalente
	Garantizar el cumplimiento regulatorio	a COBIT 4.1 – ME3
	15.2. Cumplimiento con normas y políticas de seguridad y cumplimiento técnico	ISO 27002 – 15.2 se toma tal cual la norma lo presenta.
	15.3. Consideraciones de la auditoría de sistemas.	ISO 27002 – 15.3 se complementa con sub
	Monitorear y evaluar el control interno.	controles COBIT 4.1 – ME2
	6. ADMINISTRACIÓN DE LA SEGURIDAD	Metodología para administrar Redes - 5.

Tabla N° 34. Objetivos de Control Propuestos.

ANEXO N° 05

FORMATO DE ANÁLISIS DE LA EMPRESA

1. Descripción de la Empresa

1.1. Nombre de la Empresa: _____
1.2. Giro de la Empresa: _____
1.3. Ubicación Geográfica: _____
1.4. Estructura Orgánica (Áreas de la empresa): _____
_____
_____
1.5. Distribución Física Actual del Hotel (PLANO DEL HOTEL)
1.6. Descripción de las áreas de desarrollo del proyecto

2. Revisión de objetivos de la empresa

2.1. Misión: _____
2.2. Visión: _____
2.3. Análisis FODA:

FORTALEZAS	DEBILIDADES
OPORTUNIDADES	AMENAZAS

3. Paso de la Información Vital (Basándose en el punto 1.4)

4. Arquitectura del Sistema

4.1. Descomposición Funcional **(Basándose en el punto 1.4)**

4.2. Arquitectura del proceso de la información

4.3. Análisis de los problemas encontrados

ANEXO N° 06

INVENTARIO DE EQUIPOS DE TELECOMUNICACION

- INVENTARIO DE ESTACIONES

N°	STA MAC	Ultimo SSID	Ultimo Ch#	Nombre	Ubicación	Adaptador	Clasificación
1	: : : : :						
2							
3							
…							

N°	Estación MAC	Tipos de Protocolos	Asoc. ESSIDs	Encriptación 802.11	PSK	802.1X	Tipo EAP	Usuario
1	: : : : :							
2								
3								
…								

- INVENTARIO DE PUNTOS DE ACCESO

N°	**AP MAC**	**ESSID**	**Ch#**	**IP Address**	**SNR[4]**	**Nombre**	**Ubicación**	**Clasificación**
1	: : : : :							
2								
3								
…								

N°	**AP MAC**	**Tipos de Protocolos**	**SSID Beacon**	**Encriptación 802.11**	**PSK**	**802.1X**	**Tipo EAP**	**Otros**
1	: : : : :							
2								
3								
…								

ANALISIS DE LA RED

TOPOLOGÍA:		
ESTÁNDAR		
MODELO DE RED		

[3] Extensible Authentication Protocol (EAP) es una autenticación framework usada habitualmente en redes WLAN Point-to-Point Protocol.
[4] Signal-to-Noise Ratio: Relación señal-ruido

DISEÑO FISICO	EQUIPOS DE COMUNICACIÓN	
	Nombre del Equipo	Ubicación
DISEÑO LOGICO	Sistema Operativo:	
	Protocolos de Red:	
CONFIGURACION DE EQUIPOS DE RED	Puntos de acceso (Por cada uno):	Nombre:
		Dirección IP:
		Mascara de Red:

ANEXO N° 07

CUESTIONARIO PARA EL ANÁLISIS TECNOLOGICO DE LA ORGANIZACIÓN

Área de evaluación: Gerencia de Tecnologías de Comunicación
Nombres Y Apellidos:
Cargo: Gerente de Sistemas
Objetivo: Análisis tecnológico de la organización.

PREGUNTAS

1.- ¿Con cuántos nodos de red trabaja la red inalámbrica?
A) 1 – 5 Pc's B) 6 – 10 Pc's C) 11 – 20 Pc's D) 21 – más Pc's

2.- ¿Con cuántos canales trabaja la red inalámbrica?
A) 1 B) 2 C) 3 D) 4 E) 5

3.- ¿Con qué canales trabaja la red?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11
☐ 12 ☐ 13

4.- ¿Qué topología inalámbrica utiliza?
A) Red Inalámbrica Ad-Hoc o Grupo De Trabajo Independiente
B) Red de Infraestructura o Grupo De Trabajo Extendido
C) Otro

5.- ¿Con qué estándar trabaja la red cableada?

☐100baseT ☐1000BaseT ☐1000base SX ☐1000BaseLX ☐10GigabitEthernet

6.- ¿Cuál es el área de la red inalámbrica?
A) 200 – 399 m^2 B) 400 – 799 m^2 C) 800 – 1499 m^2 D) 1500 – Mas m^2

7.- ¿Qué estándar inalámbrico utiliza?

☐ 802.11a ☐ 802.11b ☐ 802.11g ☐802.11n

8.- ¿Qué tipo de frecuencia inalámbrica utiliza?
A) 2.4 Ghz B) 5 Ghz C) Ambos

9.- ¿Qué tipo de cifrado trabaja la red?
A) Privacidad equivalente a la cableada (WEP)
B) Acceso Protegido Wi-Fi (WPA)
C) Acceso Protegido Wi-Fi 2 (WPA2)
D) Estándar avanzado de encriptación (AES)
E) Control de Integridad de Mensajes (MIC)

F) Rotación Clave de Broadcast (BKR)
G) N.A.

10.- ¿Qué tipo de autenticación trabaja la red inalámbrica?
A) Ligero protocolo de autenticación extensible (LEAP)?
B) Protocolo de autenticación extensible protegido (PEAP)?
C) Servicio al Usuario de Acceso Telefónico Remoto (RADIUS)?
D) N.A.

ANEXO N° 08

RECOMENDACIONES EN RELACIÓN A LA GESTIÓN Y ESTABLECIMIENTO DE CONTRASEÑAS.

Para gestionar correctamente la seguridad de las contraseñas, se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave. Esto conlleva a la mejora del tiempo para descubrir la clave se vea aumentado.

2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.

3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.

4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

5. Las contraseñas hay que cambiarlas con una cierta regularidad. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, P. ej.: pasar de "01Juitnx" a "02Juitnx".

6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: "Tr-.3Fre". En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos. Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

7. Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Ej.: "Comí mucho chocolate el domingo 3, por la tarde", resultaría la contraseña: "cmCeD3-:xLt". En ella, además, se ha introducido alguna mayúscula, se ha cambiado el "por" en una "x" y, si el sistema lo permite, se ha colocado algún signo de puntuación (-).

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios.
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono.
3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
4. No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej.: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej.: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),
9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como "ataque por diccionario".
10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o "vuelta atrás".
12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

ANEXO N° 09

RECOMENDACIONES PARA LA CONCIENTIZACION EN SEGURIDAD DE INFORMACIÓN.

1. Utilice una contraseña

Utilice una contraseña segura

- Utilice una contraseña segura para proteger sus datos: Use al menos ocho caracteres y combinar letras (mayúsculas y minúsculas), números y símbolos. Cuanto mayor sea la diversidad de caracteres en su contraseña, más difícil es adivinar.
  No utilice información personal como su nombre, el Nombre de su hijo o un cumpleaños, la persona ya sabe o puede saber fácilmente. Además, trate de evitar las palabras de lenguaje común, ya que algunos hackers utilizan programas que tratan de cada palabra en el diccionario.

Cambie su contraseña

- Si tiene la impresión de que se ha accedido ilegalmente en su sistema, cambie inmediatamente su contraseña.
- Mantenga su contraseña en secreto
- Su contraseña es única y debe ser comunicada a nadie.
- Si es posible, trate de memorizar las contraseñas. Diseñar una estrategia sobre la manera de recordar las contraseñas.
- Si usted anote sus contraseñas, almacenar de forma segura. Archive la grabación de sus contraseñas donde usted también archivaría los datos que protegen las contraseñas.

Use contraseñas diferentes

- Utilizar para cada cuenta en línea a la que tienen acceso a una contraseña diferente (o al menos usar varias contraseñas diferentes). Si utiliza la misma contraseña para varias cuentas, un atacante que obtenga acceso a una de sus cuentas, el acceso a todas sus cuentas.

2. Proteja su computadora

- Mantener alejado de su escritorio accesos no autorizados, cuando usted pone su orden de ir a una reunión, un breve descanso o del almuerzo.
- No deje que otras personas utilicen su dispositivo de almacenamiento USB en una computadora infectada, especialmente si son de carácter privado, no seguro tarjetas de memoria.
- No instale ningún software ilegal o no autorizada, porque entonces comprometer la seguridad de datos y violar la ley. Programas desconocidos fuera de la red puede llevar a su organización a riesgos de seguridad.

- No incluye las unidades privadas, los reproductores de música y memorias USB a su estación de trabajo.
- No conecte su ordenador portátil a la red de su organización, ya que podrían estar infectados con virus o malware.

3. **Tenga cuidado al tratar con el correo electrónico e Internet**

- No abra mensajes de correo electrónico y archivos adjuntos de remitentes desconocidos.
- No abrir hipervínculos de correos electrónicos sospechosos.
- Avance e-mails si es necesario. Considere, sin embargo, antes de borrar el historial de mensajes.
- Use sólo los documentos en formato PDF en conjunto para asegurar que los archivos no puedan ser modificados.
- La información confidencial debería ser codificada, antes de ser enviada por correo electrónico.
- Tenga cuidado al navegar por Internet.
- No dar ninguna información en foros de Internet sobre su organización y su trabajo.
- No escribir un blog, donde sus puntos de vista y las opiniones se podría interpretar como los de su organización.
- No descargar documentos y materiales, cuyas fuentes no son confiables.
- Evite abrir el material con contenido ilegal u ofensivo, descargar, guardar o enviar.
- Recuerde que los sitios de Internet que tiene acceso desde la estación de trabajo, se puede rastrear.

4. **Tenga cuidado cuando se trata de dispositivos portátiles en su organización: Ordenadores portátiles, memorias USB, teléfonos móviles y Blackberrys**

Ordenadores portátiles

- No instale ningún software ilegal o no autorizada, porque entonces comprometer la seguridad de datos y violar la ley.
- Abandone conexiones inalámbricas, si no lo necesita.
- Conecte su portátil con regularidad a la red de su organización para actualizar los controles de seguridad.
- Haga una copia de seguridad de los datos almacenados en su computadora portátil.
- Proteger al salir de su equipo contra el acceso no autorizado cuando usted va ir a una reunión, un breve descanso o el almuerzo.
- No permita que otras personas usen su memoria USB infectada en su computadora portátil, especialmente si son de carácter privado, no seguro tarjetas de memoria
- No deje su computadora portátil desatendida.
- No deje su computadora portátil visible en su coche.

Memoria USB

- Utilice una memoria USB encriptada.
- Guardar datos de la empresa sólo hasta cierto punto en su memoria USB, especialmente si, es una organización privada.
- Conecte su memoria USB a su llavero, con el fin de no perderlos, debido a su pequeño tamaño, se pierden muy fácilmente o pueden ser robados con facilidad. Además, una mayor capacidad de almacenamiento aumenta, el riesgo de acceso no autorizado a datos expuestos. Las unidades flash USB se guardan generalmente en bolsos, mochilas, bolsas para portátiles, chaquetas o los bolsillos del pantalón o dejarlo sólo en el lugar de trabajo. Más recientemente se ha repetido los incidentes, desde memorias USB perdido una y otra vez, se mueve y prestado sin permiso o incluso robados.
- Establecer que las tarjetas de memoria USB de los usuarios, se ejecute en modo de sólo lectura para evitar la transmisión del virus: Algunas unidades flash USB presentan un interruptor o un bloqueo para apagar el dispositivo en modo lectura para activar el modo único que impide escribir en el disco o el cambio de los datos almacenados en el ordenador anfitrión.
- Inspeccione visualmente el dispositivo de memoria USB a un análisis anti-virus si ha copiado los archivos de un ordenador que no es de confianza o no autorizado.
- Antes de conectar su dispositivo de memoria USB a la PC de otra persona, borre todos los archivos que no hay necesidad de ese proceso.
- Establecer copias de seguridad para restaurar a la memoria USB los datos almacenados cuando sea necesario.

Teléfonos móviles y Blackberrys

- Abandone conexiones inalámbricas (es decir, Bluetooth y WLAN), si no los utilizan. Con la ayuda de la tecnología Bluetooth permite que los dispositivos electrónicos para comunicarse a través de corto alcance de redes inalámbricas entre sí. Algunos teléfonos móviles con Bluetooth se ven afectados por los errores de software que permiten Bluejacking y bluesnarfing. Bluejacking hace el envío anónimo de tarjetas de visita electrónicas que contienen un mensaje a los dispositivos con capacidad Bluetooth. Bluejacking es operado para enviar mensajes no solicitados. Bluesnarfing es operado a fin de que los datos personales (por ejemplo, Acceso a la información de contacto) en un teléfono móvil y copiarlos en otro teléfono móvil.
- No deje sus teléfonos móviles y Blackberrys desatendido. Recuerde que de lo contrario podría perder datos.

5. Tenga cuidado al tratar con datos

- Identificar cada documento con cada código de clasificación.
- Proteger los datos sensibles con una contraseña para que no puedan ser alterados o suprimidos por personas no autorizadas.

- Mantenga su escritorio en orden y no dejar información sensible por ahí. Disponer de los documentos con cuidado.
- No abandone datos sensibles en mediante el uso de salas de conferencia o de reunión, para que no sean accesibles para las personas que utilizan la sala después de ti.
- Impresión segura: Los datos de impresión, copiado y escaneo sólo si es realmente necesario. No deje que el documento quede sobre la impresora.
- Siempre destruir los documentos que contengan datos sensibles o marcados como confidencial.
- No coloque los datos en su disco duro local.
- Asegúrese de que cada tercera persona que trabaja con usted, ha firmado un acuerdo de confidencialidad antes de tomar los datos confidenciales que le sea accesible.

6. **Visitante**

- Todos los visitantes deben estar registrados y conectados al llegar y al salir del edificio una vez más la sesión.
- Todos los visitantes deben obtener un pase de visitante, se debe usar durante su visita a las instalaciones de la empresa en cualquier momento.
- Acompañar a los visitantes en cualquier momento durante su estancia, edificios corporativos. Permitir a los visitantes en las oficinas de vigilancia, puede llevar a riesgos.

7. **Incidentes de registro y la pérdida o daño de los dispositivos portátiles de su organización**

- Notificar al departamento de TI para la asistencia de cualquier pérdida o daño a los dispositivos portátiles para su organización (teléfonos móviles, PDAs y memorias USB).
- Notificar al departamento de TI de su organización si tiene un dispositivo portátil de su organización encontró.
- Reporte cualquier violación e incidentes relacionados con la seguridad de la información, incluso si usted no está seguro.
- Informe si en su escritorio aparece algo sospechoso o si una aplicación es de repente ya no está disponible, sin que su departamento de TI ha informado de antemano.

8. **Proteger sus datos fuera de su organización.**

- Asegurar su ordenador y sus datos sensibles guardados en todo momento cuando se esté fuera de su organización para evitar el robo o pérdida. Tenga especial cuidado cuando se trata de los datos públicos.
- Prestar atención que otras personas puedan escuchar lo que usted dice. Hacer que la información sensible de su organización no está al alcance de todos.

- Si usted está viajando o trabajando desde una estación de trabajo a distancia, asegúrese de que nadie puede mirar por encima del hombro. Protéjase contra el hombro-surf.

9. **Se adhieran a las normas y procedimientos de su organización en relación con la seguridad de la información**

   - Atenerse a las normas y procedimientos de su organización en relación con la seguridad de la información.
   - Garantizar la confidencialidad, integridad y disponibilidad de los datos.
   - Prestar atención a los requisitos legales, como las restricciones de derechos de autor, derechos de propiedad intelectual, derechos de privacidad y las licencias de software.
   - Notificar inmediatamente si observa que los colegas hayan violado las normas y procedimientos de su organización en relación con la seguridad de la información.

10. **Contribuir mediante la retroalimentación para mejorar las normas de seguridad establecidas y las soluciones.**

    - Contribuir a una mejora de las normas de seguridad establecidas y las soluciones.
    - Fomentar la compra de software adicional si lo necesita para su trabajo.
    - Formule preguntas o hacer sugerencias tendentes a mejorar los estándares de seguridad y soluciones.