UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS

Tema: METODOLOGÍA ISO 27000 PARA OPTIMIZAR RENDIMIENTO DE REDES CORPORATIVAS MEDIANAS MÓVILES MANTENIENDO ESTÁNDARES DE DISPONIBILIDAD Y SEGURIDAD

AUTOR: JULIO ENRIQUE AGUIRRE GALARZA

TUTOR: PhD. RENÉ ALBERTO CAÑETE BAJUELO

D. M. Quito septiembre del 2017

UNIVERSIDAD TECNOLÓGICA ISRAEL

PLAN DEL PROYECTO INTEGRADOR DE CARRERA

CARRERA:	INGENIERÍA EN SISTEMAS INFORMÁTICOS
AUTOR:	JULIO ENRIQUE AGUIRRE GALARZA
TEMA DEL TT:	**APLICAR LA METODOLOGÍA ISO 27000 PARA OPTIMIZAR RENDIMIENTO DE REDES CORPORATIVAS MEDIANAS MÓVILES MANTENIENDO ESTÁNDARES DE DISPONIBILIDAD Y SEGURIDAD**
ARTICULACIÓN CON LA LÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	TECNOLOGÍA APLICADA A LA PRODUCCIÓN Y SOCIEDAD
SUBLÍNEA DE INVESTIGACIÓN INSTITUCIONAL:	SEGURIDAD INFORMÁTICA Y REDES DE COMUNICACIÓN
FECHA DE PRESENTACIÓN DEL INFORME FINAL:	Miércoles 24 de mayo de 2017

Declaración y autorización

Yo, **Julio Enrique Aguirre Galarza**, CI: 1713293015 autor del trabajo de graduación: **Aplicación de la metodología ISO 27000 para optimización de rendimiento en redes corporativas medianas móviles manteniendo estándares de disponibilidad y seguridad**, previo a la obtención del título de **Ingeniería en Sistemas Informáticos** en la UNIVERSIDAD TECNOLÓGICA ISRAEL.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Articulo 144 de la Ley Orgánica de Educación Superior, de difundir el respectivo trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de graduación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Quito, mayo del 2017

Atentamente.

Julio Enrique Aguirre Galarza.
C.I. 1713313573

Dedicatoria

A mi Madre

A mis hijos

A mis hermanos

Agradecimiento

A mi madre por su sacrificio y ejemplo.

A mis hijos por su amor y comprensión.

A mi esposa por su compañía y apoyo.

A mis revisores de tesis por su constante, entusiasta y amable transmisión de conocimientos tan útiles para el desarrollo de la investigación.

A la Universidad Israel por su trabajo constante en la formación de los profesionales de mi patria.

Índice de contenidos

Índice de figuras

Índice de tablas

UNIVERSIDAD TECNOLÓGICA ISRAEL
TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:
INGENIERO EN SISTEMAS

TEMA: “METODOLOGÍA ISO 27000 PARA OPTIMIZAR RENDIMIENTO DE REDES CORPORATIVAS MEDIANAS MÓVILES MANTENIENDO ESTÁNDARES DE DISPONIBILIDAD Y SEGURIDAD”

Autor: Julio Enrique Aguirre Galarza
Tutor: PhD. René Alberto Cañete Bajuelo
Fecha: julio de 2016

Resumen

En Ecuador como consecuencia de las políticas públicas para universalizar el acceso a las Tecnologías de la Información y Comunicación (TIC), procurando generar bienestar social a la ciudadanía y priorizando la Investigación, Desarrollo e innovación (I+D+i) ya que las considera actividades cruciales para el desarrollo sostenible del país, desde el en el plan de desarrollo 2014 – 2017 se ha conseguido que nuestro país disponga de una de las mejores redes de telecomunicaciones de Sudamérica, lo que permite conectividad con parámetros muy aceptables en la mayor parte del territorio nacional. En este contexto las instituciones públicas y privadas así como también corporaciones y empresas nacionales e internacionales han expandido sus operaciones en varios sitios fuera de las capitales o ciudades principales, movilizando infraestructura tecnológica de manera temporal o permanente a sitios considerados remotos aunque de mucho interés, para estos fines requieren la implementación de redes de telecomunicaciones corporativas externas pero con parámetros de acceso garantizado, disponibilidad de conexión permanente y seguridades, para este efecto la incorporación de políticas de

seguridad de la información e infraestructura corporativa de alto desempeño basados en Sistemas de gestión de seguridad de la información, son indispensables para garantizar estas aplicaciones.

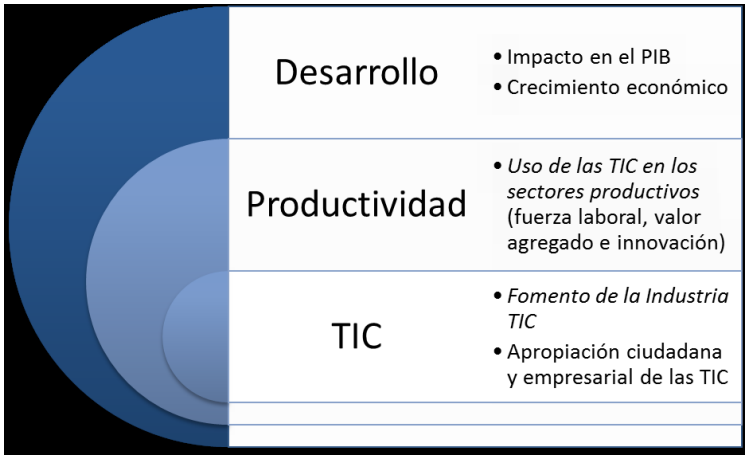


Ilustración 1 Modelo de Desarrollo Tecnologías de la Información y Comunicaciones (TIC) (Mintel, 2016)

En atención a lo expuesto se propone a consideración la implementación de dos alternativas tecnológicas desplegadas aplicando la metodología SGSI de la norma ISO 27001 que buscan optimizar la seguridad informática y la provisión del servicio de acceso a enlaces de datos e internet.

Descriptores: Implementación y análisis de procedimientos habituales fuera de la ISO 27001; Implementación y análisis de procedimientos estándar aplicando ISO 27001; análisis de ventajas y riesgos de implementaciones fuera de la aplicación de políticas ISO 27001, guía básica de implementación utilizando SGSI ISO 270001.

UNIVERSIDAD TECNOLÓGICA ISRAEL
TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:
INGENIERO EN SISTEMAS

Theme: “METHODOLOGY ISO 27000 TO OPTIMIZE PERFORMANCE OF MOBILE CORPORATE NETWORKS MAINTAINING AVAILABILITY AND SAFETY STANDARDS”

Author: Julio Enrique Aguirre Galarza
Directed by: PhD. René Alberto Cañete Bajuelo
Date: July 2016

Abstract

In Ecuador as a result of public policies to universalize access to Information and Communication Technologies (ICT), seek social welfare to citizens and prioritizing Research, Development and Innovation (R & D) activities for the Sustainable development of the country, since the development plan 2014 - 2017 has been achieved that our country has one of the best telecommunications networks in South America, which allows connectivity with parameters very acceptable in most of the national territory In this In this context, public and private institutions as well as corporations and national and international companies have expanded their operations in several places outside the capitals or major cities, mobilizing the technological infrastructure of temporary or permanent way to the remote but very interesting sites. These fines Require the implementation of telecommunications networks corporative External access, but with the access parameters guaranteed, the availability of permanent communications and security, for this purpose the incorporation of information security policies and high performance corporate

infrastructure based on Security Management Systems of the Information, are indispensable to guarantee these applications.

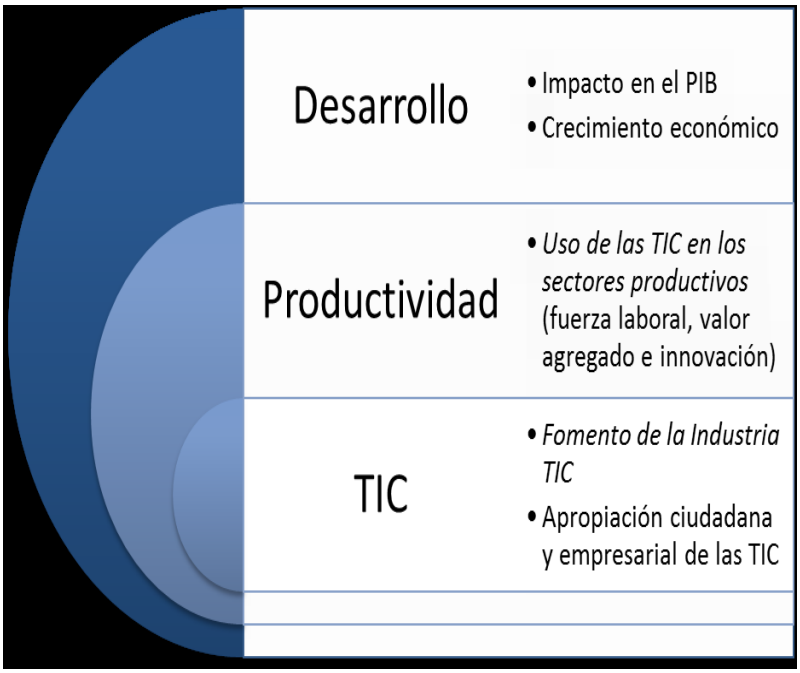


Ilustración 2 Modelo de Desarrollo Tecnologías de la Información y Comunicaciones (TIC) (Mintel, 2016)

In consideration of the above, it is proposed to consider the implementation of two technological alternatives deployed applying the ISMS methodology of the ISO 27001 standard that seek to optimize IT security and the provision of access service to data and internet links.

Descriptors: Implementation and analysis of procedures common outside ISO 27001; Implementation and analysis of standard procedures applying ISO 27001; Analysis of advantages and risks of implementations outside the application of ISO 27001 policies, basic implementation guide using ISMS ISO 270001.

Introducción:

La necesidad de gobiernos y empresas de mantener reuniones en sitios fuera de oficinas e infraestructura informática corporativa habitual hace imprescindible la implementación de redes externas “temporales” pero conservando sus parámetros de acceso garantizado, disponibilidad de conexión y seguridades mediante la incorporación de políticas de seguridad de la información, infraestructura y de conexión en una versión corporativa que permita disponer de todas las características de nuestra red habitual pero en entornos externos.

Esta investigación corresponde al diseño de un modelo óptimo para una red corporativa que se utiliza fuera de la infraestructura empresarial habitual, en diferentes ubicaciones geográficas, en circunstancias fuera del entorno corporativo donde no tenemos completo control de varios aspectos lo que origina un alto riesgo para el bien más preciado de la sociedad actual es decir la información.

A pesar de todos los inconvenientes que pudieran presentarse en la provisión del servicio de conexión y acceso a los recursos de red, el objetivo de la investigación será garantizar la seguridad, confianza, integridad y disponibilidad de la información.

Se detallara en el desarrollo del análisis el comportamiento actual del sistema implementado, previo a las correcciones realizadas con motivo del desarrollo de la investigación y los resultados conseguidos una vez implementado en la infraestructura el SGSI ISO 27001.

Como parte fundamental de la investigación se analizarán las leyes y reglamentos de telecomunicaciones y seguridad de la información que guarde relación directa con nuestro estudio esto permitirá tomar conciencia a las empresas y personas acerca de los derechos, obligaciones y sanciones garantizadas en Ecuador acerca de tecnologías de la información y la comunicación (TIC).

CAPÍTULO 1

Descripción del Problema

En el Ecuador la escasa disponibilidad de especialistas en el área de seguridades de redes informáticas corporativas y la poca inversión de las instituciones y empresas en herramientas informáticas que garanticen parámetros adecuados de alta disponibilidad y seguridad de la información, ocasiona infraestructuras tecnológicas vulnerables y expuestas a ataques informáticos.

El modelo actual y en funcionamiento no considera parámetros de red corporativa se enfoca únicamente en conseguir la conectividad de sus interfaces WAN y LAN, no considera altos estándares de disponibilidad y seguridad, a pesar de que esta infraestructura opera de forma periódica en sitios diferentes, y fuera de entornos corporativos no considera el transporte adecuado de los equipos y materiales como una prioridad es decir no mantiene ningún estándar de cuidado en el embalaje y transporte de los equipos, como precaución en cualquier movilización lo único que se realiza es agruparlos en un cartón para su la mayor cantidad de equipos para que se pueda transportar en un solo cartón.
El diseño de infraestructura de acceso, última milla, conexiones para redes de datos e internet dirigidas a entornos corporativos que se desarrollen fuera de su centro habitual de trabajo, políticas de seguridad de la información e implementación y monitoreo de ancho de banda mediante una aplicación móvil no son considerados pueden o no ser parte de las implementaciones actuales quedando su aplicación a criterio del operador de turno.

En la mayoría de las veces por desconocimiento y en otras ocasiones por falta de procesos que regulen esta operación se ha evidenciado que no se contempla ningún parámetro de cableado estructurado para la implementación del servicio una vez más se verifica que el objetivo es la conectividad básica sin ningún criterio técnico, este parámetro es crítico ya que representa riesgo de intrusiones en la red debido a que no se dispone de los controles del cableado estructurado.
Para la implementación de la solución entre otros conceptos el ingeniero de soporte técnico debería conocer de manera suficiente lo siguiente:

- Conceptos de estándar IEEE 802.1X definición Internacional de Redes que regula las redes locales inalámbricas, rangos de frecuencia disponibles para los dispositivos que desearan emitir de esta forma: 2.4 GHz y 5 GHz.
- Conceptos de Gestión de la Seguridad de Información estándares bajo el nombre de ISO/IEC 27001.
- Conceptos de redes LAN, estándar IEEE 802.3. Para los estándares de cableado de última milla aplicaciones redes WAN.

Se considera la configuración de la solución actualmente implementada y que nos servirá como base para el desarrollo de la investigación, conservando los mismos equipos, pero optimizando las líneas de código, mejorando el diseño de la red, de la seguridad informática y aplicando procedimientos ISO 27001.

Se debe considerar el aspecto legal que compete a la infraestructura instalada, ya que estos servicios están regulados en la legislación ecuatoriano y no son considerados con sus respectivas reglamentaciones.

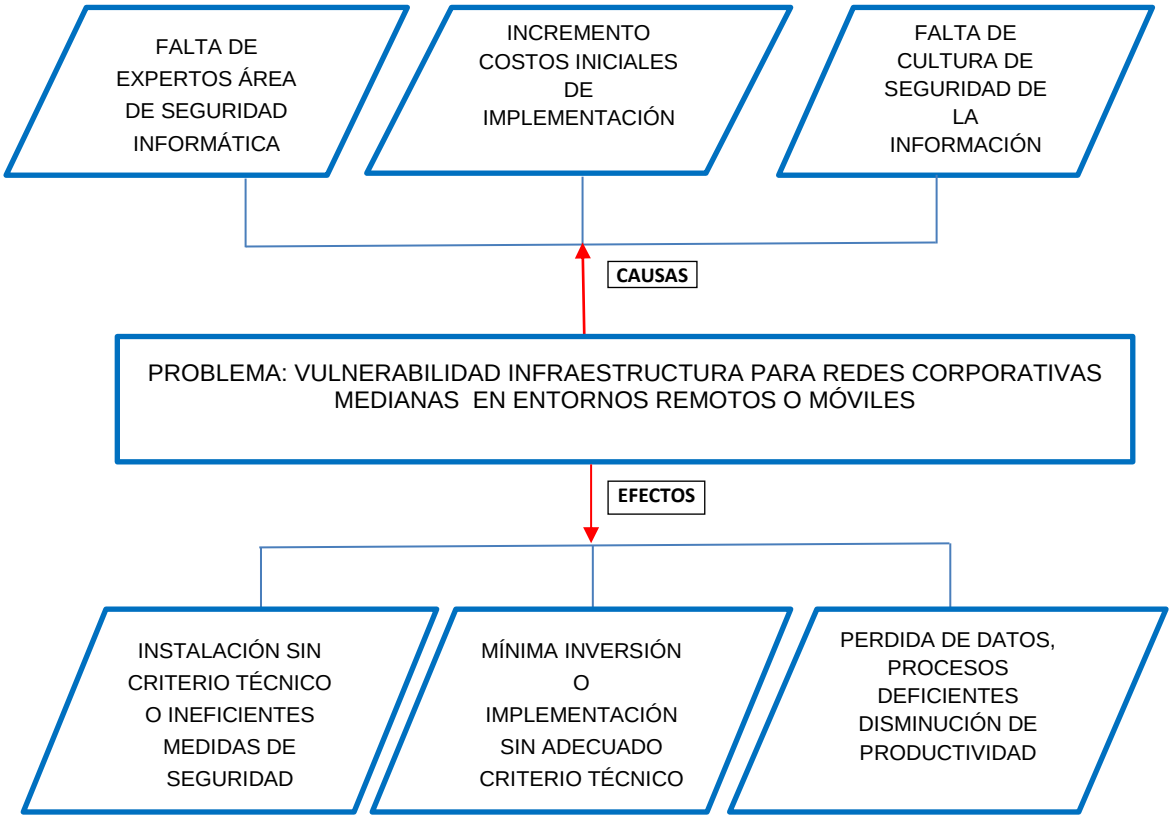


Tabla 1 Causas Efectos Problema Propuesto (Julio, 2016)

1.2.1. Objetivo General:

Configurar controles de seguridad y optimización de gestión de redes, a los procesos de implementación, gestión y monitoreo de una red corporativa móvil mediana utilizando para su despliegue, gestión y monitoreo el estándar ISO 27001.

1.2.2. Objetivos Específicos:

- Análisis de la infraestructura situación actual

- Diseño de red LAN, WLAN, WAN propuesta en base a las mejoras realizadas a la red actual y código de configuración de equipos.

- Análisis y diseño de políticas de seguridad basados en ISO27001

- Análisis de resultados y comparativa de la infraestructura anterior e infraestructura propuesta.

Ideas a sostener en el proceso investigativo

- La presente investigación busca la eficiencia y eficacia en el desempeño de redes corporativas medianas móviles, manteniendo altos estándares de disponibilidad y seguridad de la información.

- Minimizar recursos y maximizar resultados será una premisa del desarrollo de la investigación.

1.4. Alcance

El resultado final de la investigación plantea optimizar la implementación de infraestructura de red para enlaces de datos e internet dirigidas a redes corporativas medianas que se desarrollen fuera de su centro habitual de trabajo, mediante el dimensionamiento de hardware y software en base a porcentajes de utilización observados, aplicando las políticas y procesos de seguridad del estándar ISO 27001, se considera además los parámetros mínimos de infraestructura de acceso última milla.

A continuación se detalla los elementos de análisis y desarrollo.

- Hardware
- Software de gestión
- Software de monitoreo
- Cableado estructurado
- Red LAN
- Red WAN
- Administrador de red capacitado
- Usuarios autorizados y perfiles de acceso al sistema
- Proveedores de servicios
- Documentos de control
- Políticas y procesos de seguridad informática
- Personal autorizado para acceso a centros de almacenamiento de información o gestión de comunicaciones.
- Entrevista estructurada de gestión a administradores de red para definir situación actual y oportunidades de mejora
- Diseño de documento de lista de verificación de responsables de proceso y hardware asignado.
- Definir requerimientos del cliente y clasificación en requerimientos deseables y requerimientos que pueden ser atendidos.

- Dimensionamiento y asignación de equipos en base al requerimiento del cliente y en base a análisis costo beneficio de hardware
- Asignación de infraestructura lógica
- Análisis y diseño de políticas de gestión y monitoreo.
- Diseño de formato acta de entrega recepción el servicio de datos e internet.

CAPÍTULO 2

2. Marco Teórico

La investigación realizada analiza La implementación de una red corporativa de acceso a datos e internet desplegado en entornos externos temporales, la misma que instalada de manera básica limita su configuración e infraestructura a establecer el acceso WAN y LAN sin considerar ningún parámetro adicional, por lo que dicha infraestructura carece de principios de seguridad básicos. Se puede considerar entre los principales inconvenientes, instalaciones físicas inadecuadas para el desarrollo de las actividades, el espacio insuficiente para el correcto despliegue de nuestros materiales y equipos de trabajo, garantías mínimas de seguridad para los equipos y conexiones, suministro eléctrico de mala calidad, exposición de la red a usuarios malintencionados que puedan representar un riesgo de ataque a la red, mal uso de los recursos, vulneración de información de la empresa entro otros riesgos inherentes a la implementación analizada.

La falta de políticas de seguridad en esta infraestructura expongan el servicio al máximo riesgo de afectación permitiendo acceso de usuarios no autorizados afectando los estándares de ancho de banda y disponibilidad del servicio, adicionalmente se consideran conceptos de redes básicos que no corresponden a redes corporativas medianas.

Origen de ataques de informáticos redes corporativas medianas.

La protección de la red corporativa debe considerar la protección contra ataque externos a nuestra infraestructura y con igual énfasis debemos proteger la red de las intrusiones o ataques que pudieran generarse desde el interior de nuestra red.

En la tabla #2 observamos que el origen de los incidentes de seguridad en su mayoría proviene de la LAN, estos ataques posiblemente realizados inconscientemente por empleados curiosos, o de manera premeditada por empleados descontentos, o personal externo con acceso a terminales dentro de la red LAN. (Cisco Systems I. , 2015) (Cisco Systems C. , 2015) (S.A.S., 2014)

% ATAQUES	INCIDENTES DE SEGURIDAD
30%	OTROS
	INCIDENTES DE SEGURIDAD EXTERNOS
	VIRUS
70%	INCIDENTES DE SEGURIDAD INTERNOS
	ERRORES DE USUARIO

Tabla 2 Incidentes de Seguridad (Julio, 2016)

Seguridad de la información

Es el conjunto de procedimientos preventivos y reactivos de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos minimizando al máximo el riesgo de la información. Para facilitar estos procesos de se utiliza normas internacionales definidas por ISO (ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN) y por IEC (COMISIÓN ELECTROTÉCNICA INTERNACIONAL) instituciones que agrupan a los principales organismos de normalización de cada país alrededor del mundo. (ISO 27001, 2013) (Julio, 2016)

Ilustración 3 ISO IEC (ISO 27001, 2013)

Familia ISO 27000

La norma ISO/IEC 27000 está conformada por varios libros que abarcan detalladamente la gestión de seguridad de la información. En la tabla a continuación podemos conocer todos los componentes de la familia ISO 27000.

ISO/IEC	Descripción
27000	Vocabulario y definiciones
27001	Especificación de la estructura metodológica (basada en el BS7799-2:2002) – **Norma Certificable**
27002	Código de prácticas (basada en ISO17799:2005).
27003	Guía de implementación.
27004	Métricas y medidas.
27005	La Administración del Riesgo (basado BS 7799-3)

Tabla 3 Familia ISO 27000 (ISO 27001, 2013)

Norma ISO/EC 27001

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información.

Conceptos básicos ISO 27001

Seguridad de la Información (SI).- Preservación de la confidencialidad, integridad y disponibilidad de la información; adicionalmente autenticidad, responsabilidad, no repudio y confiabilidad.

La Gestión de la Seguridad de la Información, debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total desapareciendo por completo el riesgo, es imposible incluso en el caso de disponer de un presupuesto ilimitado.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. (iso27000, 2013)

La Seguridad de la información se define como la preservación de las siguientes características:

- **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera. (ISO 27001, 2013) (iso27000, 2013)

Propósito fundamental de la seguridad informática

El propósito fundamental de la seguridad es:
"Administrar el riesgo al cual la organización se encuentra expuesta con respecto a la información"

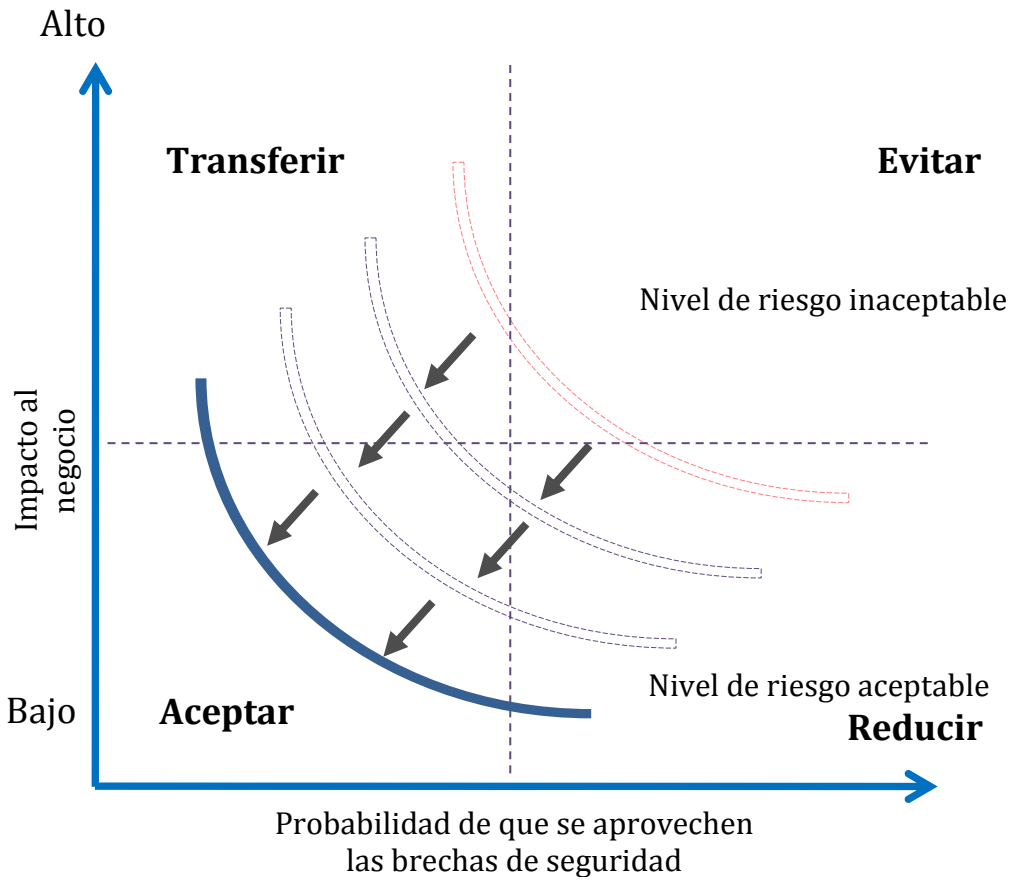


Ilustración 4 Diagrama seguridad industrial (ISO 27001, 2013)

Niveles óptimos de seguridad

El costo de la seguridad de la información y de la seguridad informática, es directamente proporcional al costo del activo que buscamos proteger.

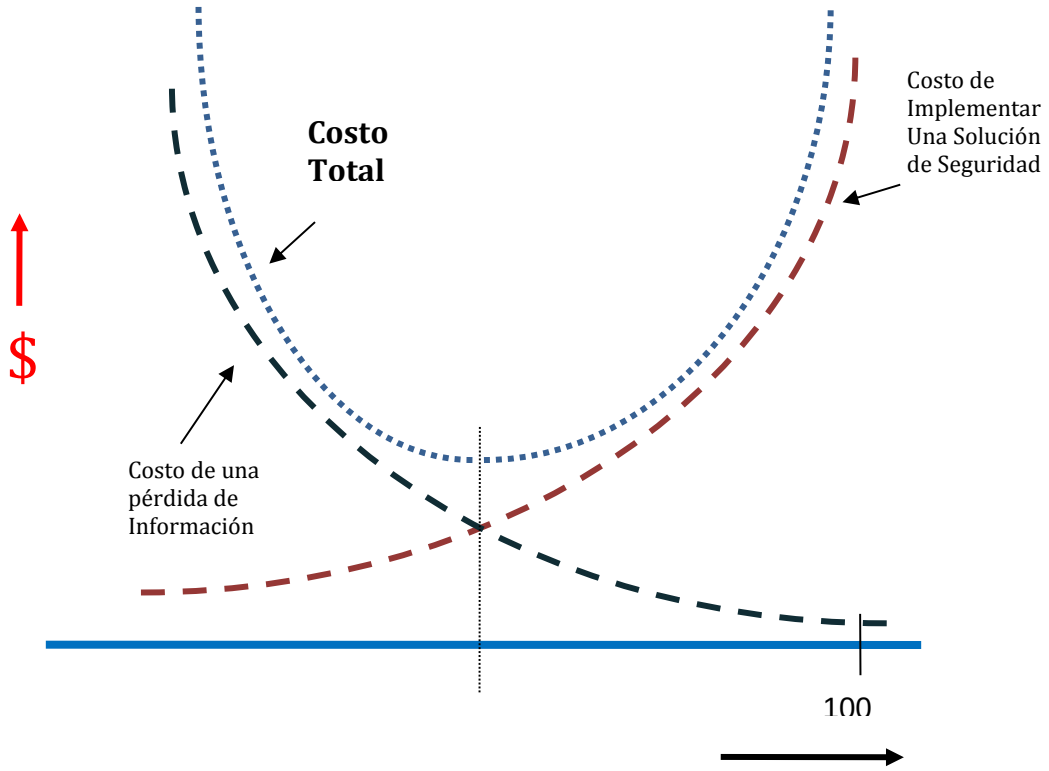


Ilustración 5 Diagrama niveles óptimos de seguridad informática (ISO 27001, 2013)

- **Amenaza**: (A) un evento o situación que podría generar un incidente peligro, heridas o pérdidas en la organización produciendo daños o pérdidas materiales y/o inmateriales.
- **Probabilidad**: (P) la posibilidad de que una amenaza se materialice.
- **Vulnerabilidad**: (V) es el grado de debilidad de un elemento frente a una amenaza.
- **Impacto**: (I) el daño ocasionado por una amenaza tras su materialización.
- **Activo**: Algo que tiene valor para la organización (ISO/IEC 13335-1:2004)

El riesgo para una amenaza está en función de la probabilidad, la vulnerabilidad y el impacto

$$R(A) = f\,(P, V, I)$$

Ecuación 1 Cálculo del riesgo en función de la amenaza (ISO 27001, 2013)

SGSI.- Sistema de Gestión de Seguridad de la Información, es la parte del sistema de gestión de la empresa, basado en un enfoque de riesgos del negocio, para: establecer, implementar, operar, monitorear, mantener y mejorar la seguridad de la información.

Sistema de gestión de seguridad de la información nos permite **CONOCER**, **GESTIONAR Y MINIMIZAR** los riesgos en referencia a la información. Estos riegos ponen en peligro la **CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD** de la información que se considera le activo más valioso de las organizaciones del cual depende el funcionamiento de la misma.

Importante diferenciar seguridad informática de seguridad de la información, la primera se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestra operación. La seguridad de la información se refiere a la protección de los activos de la información es decir email, bases de datos, web site, archivos varios, documentos físicos o lógicos es decir todo lo que contenga información referente a la organización.

El SGSI permite analizar y organizar la estructura de los sistemas de información, con lo que podremos definir procedimientos de trabajo que permitan mantener la seguridad de los activos de la información y mediante la implementación de controles podremos evaluar la efectividad de los procedimientos establecidos, todo esto en concordancia con los objetivos de la organización.

Debemos reconocer que siempre el riesgo para la información va a estar presente dentro del proceso de desarrollo de las actividades lo que procuramos es minimizar al máximo ese riesgo.

Para conseguir de manera efectiva disminuir el impacto de los riesgos se han creado las normas ISO 27000 – 2013 mismas que buscan minimizar la inversión en software, hardware y departamentos de personal dedicados a este fin ya que busca mediante el aporte integral de todos los miembros de la organización establecer una cultura de seguridad.

Las normas de SGSI de una manera empírica han sido utilizadas desde tiempos antiguos, podemos ver en los siguientes 3 ejemplos los esfuerzos realizados para proteger la información.

Sarcófago antiguo Egipto siglo XIII a. C., fabricado de granito negro contenía momia del toro sagrado de Apis y pergaminos con información referente, la tapa del sarcófago pesaba 20 toneladas lo que aseguraba no sea removida por los intrusos, el material de elaboración procuraba la seguridad y preservación de la información contenida e información escrita en sus paredes. (bibliophile, 1993)

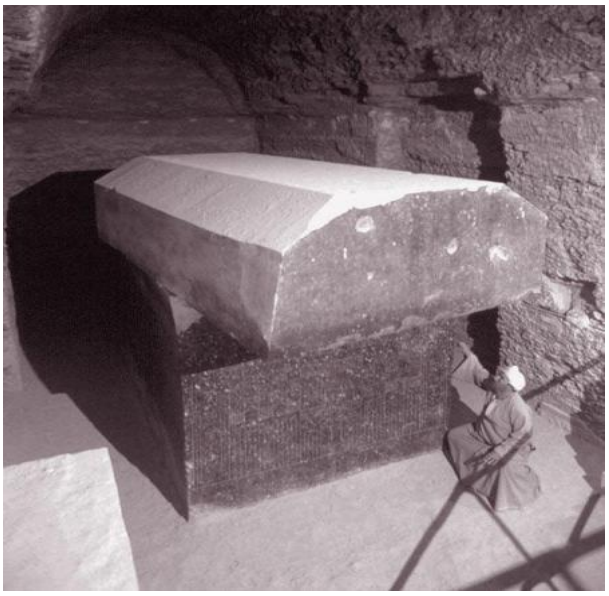


Ilustración 6 seguridad de la información antiguo Egipto (Julio, 2016)

Caja fuerte conteniendo documentos época inicios de imperio romano (bibliophile, 1993)

Ilustración 7 Seguridad de la información imperio romano (Julio, 2016)

Máquina de cifrado rotatorio enigma 1920 Alemania, buscaba encriptar la información del ejército alemán preservando su CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD. (Museo Ejercito España, 2016)

Ilustración 8 seguridad de la información Alemania 1920 (Julio, 2016)

La falta de SGSI en las empresas o instituciones y la gran cantidad y facilidad de acceso a herramientas informáticas que permiten a personas no autorizadas y con poco conocimiento relativo llegar hasta la información protegida de las organizaciones causando graves perjuicios para la empresa.

La información puede estar expuesta a riegos físicos como incendios, inundaciones, terremotos, vandalismo, etc., y a riegos lógicos, como hackers, robos de identidad, spam, pishing, virus, robos de información, espionaje industrial, etc.

Beneficios SGSI

Reducción de riesgos, lo que garantiza la continuidad de la operación.

Ahorro de costos, producto de un adecuado dimensionamiento de requerimientos.

Participación integral de la organización en el proceso de SGSI

Cumplimiento de legislación vigente lo que protege a la empresa de posibles demandas por un tratamiento inadecuado de la información.
Mejora imagen y competitividad siendo más confiable para sus clientes y usuarios.
Permite interactuar en el ámbito de globalización con empresas extranjeras que mantienen estos estándares.
Cumplir con la legislación vigente del país es un requisito indispensable para la implementación de un SGSI. Esto nos permitirá conocer nuestros derechos, los derechos de nuestros clientes o usuarios, así como también nuestros deberes y los de nuestros usuarios o cliente, evitando cometer infracciones involuntarias. (ISO 27001, 2013) (Cisco Wiki, 2017)

Documentación para implantación de SGSI

Políticas: objetivos generales, Proveer la dirección y soporte ejecutivo a la seguridad de información de acuerdo a los requerimientos de negocio, a las regulaciones relevantes y a los requerimientos impuestos.
Procedimientos: desarrollo de objetivos
Instrucciones: comandos técnicos y procedimientos
Registros: indicadores, métricas

Modelo PDCA

PLAN, DO, CHECK, ACT (PLANIFICACIÓN, EJECUCIÓN, SEGUIMIENTO, MEJORA)
Planificación: estudio de la situación actual de la organización para definir y valorar los activos de la información en base a su importancia en relación a la continuidad de la operación. Una vez definida la información crítica de la organización se realiza un análisis de riesgos a los que pudiera estar expuesta la información, a continuación se establece la gestión de los riesgos, una vez finalizados estos procesos se establecen controles que permitan minimizar los riesgos.
Ejecución: implantación de controles técnicos y documentación necesaria, capacitación y concientización al personal involucrado con el proceso.

Seguimiento: evaluación de la eficacia de los controles implementados en la fase anterior, para lo cual se debe disponer de registros e indicadores.

Mejora: Todos los controles o procesos que se ha detectado en la fase de seguimiento que tienen falencias se mejoran en esta fase mediante 3 tipos de medidas, correctoras, preventivas de mejora. Cada ciclo completo debería tener una duración de un año. (ISO 27001, 2013) (ISO 27001, 2013)

Aplicación de SGSI

Conocer

Debe delimitar que se debe proteger de quien y porque, establecer pautas de actuación en caso de incidentes, explicar que está permitido y que no lo está e identificar claramente los riesgos a los que está sometida la organización. Debe tener revisiones anuales y en los casos que se produzcan cambios o incidentes importantes en la organización.

Debe ser corta precisa y de fácil compresión debe ser aprobada por la dirección y aprobada por la misma, debe ser publicitada de manera suficiente en el ámbito de la organización.

Asignación de responsabilidades, responsable de la seguridad, comité de dirección, comité de gestión, Definir el conjunto de responsables en la administración de la seguridad de información, así como las interacciones entre estos responsables, la organización, sus empleados y grupos externos.

Gestionar:

Gestión de riesgos es el proceso por el cual se controlan, minimizan o eliminas los riesgos que afecten a los activos de la información.

Eliminar el riesgo: se consigue eliminando el activo de información, lo cual no es aplicable.

Transferir el riesgo: se consigue con la subcontratación del servicio o mediante la contratación de un seguro que cubra los gastos y pérdidas en caso que ocurra una incidencia. En Este caso se debe verificar si el bien es más valioso que el costo del seguro y también si el bien puede ser manejado por terceros ya que al ser confidencial puede ser manejado solo por la organización.

Asumir el riesgo: la decisión debe ser tomada y firmada por la dirección de la empresa esto es viable solo en caso que la organización controle el riesgo y vigile que no aumenta.

Mitigar el riesgo: se consigue implantando una serie de medidas para salvaguardar los activos de información

Riesgo residual: Es el nivel de riesgo aceptable por la organización en el cual se detallan todos los riesgos de la organización. (ISO 27001, 2013) (ISO 27001, 2013)

Para determinar controles debemos en primer lugar realizar una cálculo del costo del control versus el costo del impacto de esa manera se determinar su eficiencia. A la vez se debe definir controles existentes que puedan ser reutilizables y el consto de implantación y mantenimiento.

Para la implantación de los controles técnicos (antivirus, firewall) de la solución se encargara al responsable técnico mientras que los controles administrativos (reglas procesos) la dirección es la que deberá establecer y difundir a la entidad.

Asegurar el cumplimiento de la normativa de Seguridad de Información durante la selección, contratación y termino de empleo o contrato de los aspirantes, colaboradores internos o externos, contratistas o terceras partes que tengan o vayan a tener acceso a los activos organizacionales.

La definición de indicadores permitirá verificar si el funcionamiento de los controles es el adecuado o requiere mejora.

Alcance del sistema de seguridad

Definir que procesos críticos deben ser protegidos, y de que, se deben proteger

Definir actividades de la organización

Ubicaciones físicas que deben ser protegidas

Tecnología disponible para el proyecto

Procesos excluidos de la implantación del sistema.

Definición de presupuesto y personal técnico para la implantación y mantenimiento del sistema (ISO 27001, 2013)

Definición de políticas de seguridad

Definir directrices en función de las necesidades de la organización y de la legislación vigente

Que se debe proteger, de quien y por qué. Límites de comportamiento aceptable y cuál es la respuesta si estos límites se sobrepasan.

Corta precisa y de fácil comprensión, aprobada por la dirección y publicitada por la misma, disponible para consulta todo el tiempo.

Definir responsabilidad, concientizar que la política de seguridad protege la información, el personal, la reputación de la empresa y procura la continuidad de la misma

Documentos: Política de seguridad, compromiso de la dirección con la política, resumen de las políticas, definición de responsabilidades generales y específicas, referencias a documentación que sustente la política de la seguridad implementada.

La política de seguridad debe tener revisiones de versión anuales, y también en caso de incidentes graves, auditoria, cambios estructurales de la organización.

Roles: responsable de seguridad, comité de dirección de la seguridad, comité de gestión de la seguridad. Identificar riesgos por parte de terceros en caso que tengan cualquier nivel de acceso a la información de la organización se debe involucrar en el proceso de seguridad de la información entregando información general del proceso y comprometiendo a la seguridad de la información de la empresa mediante la firma de convenios de confidencialidad.

Como parte de la organización de la seguridad se deben implementar programas de concienciación y formación. (ISO 27001, 2013)

Tipos de activos

Servicios: Ofrecidos a clientes tanto internos como externos de la organización
Datos / Información: todo lo referente a los datos que genera la operación de la organización.
Aplicaciones: todos los programas informáticos que dispone la empresa para su operación.
Equipos informáticos: todo el hardware que disponga la empresa para su operación.
Personal: incluye personal de nómina, subcontratado, clientes, toda persona que se relacione con la organización.
Redes de comunicaciones: pueden ser redes propias de la empresa o contratadas a terceros.
Soportes de información: dispositivos físicos que permiten el almacenamiento de información durante un largo periodo de tiempo pudiendo ser propios o contratados.
Equipamiento auxiliar: Se refiere a equipos como climatización, luminarias, destructoras de papel.
Instalaciones: se refiere al sitio físico en el que están los diferentes tipos de activos, pueden ser oficinas, edificios, vehículos, etc. Estructurar el conjunto de controles de restricción física para salvaguardar la integridad de los activos de información organizacional, sea cual sea su naturaleza.
Intangibles: se refiere a la imagen y reputación de la empresa. (ISO 27001, 2013)

Inventario de activos: documento en el que se identifica y clasifica cada activo del SGSI debe disponer cada uno de los siguientes ítems:
Descripción: resumen de las características del activo
Localización: ubicación del activo puede ser física o lógica
Propietario: define el grado de seguridad que requiere el activo, y no necesariamente es la persona que gestiona la seguridad o mantenimiento del activo, por ejemplo base de datos de clientes o usuarios pertenece al director comercial de la organización pero la gestiona el área de sistemas y sus usuarios son los ejecutivos del área comercial.

Árbol de dependencias de activos evidencia la relación existente entre los activos de la información nos permite analizar riesgos en caso de presentarse fallos o incidencias de seguridad.

Valoración de activos

Cuantitativa: en función del costo de los activos

Cualitativa: en función de la importancia puede definirse del 1 al 10 o como alto, medio o bajo. Para realizar esta calificación se debe considerar los parámetros de integridad, disponibilidad y confidencialidad, para lo cual nos haremos la pregunta cómo afectaría a la organización si este activo tuviera problemas con su integridad, o cómo afectaría a la empresa si este activo tuviera problemas con su disponibilidad, o cómo afectaría a la empresa si este activo tuviese problemas con su confidencialidad. (ISO 27001, 2013)

Análisis y valoración de los riesgos

Para el análisis de riesgos se debe identificar los riesgos de los activos de la organización, determinar la magnitud del riesgo e identificar las áreas que requieren salvaguardas, con estos datos podemos determinar el impacto económico de un fallo de seguridad y la probabilidad de que ocurra un fallo sobre el activo analizado. Para el análisis de riesgos debemos considerar en todo momento los recursos humanos y económicos con los que cuenta la organización, es decir optimización de recursos considerando que la inversión en seguridad es directamente proporcional con el valor del activo que protegemos además se debe calcular la inversión de mantenimiento.

Proceso:

1. Inventario de activos
2. Identificación de las amenazas de activos
3. Vulnerabilidades de los activos en función de las amenazas
4. Análisis de las medidas de seguridad implementadas

Al finalizar este proceso podremos medir el nivel de riesgo de la organización y tomar medidas al respecto. Para facilitar los procesos se utilizan metodologías detalladas continuación:

Magerit descrita en la norma ISO/IEC 27005

Esta metodología de análisis de riesgos tiene disponible herramientas informáticas, ninguna de uso gratuito.

https://www.sigea.es/gxsgsi-analisis-de-riesgos7/

https://www.r-box.com.ar/demo/

http://www.secitor.com/prod01-secitor.htm

Octave descrita en la norma NIST SP 800-30

Dispone de varias versiones basadas en la cantidad de activos de la información, OCTAVE-ALLEGRO menos de 100 activos, OCTAVE-S menos de 300 activos, OCTAVE más de 300 activos. Tiene su herramienta informática basada en hojas de cálculo de igual forma licencias no son de uso gratuito. Tipos de activos de OCTAVE

1. Sistema (hardware, software y datos).
2. Personas.

Análisis de Riesgos

Comparativa de Metodologías:

Puntos a Destacar	Magerit	CRAMM	NIST SP 800-30	Octave
Aplicación	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad	* Analisis de riesgos * Gestión del riesgos * Plan Director de Seguridad
Quien lleva a cabo la metodología	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa	* Pequeño grupo interdiciplinario conformado por empleados de la misma empresa
Costo	* No tiene costo, ya que es una normativa de libre aplicación * Plantea un analisis de costo beneficio, expresa una formula de ROI (Retorno de la inversión)	La versión 4 costaba por el año 2001: * Para una compañia comercial: £2800 + £850 al año de mantenimiento * Para agencias y departamentos del estado britanico: £1600 + £850 al año de mantenimiento	* Habla de costo relacionado con el beneficio, otorgando una condición relativa al costo de un plan director de seguridad, siempre que el costo sea menor al costo del riesgo analizado y solventado, el costo será bajo	* Uso Interno: Gratuito * Uso Externo: Se debe comprar la licencia al SEI si se quiere implementar la metodología a un tercero
Resultado del analisis (outputs)	Resultados ordinales y cardinales	* Tabla de valorazión del riesgo sobre los activos (escala de 1 a 10)	* Lista de controles recomendados * Resultados de la documentación	Fase 1: Activos Critivos, requerimientos criticos para activos criticos, vulnerabilidades de activos criticos, lista de practicas de seguridad actuales, lista de vulnerabilidades actuales de la organización Fase 2: Componentes clave, vulnerabilidades tecnologicas actuales Fase 3: Riesgos de los activos críticos, metricas del riesgo, estrategia de protección, planes de mitigación del riesgo

Tabla 4 comparativa software para análisis de riesgos **(ISO 27001, 2013)**

Seguimiento monitorización y registro

Debemos mantener un registro de incidencias que guarde relación con cada uno de nuestros objetivos anuales de cumplimiento, ese registro de incidencias nos permitirá conocer si los objetivos se cumplieron. Este análisis se realiza en el procedimiento de AUDITORIAS INTERNAS. El resultado de esta auditoría interna se entrega a la dirección de la empresa de esa manera podemos conocer si los objetivos se cumplieron y tomar las medidas pertinentes para optimizar nuestro SGSI. Aquí es donde se aplica el modelo PDCA.

Acciones correctivas: requiere acción inmediata de resolución

Acciones preventivas: se debe tomar en cuenta a ser aplicada como oportunidad de mejora.

Plan de continuidad del negocio

El objetivo es impedir que la operación se interrumpa, mantener el nivel de servicios y de ser el caso que se presente un incidente de seguridad de la información, estar preparados para que el tiempo de afectación a la operación sea mínimo.

Se debe determinar cuáles son los procesos críticos que requieren recuperación inmediata ya que no es siempre posible recuperar todos los procesos al mismo tiempo. Los fallos deben ser documentados y registrados de forma exhaustiva ya que debemos elaborar medidas de respuesta que garanticen no verse afectados por el mismo fallo nuevamente. (Julio, 2016) (Cisco Systems I. , 2015)

Definición de situaciones críticas

Son riesgos que no pueden ser evitados a pesar de las medidas de seguridad implantadas.

Comité de emergencias

Es el responsable de organizar al personal y las acciones para que la empresa pueda recuperarse de un incidente.

Definición de posibles situaciones

- Situación que provoca una incidencia
- Acciones y secuencias
- Registros

Conceptos básicos de networking y seguridad informática

Wan

Red de área extensa: las redes de área extensa (WAN, Wide Area Network) son infraestructuras de red que proporcionan acceso a otras redes en un área geográfica extensa, pueden interconectar sitios dentro de una misma ciudad o entre ciudades o entre países. (Cisco Systems C. , 2015)

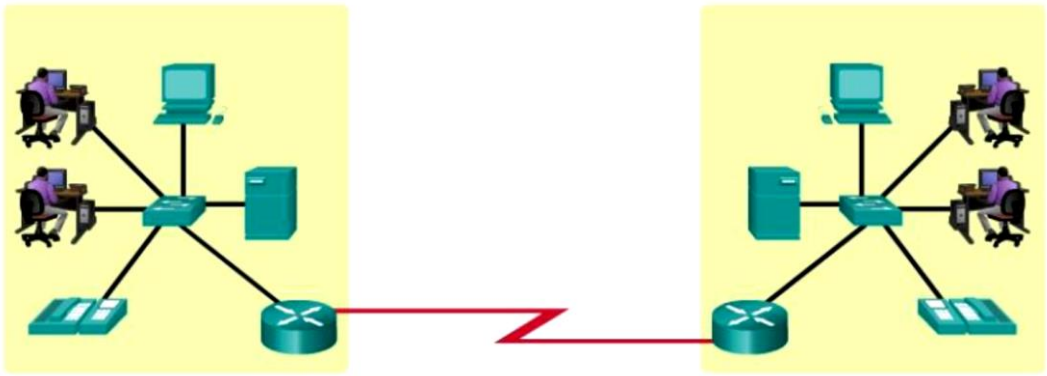


Ilustración 9 WAN red de área extensa (Cisco Systems C. , 2015)

Lan

Red de área local: las redes de área local (LAN, Local Area Network) son infraestructuras de red que proporcionan acceso a los usuarios y a los dispositivos en un área geográfica pequeña, una oficina, o una casa. (Cisco Systems C. , 2015)

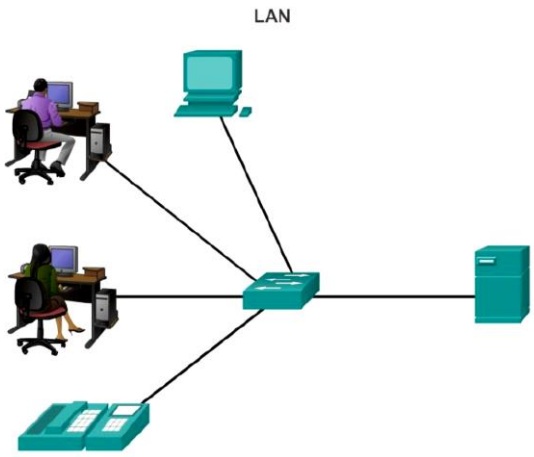


Ilustración 10 LAN red de area local (Cisco Systems C. , 2015)

Wlan

LAN inalámbrica: las LAN inalámbricas (WLAN, Wireless LAN) son similares a las LAN, pero se interconectan de forma inalámbrica entre los puntos de acceso y los usuarios, se utilizan para un área geográfica pequeña, oficinas o casas. (Cisco Systems C. , 2015)

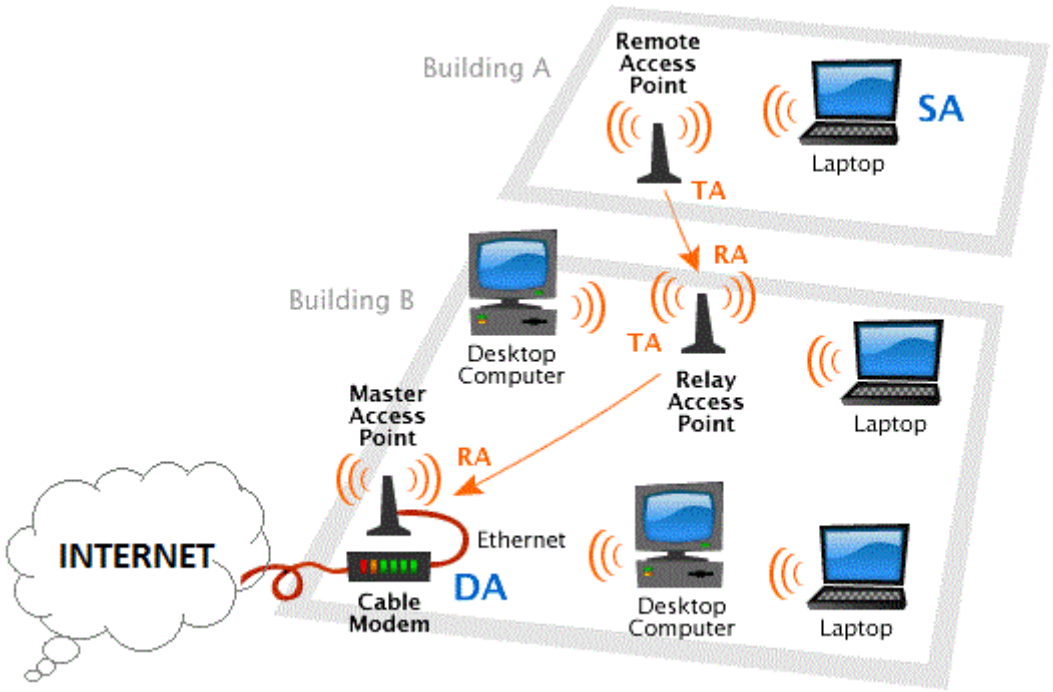


Ilustración 11 WLAN red de área local inalámbrica (Cisco Systems C. , 2015)

Definitivamente la tecnología WLAN es el estándar de conectividad que se está imponiendo debido a la facilidad de conexión y movilidad que proporciona a los usuarios finales, sin embargo se deben considerar aspectos importantes de implementación sobretodo en redes corporativas medianas.

Cuando se definió el estándar IEEE 802.11 (que regula las redes locales inalámbricas), se especificó también los tres rangos de frecuencia disponibles para los dispositivos que desearan emitir de esta forma: 2.4 GHz, 3.6 GHz y 5 GHz. La mayoría de dispositivos actuales operan, por defecto, en la franja de frecuencias cercana a 2.4 GHz, por lo que es en la que vamos a centrarnos. Cada rango de frecuencias fue subdividido, a su vez, en varios canales.

Para 2.4 GHz, estamos hablando de 14 canales, separados por 5 MHz. Eso sí, cada país y zona geográfica aplica sus propias restricciones al número de canales disponibles.

Por ejemplo, en Norteamérica tan sólo se utilizan los 11 primeros, mientras que en Europa disponemos de 13. El problema de esta distribución es que cada canal necesita 22MHz de ancho de banda para operar, esto produce un solapamiento de varios canales contiguos.

Aquí aparece un concepto importante a tener en cuenta: el solapamiento. Como puede observarse en el gráfico, el canal 1 se superpone con los canales 2, 3, 4 y 5, y por tanto los dispositivos que emitan en ese rango de frecuencias pueden generar interferencias. Lo mismo ocurre con el canal 6 y los canales 7, 8, 9 y 10. Parece lógico pensar entonces que, si nuestra conexión Wi-Fi no va todo lo bien que debería, podría intentarse mejorar la red cambiando el canal a otro menos usado entre los puntos de acceso cercanos y que no se superponga con ellos.

Para saber los canales de las redes cercanas, y si estamos usando Windows Vista o Windows 7, es tan sencillo como abrir la consola de comandos (haciendo clic en Inicio y escribiendo cmd en “Buscar programas y archivos”). Una vez dentro, escribimos el comando netsh wlan show all y pulsamos enter. Si todo ha ido bien, en la ventana con fondo negro nos aparecerán todas las redes que veíamos antes, pero con más datos.

Lo que seguramente verán entonces son muchas redes que utilizan el canal 7.
Entonces, lo ideal sería cambiar nuestro canal al 1 o al 11, ya que no se solapan. Si, en cambio, ven que llega una señal muy potente en otro canal y creen que puede ser la causante de las interferencias, pueden cambiar a otro canal distinto. Para algún atacante de nuestra red sería tan sencillo como conectar un dispositivo WIFI y transmitir en el mismo canal de nuestra red si su antena tiene mayor potencia fácilmente afectara el desempeño de nuestra red. Los routers inalámbricos, puntos de acceso y Wireless Lan Controller actuales disponen de la función de channel autosense que evalúa las red inalámbrica en el canal de 2.4 Mhz y en caso de encontrar algún dispositivo transmitiendo en la misma frecuencia cambia automáticamente a otra frecuencia por ende de canal a una frecuencia que determine libre de transmisión en el rango de cobertura.

Dispositivos de versión corporativa pueden también incrementar la potencia de transmisión trabajando en el mismo canal en caso que el espectro este saturado. (RUCKUS, 2016) (Cisco Wiki, 2017) (Mikrotik Wiki, 2015)

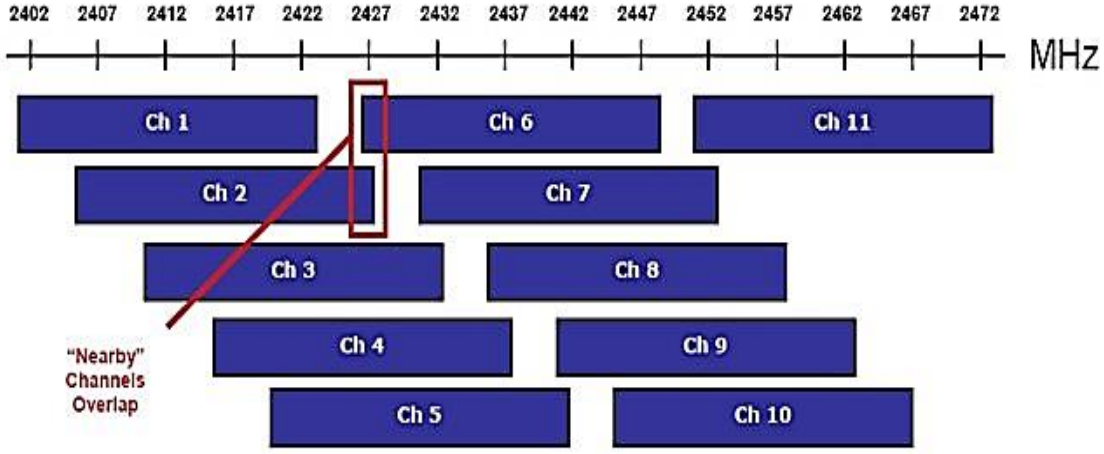


Ilustración 12 canales de transmisión WLAN (S.A.S., 2014)

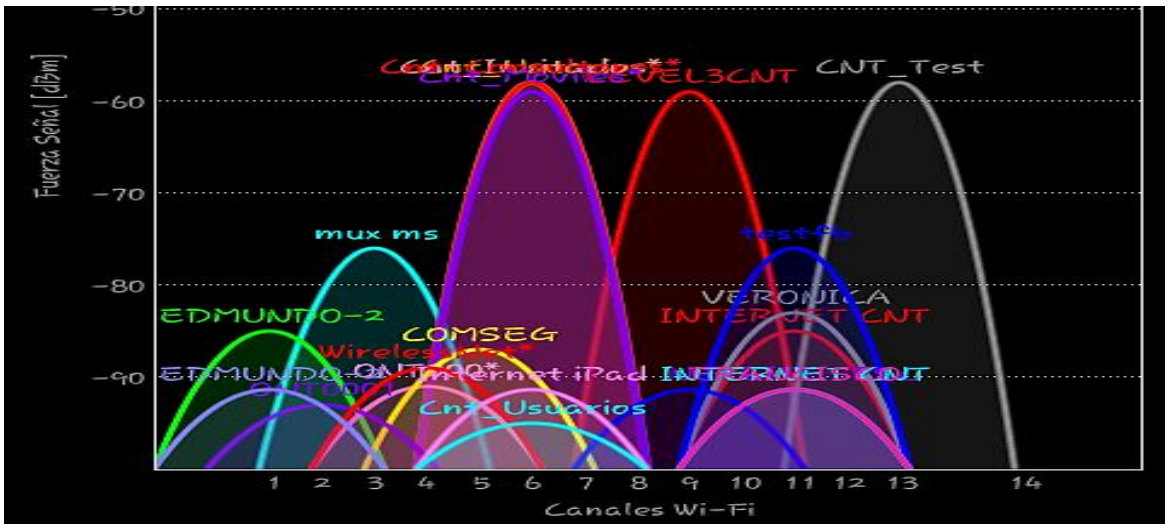


Ilustración 13 análisis de utilización de canales WLAN (Julio, 2016)

San y File Server

SAN Red de área de almacenamiento: las redes de área de almacenamiento (SAN, Storage area network) son infraestructuras de red diseñadas para admitir servidores de archivos y proporcionar almacenamiento, recuperación y replicación de datos. Un file server puede formar parte de una SAN o funcionar de forma individual para una red pequeña. (Cisco Systems C. , 2015)

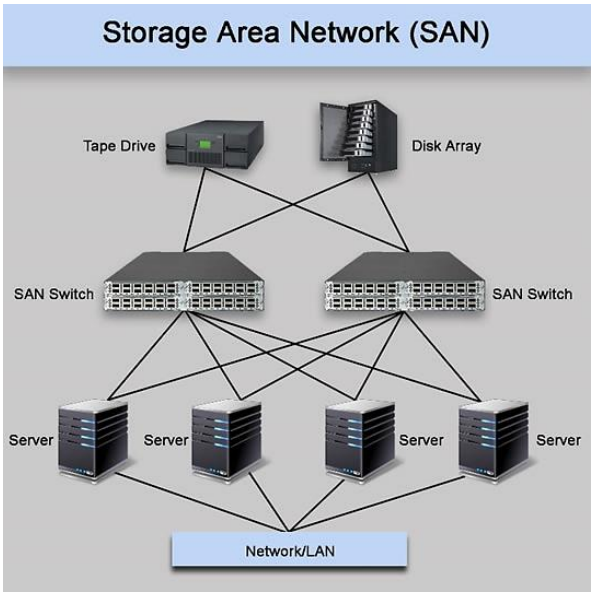


Ilustración 14 SAN red de servidores (Cisco Systems C. , 2015)

Intranet

Conexión privada de redes LAN y WAN que pertenece a una organización y que está diseñada para que solo accedan a ella los miembros de la organización. (Cisco Systems C. , 2015)

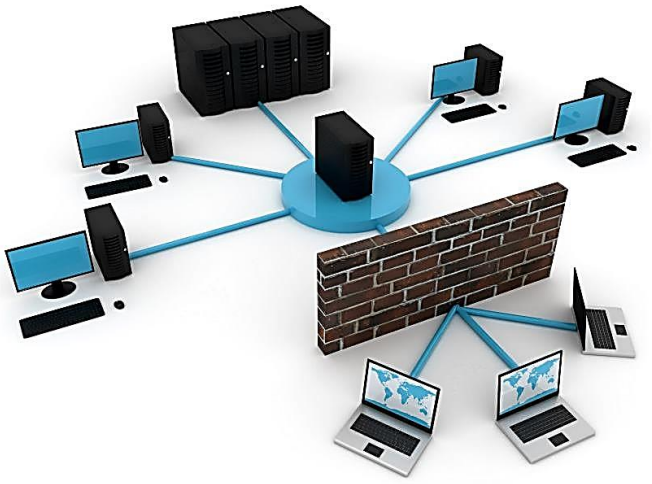


Ilustración 15 INTRANET red de uso interno (Cisco Systems C. , 2015)

Seguridad informática

Internet ha evolucionado y ha pasado de ser una intranet de organizaciones educativas y gubernamentales fuertemente controlada a ser un medio accesible para todos para la transmisión de comunicaciones comerciales y personales. Como resultado, cambiaron los requerimientos de seguridad de la red informática. La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Si se pone en peligro la integridad de esos recursos, esto podría traer consecuencias graves para la organización, por ejemplo:

- Interrupciones de la red que impidan la comunicación y la realización de transacciones, o consultas.
- Robo de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia.
- Información personal o privada que se pone en riesgo o se hace pública sin el consentimiento de los usuarios.
- Mala orientación y pérdida de recursos personales y comerciales.
- Pérdida de datos importantes cuyo reemplazo requiere un gran trabajo de recuperación o simplemente son irreemplazables o irrecuperables.

Existen dos tipos de problemas de seguridad de red informática que se deben tratar: la seguridad de la infraestructura de red de comunicación y la seguridad de los dispositivos de acceso.

La seguridad de una infraestructura de red incluye el aseguramiento físico de los dispositivos que proporcionan conectividad de red y prevenir el acceso no autorizado a la gestión de los equipos, así también prevenir el ataque a estos equipos desde redes externas de comunicación.

La seguridad de los dispositivos de accesos se refiere a proteger los equipos que se interconectan mediante la red de comunicación, ya que la información que transmiten por la red o la información almacenada en ellos podría estar infectada por virus o podría estar generando problemas en la red debido a aplicaciones que saturen los recursos afectando el desempeño.

Para alcanzar los objetivos de seguridad de red, hay tres requisitos principales.

Hay mediadas básicas que se implementan en una red para protegerla de ataques, uno de ellos es mediante la implementación de un sistema sólido de autenticación de usuarios, el establecimiento de contraseñas que sean difíciles de desencriptar o deducir una política de cambio periódico de claves.

La encriptación de datos o de transmisión de paquetes con el fin de que solamente el destinatario deseado pueda leerlos

Implementación de dispositivos de firewall de red, junto con el software antivirus, antispyware de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y la solidez del sistema para detectar, repeler y resolver esos ataques.

Crear infraestructuras de red totalmente redundantes, con pocos puntos de error únicos, puede reducir considerablemente el impacto de estas amenazas.

La implementación de seguridad de red en redes corporativas medianas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico.

Listas de control de acceso en router de borde: las listas de control de acceso (ACL, Access control list) filtran el acceso y el reenvío de tráfico.

Sistemas de prevención de intrusión: los sistemas de prevención de intrusión (IPS) identifican amenazas de rápida expansión, como ataques de día cero o de hora cero, bloquean el tráfico que genera el ataque de esta manera son se elimina la amenaza solamente desde una IP sino desde cualquier IP que genere este tráfico irregular.

IPSec VPN: las redes privadas virtuales (VPN, Virtual private networks) con IPSec proporcionan un acceso seguro a los trabajadores remotos. (Cisco Systems I. , 2015) (Cisco Wiki, 2017) (ISO 27001, 2013) (Mikrotik Wiki, 2015)

Resumen leyes y reglamentos aplicables a nuestra investigación de acuerdo a la legislación ecuatoriana.

En el desarrollo del trabajo de sistemas y telecomunicaciones es indispensable tener pleno conocimiento de las leyes y reglamentos que regulan estas actividades, a continuación el investigador enuncia las que considera son las más importantes para la investigación planteada. El documento anexa las siguientes Leyes y Reglamentos referidos para análisis:

Ley orgánica de telecomunicaciones

- Artículo 1.- Objeto de la ley.
- Artículo 2.- Ámbito de la ley.
- Artículo 3.- Objetivos. 17. mecanismos de coordinación
- Artículo 5.- Definición de telecomunicaciones

Título II redes y prestación de servicios de telecomunicaciones

Capítulo I Establecimiento y explotación de redes

- Artículo 9.- Redes de telecomunicaciones.
- Artículo 10.- Redes públicas de telecomunicaciones.
- Artículo 11.- Establecimiento y explotación de redes.
- Artículo 13.- Redes privadas de telecomunicaciones.
- Artículo 16.- Telecomunicaciones Reservadas a la Seguridad Nacional.
- Artículo 17.- Comunicaciones internas.

Título III derechos y obligaciones

Capítulo I Abonados, clientes y usuarios

- Artículo 21.- Definición y tipo de usuarios.
- Artículo 22.- Derechos de los abonados, clientes y usuarios.
- Artículo 23.- Obligaciones de los abonados, clientes y usuarios.

Capítulo II Prestadores de Servicios de Telecomunicaciones

- Artículo 24.- Obligaciones de los prestadores de servicios de telecomunicaciones.

Título VIII Secreto de las comunicaciones y protección de datos personales

Capítulo I Secreto de las comunicaciones

- Artículo 76.- Medidas técnicas de seguridad e invulnerabilidad.
- Artículo 77.- Interceptaciones.
- Artículo 78.- Derecho a la intimidad.
- Artículo 80.- Procedimientos de revelación.
- Artículo 87.- Prohibiciones. Queda expresamente prohibido:

TÍTULO XIII Régimen sancionatorio

Capítulo I Infracciones

- Artículo 117.- Infracciones de primera clase.
- Artículo 118.- Infracciones de segunda clase.
- Capítulo II Sanciones
- Artículo 121.- Clases.
- Artículo 122.- Monto de referencia.

Delitos informáticos Ecuador

Código orgánico integral penal

(Registro oficial No. 180 febrero 2014)

La presencia y proceso de las nuevas TIC´s en la Sociedad ha dado lugar al surgimiento de nuevas actividades y figuras jurídicas que han obligado a judicializar actividades consideras delitos en el ámbito informático.

- Artículo 178.- Violación a la intimidad
- Artículo 179.- Revelación de secreto
- Artículo 180.- Difusión de información de circulación restringida
- Artículo 190.- Apropiación fraudulenta por medios electrónicos
- Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles
- Artículo 230.- Interceptación ilegal de datos
- Artículo 232.- Ataque a la integridad de sistemas informáticos
- Artículo 233.- Delitos contra la información pública reservada legalmente
- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

Capitulo 3

Diagnóstico

Con la finalidad de conocer el nivel de conocimiento acerca de la norma ISO 27001 y el alcance que tiene en la actualidad se ha realizado entrevista estructurada referente al tema a 10 profesionales de telecomunicaciones y sistemas que interactúan continuamente con la infraestructura analizada, con los resultados de estas entrevistas estructuradas se ha podido concluir que el conocimiento de implementación requisitos, procedimientos costos etc., no es de dominio de los profesionales consultados se mantiene el concepto erróneo que para implementar ISO 27001 se debe certificar en la norma y que esto solo se lo puede realizar mediante la intervención de empresas especializadas, la importancia de trabajar con normas internacionales debe ser una prioridad para los profesionales ecuatorianos la investigación y disponibilidad de la información al respecto debería ser una política de estado.

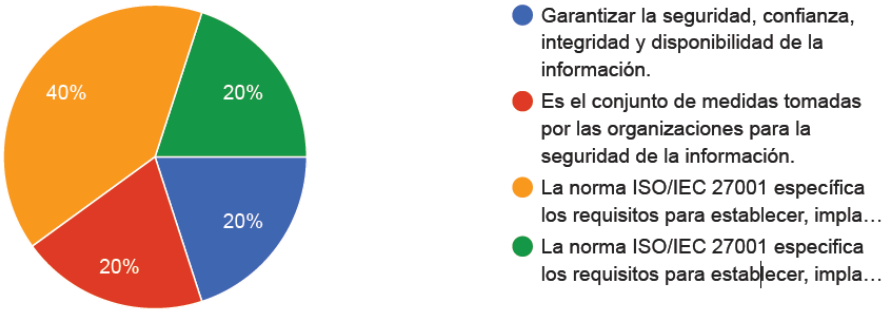
Entrevista estructurada

Interpretación resumen de datos de las preguntas individuales de entrevista estructurada

Con la finalidad de medir el conocimiento de los profesionales en funciones acerca de la norma ISO 27001 y de los procedimientos de implementación de infraestructura se realizó mediante un formulario en línea una serie de preguntas referentes al tema de investigación cuyo resultado detallamos a continuación.

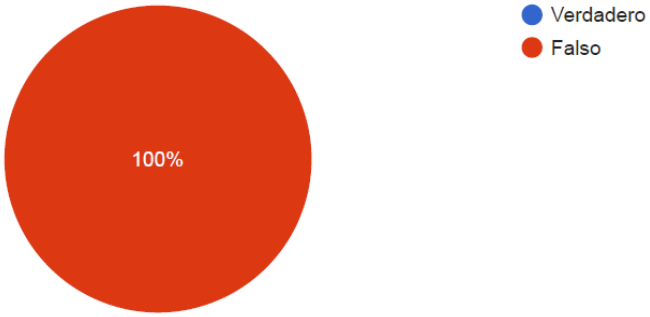
Cuál de los siguientes conceptos corresponden a la norma ISO/EC 27001

5 responses

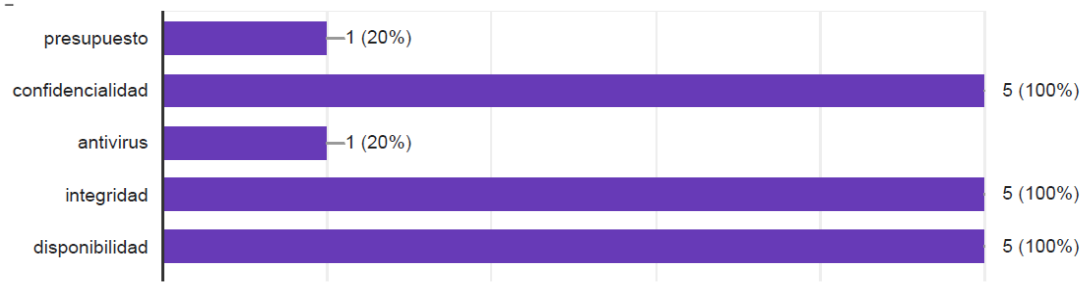


La seguridad de la información es igual a la seguridad informática?

5 responses



Seleccione los principales objetivos de la gestión de norma ISO/EC 27001



Aplica Usted el modelo PDCA en sus labores profesionales con clientes corporati si / no , por que?.

5 responses

no porque no tenemos esa costumbre dentro de la organización

no debido a que no es una exigencia de la organización en la que laboro

no corresponde a mis labores

desconosco

si ya que nos ayuda a optimizar los procesos internos

Considera Usted que la norma ISO/EC 27001 debe incluirse en toda actividad informática corporativa, si / no , por que?.

5 responses

si por que son normas internacionales de seguridad de la información que es el bien mas valioso después de las personas en una institución.

no debido a que no todos disponen de presupuesto para aplicar las normas internacionales

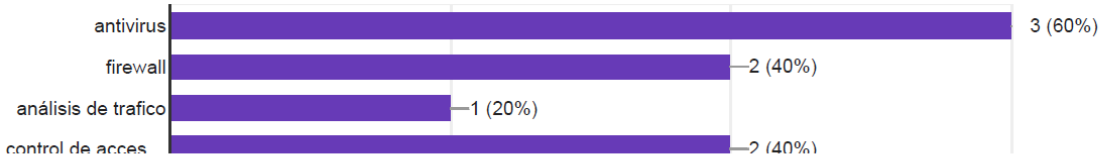
si

desconosco

si ya que representa el estándar de seguridades de la informacion

En una aplicación de acceso a Internet corporativo cual de las siguientes medidas de seguridad son implementadas por Usted como profesional informático

5 responses



Que medidas de seguridad de la información aconseja sea implementadas en toda infraestructura de acceso a Internet corporativo

5 responses

firewall, encriptacion, control de ancho de banda, niveles de privilegio de usuario, control de usuarios.

control de ancho de banda y antivirus

depende de los presupuestos asignados

antivirus

las politicas de seguridad sugeridas por la ISO 27001

Considera Usted que los profesionales informáticos y de telecomunicaciones en Ecuador utilizan normas internacionales para implementar infraestructuras tecnológicas corporativas, si / no , por que?.

5 responses

no porque no se tiene el conocimiento necesario de las misma o la conciencia de su importante aplicación

no por que no están difundidos

no porque no es un proceso no contratado

si ya que manejan los sistemas de seguridades

no al momento Ecuador inicia su actividad de gran despliegue de tecnologias de la informacion las implementaciones actuales son muy basicas

Considera Usted que Ecuador esta preparado para defenderse ante un ataque informático interno o externo dirigido a sus instituciones gubernamentales, si / no , por que?.

5 responses

no, por que no hay ningún procedimiento estándar que nos permita articular estas iniciativas

no porque no se dispone de dispositivos de seguridad adecuados

si por que se dispone de seguridades en las redes

si

no debido a que el conocimiento de técnicas efectivas de prevención y respuesta no están disponibles

Considera Usted que la seguridad de la información y la seguridad informática es parte fundamental de una red informática o se puede trabajar sin tomar en consideración estos conceptos en infraestructuras de red corporativa?

5 responses

Option 1

es posible trabajar sin tomar en cuenta lo indicado

Con el avance de la tecnología se puede considerar indispensable

claro que se puede trabajar aunque algunos problemas podrían presentarse

es parte fundamental debido a que el activo mas valioso depende de estos conceptos

Ilustración 16 resumen Entrevista estructuradas seguridad información (Julio, 2016)

Análisis de la solución actual

Para el acceso de los clientes a la red se dispone de una infraestructura inalámbrica, las características de la red actual son analizadas a continuación.

Protocolo de transmisión inalámbrico

Se verifica en el grafico que al momento de la transmisión hay muchas redes utilizando es medio de transmisión, observamos muchas redes que utilizan el canal 7. Entonces, lo ideal sería cambiar nuestro servicio al canal al 1 o al 11, ya que no se solapan. En caso que detectemos una señal muy potente en otro canal y determinamos que puede ser la causante de las interferencias, podemos cambiar a otro canal distinto que, mirando el gráfico del que hablábamos antes, no se solape con el canal interferente.

Laboratorio

Para el presente laboratorio se tomó una muestra con un analizador de señal WIFI provisto mediante la APP wifi analizer implementado Android OS, aplicación de versión gratuita, que nos permite apreciar las diferentes señales WIFI que se muestra a continuación:

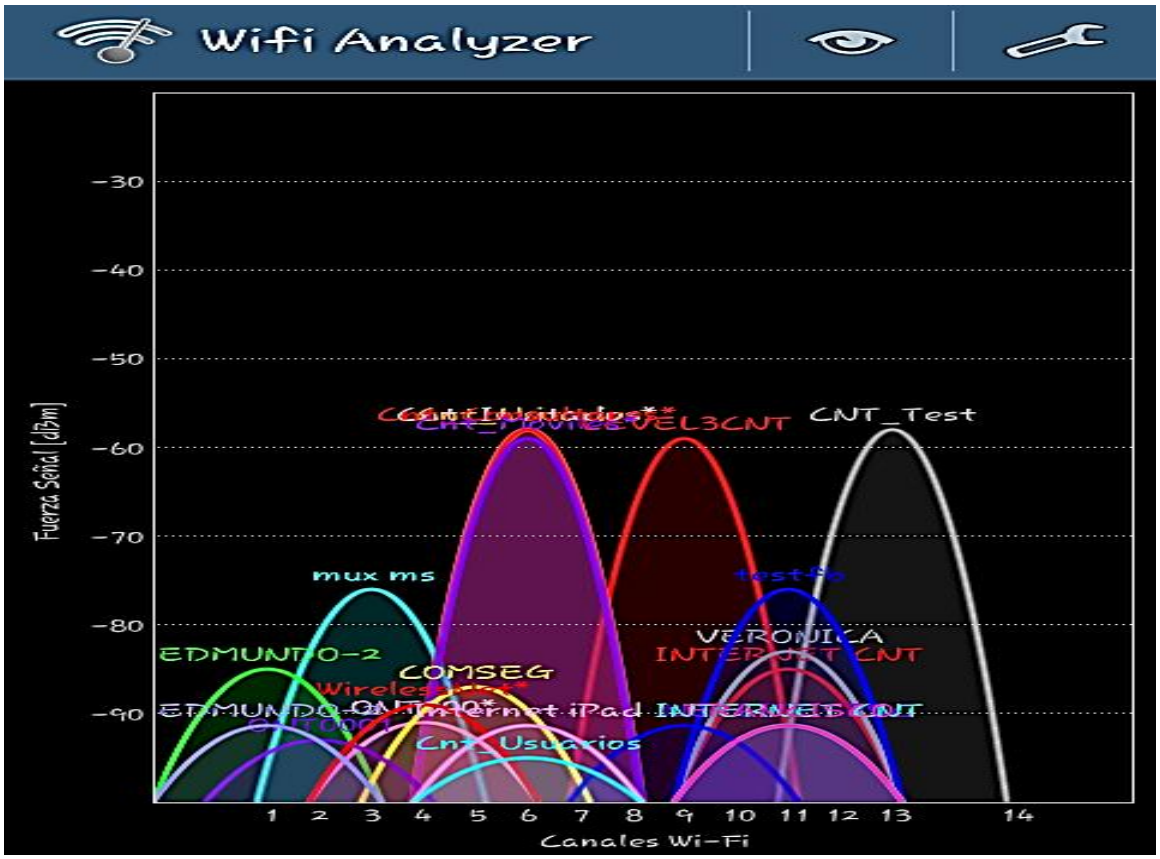


Ilustración 17 Analizador redes WLAN (Julio, 2016)

En el presente gráfico se pueden apreciar los 14 canales mencionados en la teoría de este informe, y las diferentes redes WIFI que se pudieron capturar al momento de escaneo. La presencia de diferentes redes inalámbricas que se solapan una a otras puede ser una fuente de interferencia importante, en este caso procederemos a encender el AP CISCO que se utiliza en el enlace.

Una vez que se activó el AP, se puede apreciar las redes inalámbricas aparecen en el analizador de WIFI, ENLACE, MÓVIL Y PRENSA, a simple vista se puede notar que el centro de la portadora está en el canal 7, fijado automáticamente por el equipo inalámbrico.

Haciendo uso de la conexión por consola al equipo cisco AP 1042N, procederemos a usar el comando *show controllers* que nos permite confirmar que efectivamente el enlace se encuentra trabajando en el canal 7 tal como lo indica la siguiente gráfica.

En este caso se va a proceder a realizar una configuración manual que escoja el canal menos congestionado, el comando a usarse es channel least-congested tal como se muestra en la siguiente gráfica.

En este momento se procede a realizar nuevamente el escaneo y podemos ver que el nuevo canal asignado es el diez, así como también el comando que permite realizar este cambio.

Con esta acción se puede corregir el canal en el cual se encuentra la interferencia, es importante tomar en cuenta que la banda de 2.4 Giga Hertz está bastante ocupada y hasta cierto punto saturada debido al número de clientes que utilizan redes WIFI, otra opción es utilizar los canales de la banda de 5 Gigas que equivale a una carretera de 11 carriles en donde la distancia entre las portadoras es mucho más separada evitando que se traslape la señal entre redes inalámbricas, el inconveniente radica en que la mayoría de los equipos terminales tienen la tecnología 2.4 Giga Hertz. Esto limita el uso de la banda de 5 Giga Hertz a equipos de última tecnología en versiones de alto desempeño. Se tiene que recalcar que las pruebas de conexión se realizaron con computadoras HP, DELL, y APPLE, sin tener inconveniente alguno.

Una vez que hemos establecido la importancia de las comunicaciones en estas reuniones, debemos entender la importancia de una implementación sumamente profesional, es por esto que se debe diferenciar claramente tres etapas de implementación. (Mikrotik, 2016) (RUCKUS, 2016) (S.A.S., 2014)

Análisis de consumo ancho de banda de 10 eventos diferentes

Monitoreo de ancho de banda de 10 enlaces implementados a nivel nacional, para la obtención de los gráficos de monitoreo se utilizó la herramienta informática Cybergauge versión 6.0 de la empresa Neon software. Para la implementación de esta herramienta de monitoreo se requiere al dirección IP y comunidad SNMP del dispositivo que requerimos verificar el consumo de ancho de banda.

Con la información obtenida del monitoreo podremos determinar los máximos y mínimos de utilización de ancho de banda y de esa manera se dimensionara la infraestructura y recursos óptimos para el servicio entregado.

Enlace Principal (Wan Troncal)

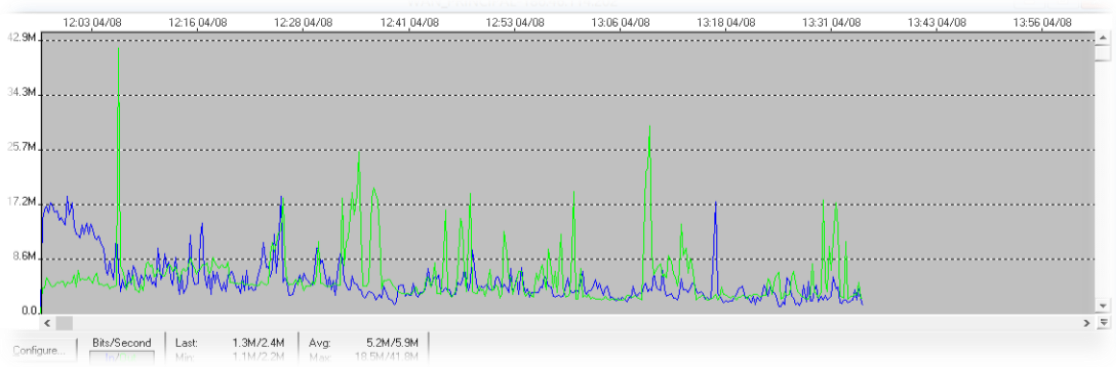


Ilustración 18 Enlace uno (Julio, 2016)

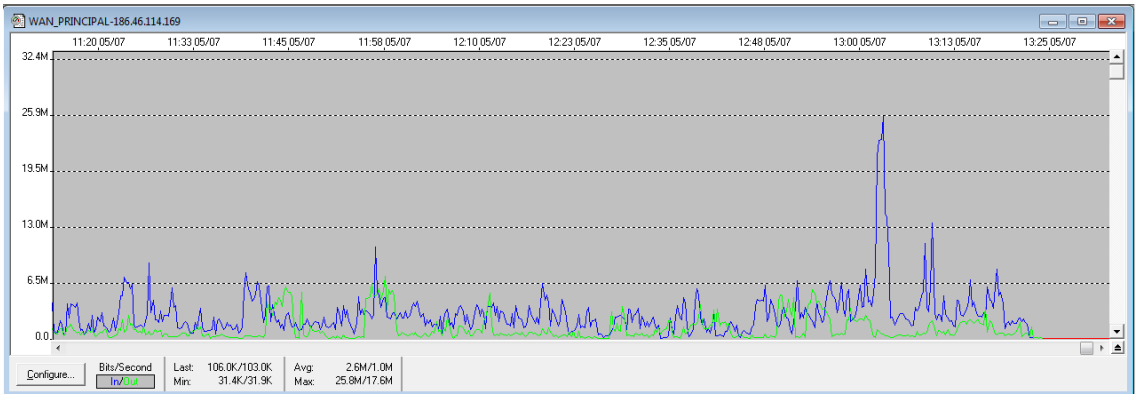


Ilustración 19 Enlace dos (Julio, 2016)

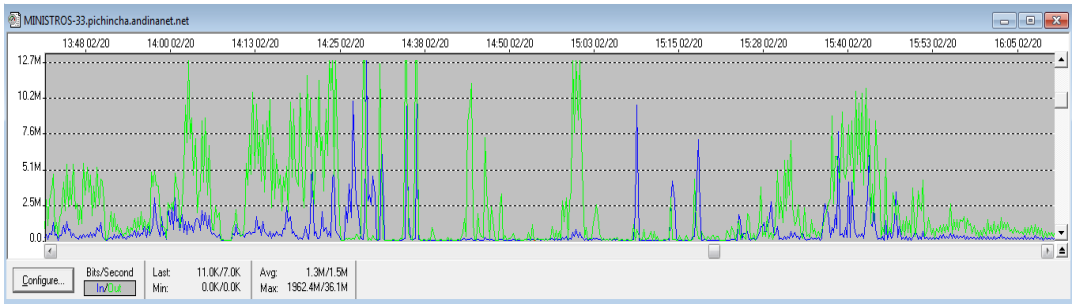


Ilustración 20 Enlace tres (Julio, 2016)

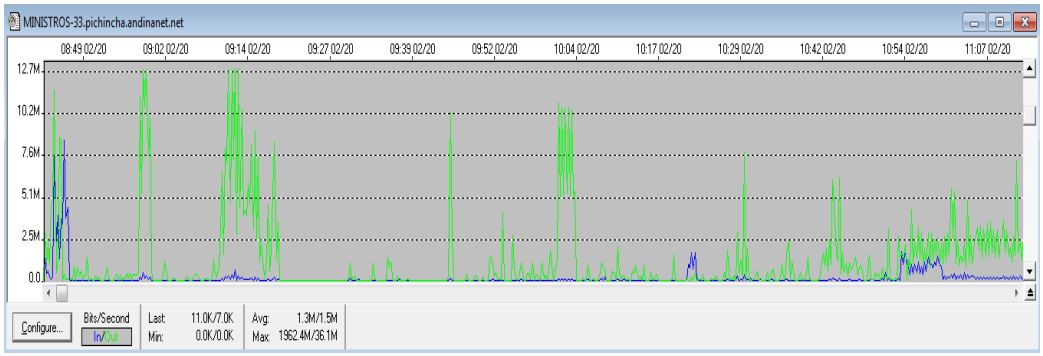


Ilustración 21 Enlace cuatro (Julio, 2016)

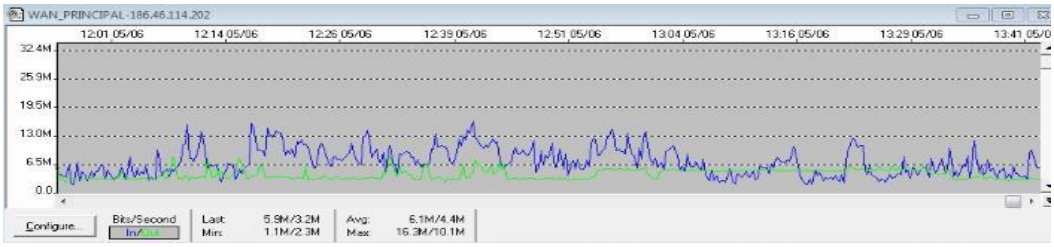


Ilustración 22 Enlace cinco (Julio, 2016)

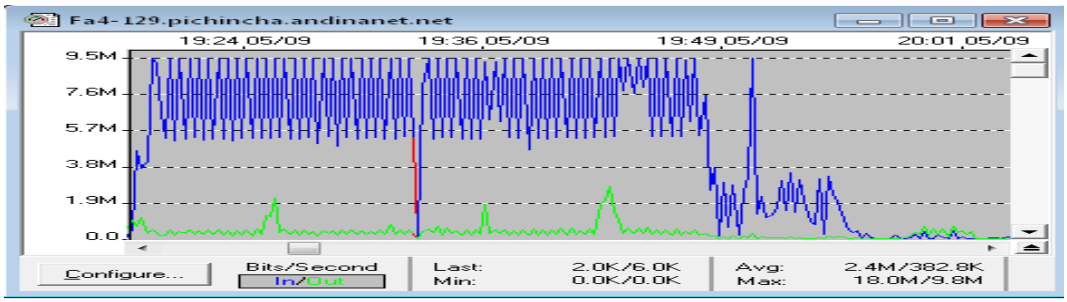


Ilustración 23 Enlace seis (Julio, 2016)

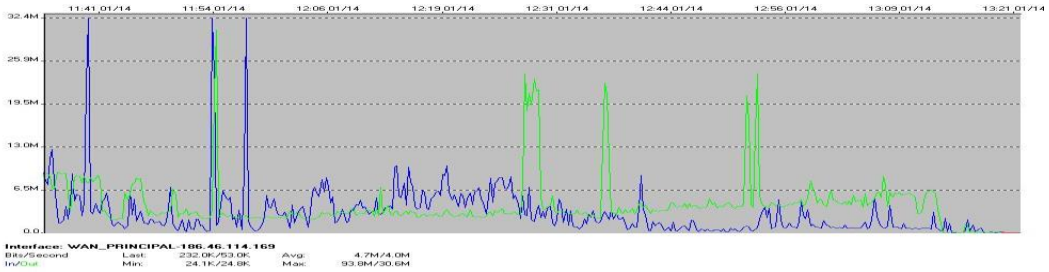


Ilustración 24 Enlace siete (Julio, 2016)

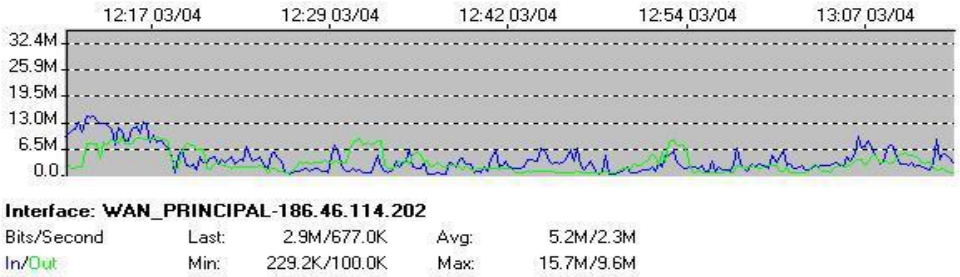


Ilustración 25 Enlace ocho (Julio, 2016)

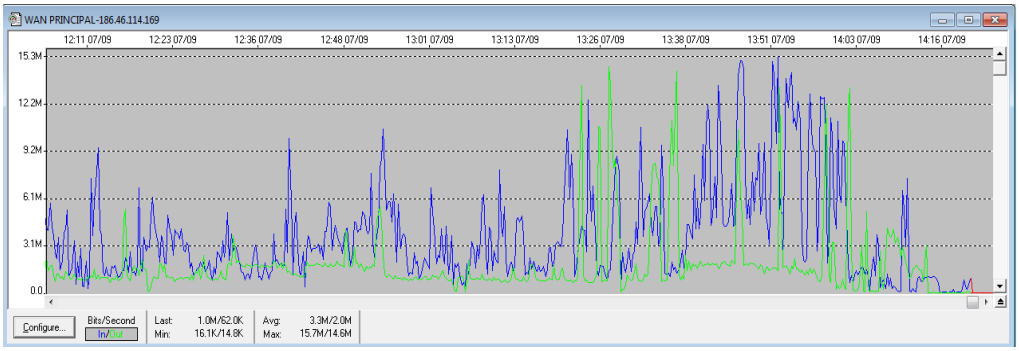


Ilustración 26 Enlace nueve (Julio, 2016)

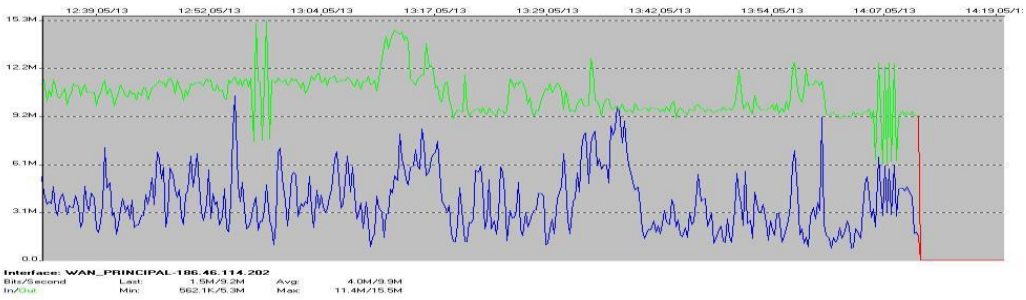


Ilustración 27 Enlace diez (Julio, 2016)

Enlace monitoreo cámaras

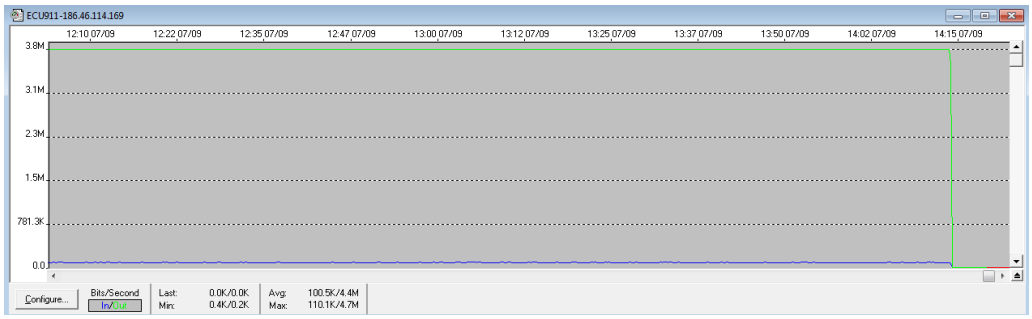


Ilustración 28 Enlace uno Cámaras (Julio, 2016)

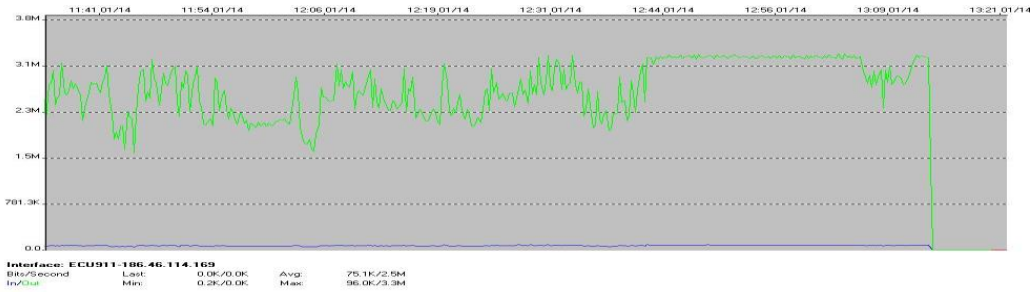


Ilustración 29 Enlace dos Cámaras (Julio, 2016)

Análisis máximo mínimo consumo ancho de banda enlace WAN principal.

ENLACE	CONSUMO WAN TRONCAL PRINCIPAL (Mbps)	
	PROMEDIO	MÁXIMO
UNO	5,9	41,8
DOS	5,2	15,7
TRES	1,3	36,1
CUATRO	2,6	25,8
CINCO	6,1	16,3
SEIS	4,7	30,6
SIETE	3,3	15,7
OCHO	2,4	18
NUEVE	4	15,5
DIEZ	1,5	36,1

Tabla 5 Consumo Ancho de Banda WAN Troncal (Julio, 2016)

Gráfico del consumo de ancho de banda

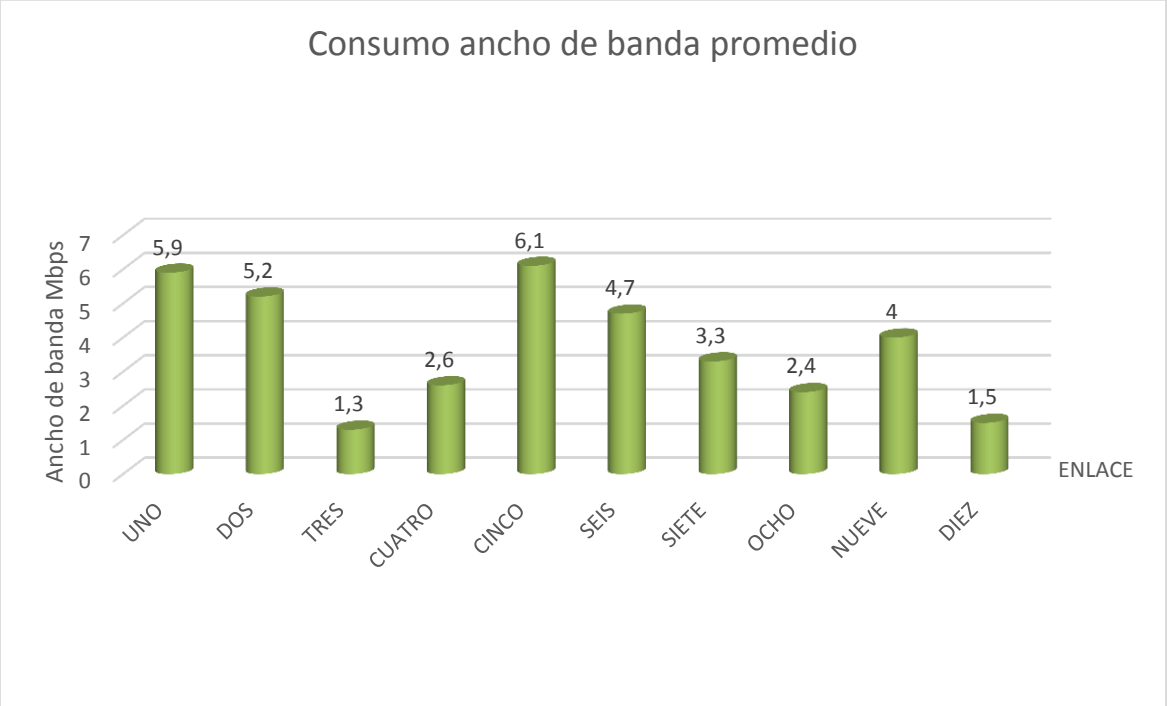


Ilustración 30 Consumo ancho de banda promedio (Julio, 2016)

Ilustración 31 Consumo ancho de banda máximo (Julio, 2016)

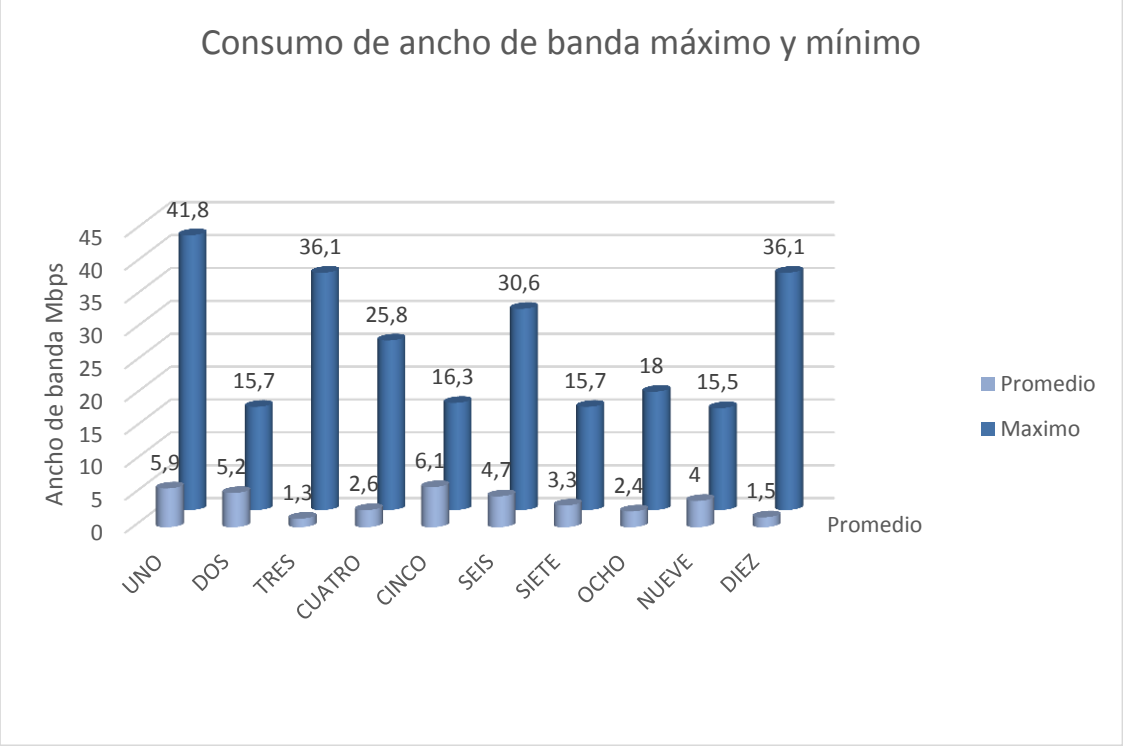


Ilustración 32 Consumo ancho de banda comparación (Julio, 2016)

Análisis máximo mínimo consumo ancho de banda enlace cámaras video vigilancia.

ENLACE	CONSUMO CÁMARAS DE VIDEO (Mbps)	
	PROMEDIO	MÁXIMO
UNO	4,4	4,7
DOS	2,5	3,3

Tabla 6 consumo cámaras de video (Julio, 2016)

Gráfico consumo del ancho de banda

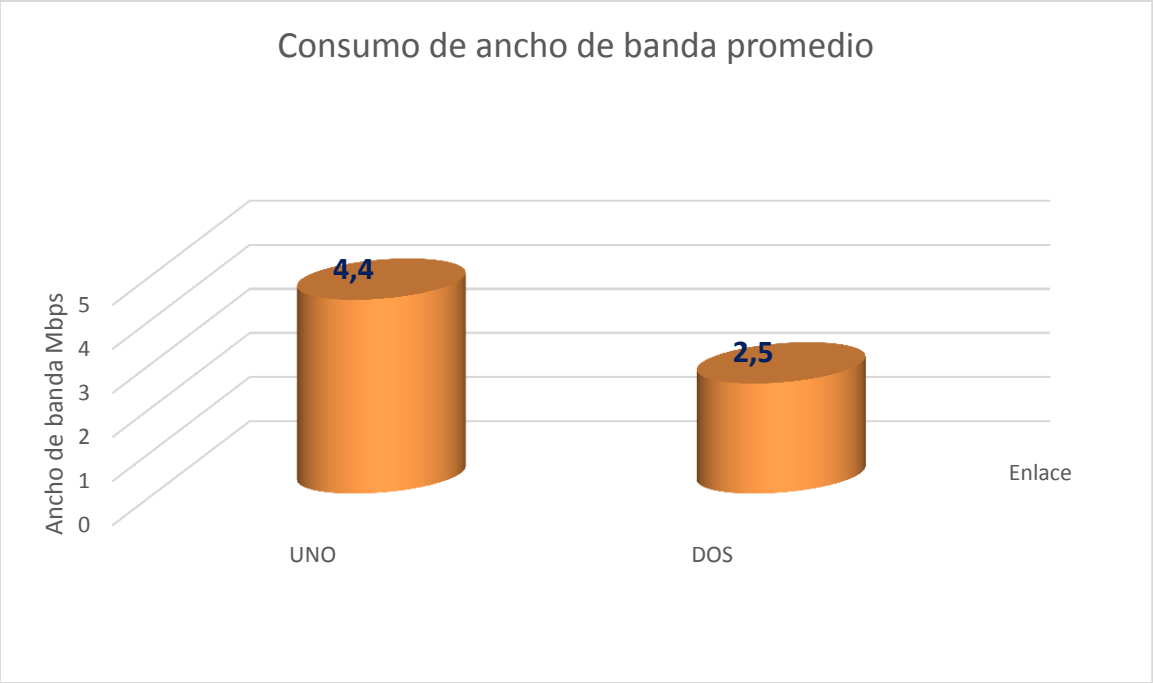


Ilustración 33 Consumo ancho de banda promedio cámaras de video vigilancia (Julio, 2016)

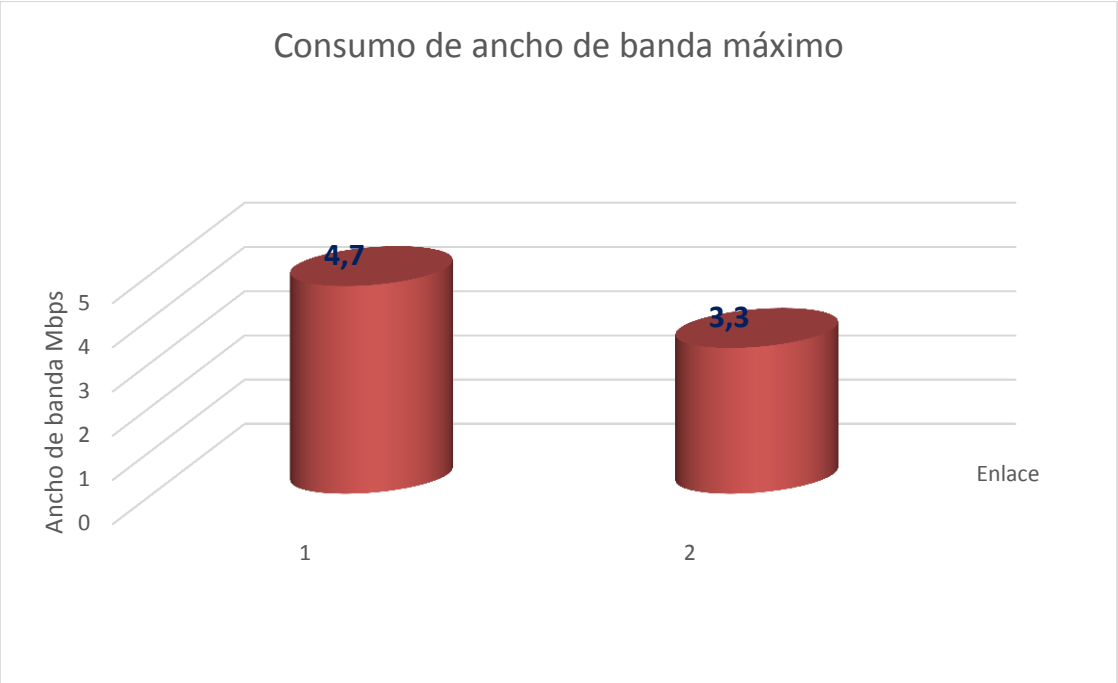


Ilustración 34 Consumo ancho de banda máximo cámaras de video vigilancia (Julio, 2016)

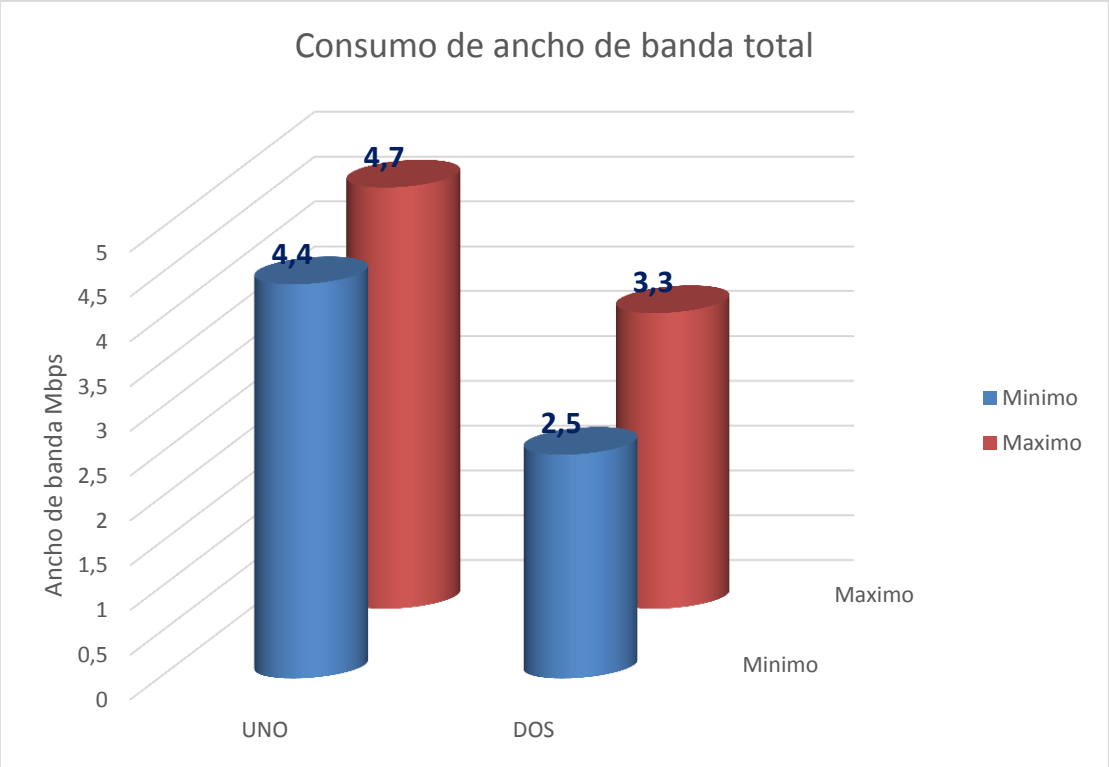


Ilustración 35 Comparación consumo ancho de banda cámaras de video vigilancia (Julio, 2016)

Análisis de requerimientos y dimensionamiento de recursos y personal.

Se requieren datos indispensables para el dimensionamiento de recursos, el dato más importante es saber en qué se va a utilizar el ancho de banda, el objetivo del enlace puede variar, y el personal y ancho banda asignados no siempre lo define el número de usuarios que van a utilizar el enlace, pueden existir enlaces en donde el usuario sea un solo equipo, podríamos considerar un streaming de audio o video, lo que hace que ese enlace tenga prioridad, o el usuario puede ser un ejecutivo o funcionario VIP, y la finalidad del enlace podría suponer una importancia de alto nivel, por ejemplo firma de convenios, reunión de alto nivel, en donde no puede fallar una video conferencia, o envío recepción de documentos, es decir estos enlaces van mucho más allá del normal acceso a navegación, revisión de correo, o utilización de redes sociales, estas redes son destinadas a eventos de gran relevancia. (S.A.S., 2014)

Procedimiento actual

Infraestructura última milla análisis actual y requerimientos mínimos

Para la provisión de enlaces de datos e internet en entornos temporales externos a la infraestructura corporativa o institucional, se requiere que el enlace disponga de un enlace principal mediante última milla de fibra óptica que permita atender la demanda de ancho de banda variable mínimo 5 Mbps máximo 50 Mbps y un enlace backup de última milla para la provisión del servicio de 4 Mbps por 2 Mbps que permita atender la red con restricciones mientras se habilita el enlace principal.

En lo que respecta al ancho de banda solicitado no siempre será posible atender el requerimiento del cliente, debido a que los sitios designados para los eventos no siempre disponen de infraestructura de telecomunicaciones de gran capacidad, es por esto que se puede garantizar 4 Mbps simétrico considerando como última opción de conectividad WAN última milla satélite utilizando dos o más antenas y modem satelitales.

Se debe considerar en las ubicaciones en que el acceso sea satelital a pesar que el ancho de banda entregado sea 4 Mbps, no podrán ser provistos todos los servicios debido a que el tiempo de respuesta en esta tecnología en promedio es 600ms lo que limita las posibilidades con aplicaciones voip y multimedia.

Es altamente deseable que en la propuesta de redundancia de enlaces principal y backup, se considere la conectividad desde diferentes nodos de acceso del ISP, ya que al conectar los enlaces principal y backup desde el mismo nodo de acceso se dispone únicamente de redundancia de última milla mas no redundancia de conectividad debido a que los dos enlaces en este caso comparten un mismo origen, susceptible a falla.

La elección del ISP para la provisión del servicio de datos o internet dependerá de las ventajas comerciales, técnicas y la garantía que incluya el servicio. La disponibilidad de una red IP / MPLS es indispensable, también la provisión de un servicio corporativo sin compartición es decir enlace 1:1 de igual manera la posibilidad de que los paquetes provenientes de la subred asignada se pueda marcar como prioritarios dentro de la red del ISP.

REQUERIMIENTOS ISP	ENLACE PRINCIPAL	ENLACE BACKUP
TIPO DE ENLACE	Enlace dedicado end-to-end, sin compartición	Enlace corporativo
ANCHO DE BANDA	simétrico regulable desde 5 hasta 50 Mbps	capacidad regulable desde 2 Mbps hasta 5 Mbps
ENLACES REDUNDANTES	SI	SI
TIPO DE REDUNDANCIA	redundancia de última milla y diferente nodo de conexión entre enlace principal y backup	redundancia de última milla y diferente nodo de conexión entre enlace principal y backup
ULTIMA MILLA	fibra óptica multimodo wdm	cobre ADSL
INFRAESTRUCTURA ISP	IP - MPLS indispensable	IP - MPLS indispensable
EQUIPAMIENTO	suministrado por el ISP	suministrado por el ISP
SLA (service level agreement)	disponibilidad 99.99 %	disponibilidad 99.99 %
SOPORTE TÉCNICO	En sitio personal certificado	En sitio personal certificado
CERTIFICACIONES	networking / cableado estructurado / ISO 27001 / seguridades de red	networking / cableado estructurado / ISO 27001 / seguridades de red

Tabla 7 Requerimientos ISP (Julio, 2016)

Capitulo 4

La propuesta

METODOLOGÍA ISO 27001 PARA OPTIMIZAR RENDIMIENTO DE REDES CORPORATIVAS MEDIANAS MÓVILES MANTENIENDO ESTÁNDARES DE DISPONIBILIDAD Y SEGURIDAD

A continuación el investigador planteara 2 aplicaciones prácticas para cualquiera de las soluciones planteadas, el requerimiento que debemos atender y garantizar es el detallado a continuación.

- Conexión compatible con cualquier dispositivo con acceso a Wi-Fi.
- No requiere configuración previa adicional a la contraseña de red.
- Red dirigida para directivos con acceso total a los recursos de red e invitados con acceso restringido y controlado a navegación web.
- Inmediata conexión.
- Ancho de banda variable en las subredes de acuerdo a los requerimientos del cliente.
- Seguridad de transmisión y recepción de datos garantizada.
- Prevención de virus y ataques en la red con altos estándares de eficiencia.

Tanto la aplicación práctica uno y la aplicación práctica dos, se basan en los mismos conceptos de conectividad, y seguridades corporativas, de igual manera la ingeniería lógica de las dos soluciones es similar, se ha seleccionado las marcas Cisco y Mikrotik, por tratarse de las marcas que disponen de un gran prestigio y confiabilidad entre los ISP, ya que son marcas con soluciones comprobadas que brindan un alto grado de garantía en su operación.

Otras marcas que provean de características similares, pueden perfectamente configurarse los servicios requeridos, se requiere siempre tomar en cuenta la experiencia del operador en la configuración de este equipamiento, es importante considerar que marcas más económicas podrían no brindar un servicio adecuado ni en su operación ni en su mantenimiento, por otra parte existen marcas que podrían considerarse especializadas en redes de altísimo desempeño

inalámbrico, por ejemplo Motorola, Juniper, HP, pero requieren personal capacitado en su operación y presupuestos mayores para su mantenimiento en el tiempo en comparación a las marcas propuestas.

Objetivos Específicos:

- Análisis de la solución actual
- Entrevista estructurada de gestión a administradores de red para definir situación actual y oportunidades de mejora
- Diseño de documento de lista de verificación de responsables de proceso y hardware asignado.
- Definir requerimientos del cliente y clasificación en requerimientos deseables y requerimientos que pueden ser atendidos.
- Diseño de red LAN, WLAN, WAN propuesta en base a las mejoras realizadas a la red actual y código de configuración de routers.
- Análisis y diseño de políticas de seguridad basados en ISO27001
- Dimensionamiento y asignación de equipos en base al requerimiento del cliente y en base a análisis costo beneficio de hardware
- Asignación de infraestructura lógica
- Análisis y diseño de políticas de gestión y monitoreo.
- Diseño de formato acta de entrega recepción el servicio de datos e internet.

Análisis de Factibilidad

La implementación sugerida representa una solución en los mismos términos presupuestarios utilizados al momento, sin embargo las actualizaciones en sus políticas de seguridad de la información y seguridad informática acompañados de la optimización de la configuración de sus protocolos de comunicaciones, aportan de manera considerable a la confidencialidad, integridad y disponibilidad.

Metodología.

Se procede de acuerdo a los lineamientos detallados en la ISO 27001, apoyándonos en algunas herramientas adicionales de la familia ISO 27000.

Análisis del riesgo

Para el análisis de riesgos se debe identificar los riesgos de los activos de la organización, determinar la magnitud del riesgo e identificar las áreas que requieren salvaguardas, con estos datos podemos determinar el impacto económico de un fallo de seguridad y la probabilidad de que ocurra un fallo sobre el activo analizado. Para el análisis de riesgos la norma ISO 27005: 2008 sugiere seguir el siguiente proceso. Los resultados del análisis de riesgo de la infraestructura implementada son un conjunto de procedimientos de evaluación y control que se detallan en las siguientes tablas. (ISO 27001, 2013)

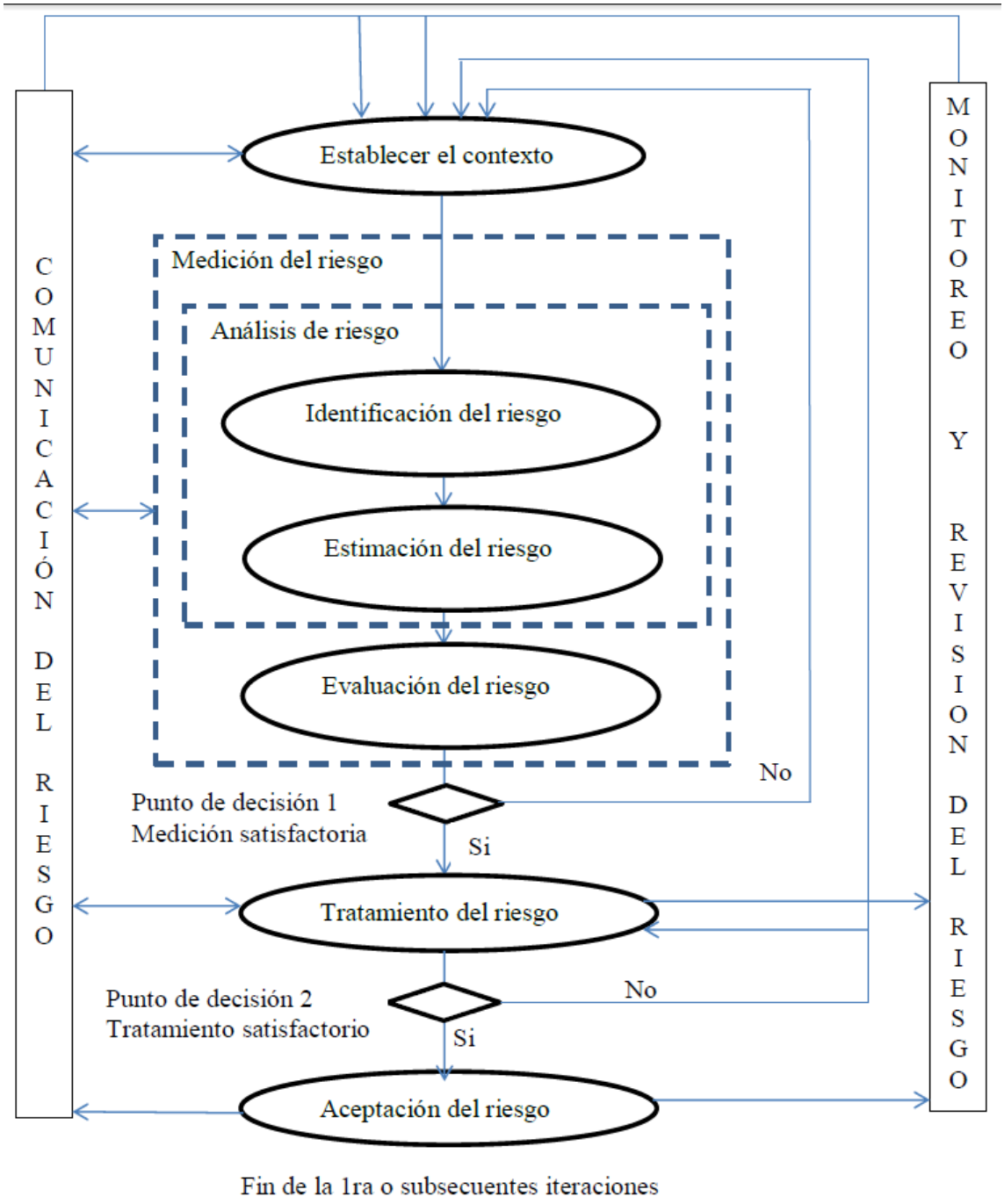


Ilustración 36 Proceso de administración de riesgos (Fuente: IEC/ITS 27005, 2008, pág. 5)

Inventario de activos

Para el inventario de activos utilizaremos la notación detallada a continuación, las dos letras mayúsculas al inicio de la identificación corresponde a la identificación del activo la notación esta detallada a continuación, los 3 números a continuación corresponden al número asignado al activo.

NOTACIÓN	SIGNIFICADO	DETALLE
DA	DATOS	activo de información
SA	SOFTWARE APLICACIÓN	software de gestión y aplicaciones
SE	SERVICIOS	servicios propios o de terceros
HA	HARDWARE OPCIÓN A	detalle de equipos informáticos y de telecomunicaciones primera propuesta
HB	HARDWARE OPCIÓN B	detalle de equipos informáticos y de telecomunicaciones primera propuesta
IF	INFRAESTRUCTURA	detalle de espacio físico e instalaciones
EA	EQUIPAMIENTO AUXILIAR	equipos e infraestructura de terceros directamente relacionada con el servicio
PS	PERSONAL DE SOPORTE	detalle del personal propio y de terceros relacionados con el servicio

Tabla 8 Notación inventario de activos (Julio, 2016)

En el inventario de activos se incluye código de barras que nos permitirá de manera automatizada y sencilla registrar los equipos en cada instalación, de igual manera permite mantener un control de los activos de la empresa. (ISO 27001, 2013) (Ing. Mayorga, 2014)

Inventario de activos

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación Física	Código de barras
DA001	DATOS	Registro de conexiones	archivo de Excel	Jefatura STCN2		DA001
DA002		registro de monitoreo de ancho de banda	archivo de Excel	Jefatura STCN2		DA002
DA003		información histórica de monitoreo	archivo de Excel	Jefatura STCN2		DA003
DA004		registro de novedades y observaciones	archivo de Excel	Jefatura STCN2		DA004
DA005		actas de entrega recepción de servicios	documento	Jefatura STCN2		DA005
SA001	APLICACIÓN	monitoreo de ancho de banda	software Cibergauge	Jefatura STCN2		SA001
SA002		gestión de router / switch	software ssh (putty, Secure SRT)	Jefatura STCN2		SA002
SA003		gestión de Access Point	software ssh (putty, Secure SRT) o/y http	Jefatura STCN2		SA003
SA004		software de análisis de redes inalámbricas	wifi analizer	Jefatura STCN2		
SA005		ftp archivos LAN	ftp server LAN	Jefatura STCN2		SA005
SE001	SERVICIOS	impresión LAN y WLAN	conexión de impresoras en red LAN diferentes subredes	Jefatura STCN2		SE001
SE002		acceso WLAN	SSID y password para conexión a WLAN diferentes subredes	Jefatura STCN2		SE002
SE003		acceso LAN (control)	instalación de cableado estructurado equipos AAA	Jefatura STCN2		SE003
SE004		firewall	firewall políticas de navegación y privilegios	Jefatura STCN2		SE004
SE005		ancho de banda dinámico	cambio de ancho de banda remoto bajo demanda	Jefatura STCN2		SE005

Tabla 9 Inventario de activos (Julio, 2016) (Ing. Mayorga, 2014)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación Física	Código de barras
HA001	HARDWARE OPCION 1	ROUTER	ROUTER CISCO 1900 K9	ORGANIZACIÓN		HA001
HA002		SWITCH	SWITCH CISCO 24 PORT POE	ORGANIZACIÓN		HA002
HA003		CONVERSOR OPTICO ELECTRICO	CONVERSOR OPTICO ELECTRICO CNET 10/100/1000	ORGANIZACIÓN		HA003
HA004		MODEM ADSL	MODEM ADSL HUAWEI	ORGANIZACIÓN		HA004
HA005		ACCESS POINT CISCO 1	ACCESS POINT CISCO AIRONET 10/100	ORGANIZACIÓN		HA005
HA006		ACCESS POINT CISCO 2	ACCESS POINT CISCO AIRONET 10/100	ORGANIZACIÓN		HA006
HA007		PATCH CORE FIBRA OPTICA 1	PATCH CORE FIBRA OPTICA 1	ORGANIZACIÓN		HA007
HA008		PATCH CORE UTP	PATCH CORE UTP CAT 5e 1,50 m CANT: 10	ORGANIZACIÓN		HA008
HA009		PATCH CORE UTP	PATCH CORE UTP CAT 5e 15 m CANT: 10	ORGANIZACIÓN		HA009
HA010		MULTITOMA ELECTRICA	MULTITOMA ELECTRICA CON SUPRESOR DE PICOS	ORGANIZACIÓN		HA010
HA011		ODF ISP	ODF 2 HILOS FIBRA OPTICA	ISP		HA011
HA012		CASE RACK	RACK CON CUBIERTA 8 UNIDADES 19"	ORGANIZACIÓN		HA012
HB001	HARDWARE OPCION 2	ROUTER	ROUTER MIKROTIK RB950	ORGANIZACIÓN		HB001
HB002		SWITCH	SWITCH CISCO 24 PORT POE	ORGANIZACIÓN		HB002
HB003		CONVERSOR OPTICO ELECTRICO	CONVERSOR OPTICO ELECTRICO CNET 10/100/1000	ORGANIZACIÓN		HB003
HB004		MODEM ADSL	MODEM ADSL HUAWEI	ORGANIZACIÓN		HB004

Tabla 10 Inventario de activos (Julio, 2016) (Ing. Mayorga, 2014)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación Física	Código de barras
HB005	HARDWARE OPCION 2	WLC	WIRELLESS LAN CONTROLLER RUCKUS 10/100/1000	ORGANIZACIÓN		HB005
HB006		ACCESS POINT 1	ACCESS POINT RUCKUS 10/100/1000	ORGANIZACIÓN		HB006
HB007		ACCESS POINT 2	ACCESS POINT RUCKUS 10/100/1000	ORGANIZACIÓN		HB007
HB008		PATCH CORE FIBRA OPTICA 1	PATCH CORE F O 1	ORGANIZACIÓN		HB008
HB009		PATCH CORE UTP	PATCH CORE UTP CAT 5e 1,50 m CANT: 10	ORGANIZACIÓN		HB009
HB010		MULTITOMA ELECTRICA	TOMA ELECTRICA CON SUPRESOR DE PICOS	ORGANIZACIÓN		HB010
HB011		ODF ISP	ODF 2 HILOS F O	ISP		HB011
HB012		CASE RACK	RACK CON CUBIERTA 8 UNIDADES 19"	ORGANIZACIÓN		HB012
IF001	INSTALACIONES	CARPA O ESPACIO CUBIERTO	ESPACIO MIIMO 2 METROS CUADRADOS	EXTERNO		IF001
IF002		EQUIPOS INFORMATICOS	REQUISITOS MINIMOS CLIENTE	EXTERNO		IF002
IF003		MESA DE EQUIPOS TELECOMUNICACIONES	MESA AREA MINIMA 1 x 1.50 METROS	EXTERNO		IF003
IF004		ESPACIO DE MONITOREO Y GESTION	MESA AREA MINIMA 1 x 1.50 METROS	EXTERNO		IF004
IF005		ESPACIO PARA EQUIPOS Y ACCESORIOS	MINIMO 1 METRO CUADRADO	EXTERNO		IF005

Tabla 11 Inventario de activos (Julio, 2016) (Ing. Mayorga, 2014)

Identificación	Tipo	Activo	Descripción	Propietario	Ubicación Física	Código de barras
EA001	EQUIPAMIENTO AUXILIAR	ROUTER PROVEEDOR ISP	CERTIFICADO RED MPLS	EXTERNO		EA001
EA002		ULTIMA MILLA ENLACE PRINCIPAL	FIBRA OPTICA	EXTERNO		EA002
EA003		ULTIMA MILLA ENLACE BACKUP	MEDIO DISPONIBLE CERTIFICADO 2 MBPS MINIMO	EXTERNO		EA003
EA004		TOMA ELECTRICA EDIFICIO	ASEGURADA A TIERRA Y CON RESPALDO ELECTRICO	EXTERNO		EA004
PS001	PERSONAL SOPORTE	SOPORTE CORPORATIVO EN SITIO	PROFESIONAL CERTIFICADO	ORGANIZACIÓN		PS001
PS002		SOPORTE CORPORATIVO NIVEL 2 REMOTO	PROFESIONAL CERTIFICADO	ORGANIZACIÓN		PS002
PS003		PERSONAL DE SOPORTE ULTIMA MILLA	TECNICO CERTIFICADO	ORGANIZACIÓN		PS003
PS004		PERSONAL SUBCONTRATADO	MINIMO TECNICO	EXTERNO		PS004
TE001	TECNOLOGÍA	COMPUTADOR	OPTIMAS CONDICIONES	ORGANIZACIÓN		TE001
TE002		CABLEADO ESTRUCTRUCTURADO	CUMPLA ESTANDARES MINIMOS	ORGANIZACIÓN		TE002
TE003		CABLE DE CONSOLA	INDISPENSABLE	ORGANIZACIÓN		TE003
TE004		CABLE USB - SERIAL	INDISPENSABLE	ORGANIZACIÓN		TE004

Tabla 12 Inventario de activos (Julio, 2016) (Ing. Mayorga, 2014)

Identificación de los activos

Identificación de activos en relación con la lista con procesos.

Activos Principales

Procesos de servicio

- Provisión de servicio de conexión de Datos e Internet
- Protección de acceso y trasmisión de información en el medio provisto

Información

- Configuración de equipos
- Registro de conexiones
- Históricos de monitoreo
- Registro de novedades
- Documentos de soporte
- Actas de entrega y recepción de servicios

Activos de apoyo

Hardware

- Equipo de procesamiento de datos
- Procesamiento de periféricos
- Medios para datos
- Medios electrónicos
- Otros medios

Software

- Sistema de Gestión de configuración de equipos
- Microsoft Office
- Sistema Operativo
- Windows 7
- OS dispositivos móviles smart OS / Android

Redes

- Soporte y medios
- ISP
- Ethernet
- Wireless
- Dispositivos de comunicaciones
- Router
- Switch

Interfaz de comunicaciones

- WLAN
- LAN
- WAN

Personal

- Soporte técnico especializado presencial
- Soporte técnico especializado remoto
- Soporte técnico básico y de última milla en sitio
- Personal subcontratado de servicios de terceros

Sitio

- Exteriores fuera de la infraestructura institucional

Valuación de activos

El siguiente paso luego de la identificación de activos es establecer la escala de valuación para cada activo, hay activos que pueden evaluarse por su valor monetario pero otros como la información, o las personas no tienen una representación económica, por lo que se elige la siguiente escala:

Escala de valuación: Bajo, Medio, Alto (Ing. Mayorga, 2014) (ISO 27001, 2013)

Tipo	Activo	Criterio de valuación	Valuación	Valuación del activo
Procesos de servicio	Provisión de servicio de conexión de Datos e Internet	enlace sin seguridad	alto	alto
		interrupción de servicio	alto	
		daño de la reputación	alto	
Procesos de servicio	Protección de acceso y trasmisión de información en el medio provisto	políticas de seguridad	alto	alto
		interrupción de servicio	alto	
		perdida de información	alto	
Información	Configuración de equipos telecomunicaciones	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Información	Registro de Conexiones	pérdida de información		alto
Información	históricos de monitoreo	perdida de información		alto

Tabla 13 Valuación de activos (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de valuación		Valuación
Información	registro de novedades	perdida de información		alto
Información	documentos de soporte	perdida de información		alto
Información	actas de entrega y recepción de servicios	perdida de información		alto
Hardware	Router	interrupción del servicio	alto	alto
		políticas de seguridad	alto	
		pérdida económica	bajo	
Hardware	switch	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	conversor óptico eléctrico (Enlace Principal)	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	modem Adsl (Enlace backup)	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	Access Point 1	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	

Tabla 14 Valuación de activos (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de valuación		Valuación
Hardware	Access Point 2	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	patch core fibra óptica	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	patch core utp	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	multitoma energía eléctrica UPS	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	ODF del ISP	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	case rack	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	
Hardware	Wireless LAN Controller	adecuado nivel técnico	alto	alto
		políticas de seguridad	medio	
		documentación	medio	

Tabla 15 Valuación de activos (Julio, 2016) (Ing. Mayorga, 2014)

Valoración del Impacto

La valoración del impacto se basa en la siguiente escala: Directo o Indirecto

Tipo	Activo	Criterio de valuación	Valuación del activo	Valoración del Impacto
Proceso de la organización	servicio de datos e internet	seguridad de acceso	alto	directo
		interrupción del servicio	alto	directo
		daño de la reputación	alto	directo

Tabla 16 Valoración del impacto (Julio, 2016)

Valoración del impacto de activos de apoyo

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Información soporte	Configuración de equipos telecomunicaciones	Perdida de la reputación	bajo	directo
		falta del activo	alto	directo
		el valor del reemplazo final de la pérdida del activo	medio	directo
Información soporte	Registro de Conexiones	Perdida de la reputación	bajo	indirecto
		falta del activo	bajo	indirecto

Tabla 17 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Información soporte	históricos de monitoreo	Perdida de la reputación	bajo	indirecto
		falta del activo	bajo	indirecto
Información soporte	registro de novedades	Perdida de la reputación	bajo	indirecto
		falta del activo	bajo	indirecto
Información soporte	documentos de soporte	Perdida de la reputación	bajo	indirecto
		falta del activo	bajo	indirecto
Información soporte	actas de entrega y recepción de servicios	Perdida de la reputación	bajo	indirecto
		falta del activo	bajo	indirecto
Redes	Router	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo

Tabla 18 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Redes	switch	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Redes	conversor óptico eléctrico (Enlace Principal)	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Redes	modem Adsl (Enlace backup)	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo

Tabla 19 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Redes	Access Point 1	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Redes	Access Point 2	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Redes	patch core fibra óptica	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo

Tabla 20 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Redes	patch core utp	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Hardware	multitoma energía eléctrica UPS	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Redes	ODF del ISP	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo

Tabla 21 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Hardware	case rack	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor reemplazo final la pérdida del activo	bajo	directo
Redes	Wireless LAN Controller	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		valor del reemplazo final de la pérdida del activo	bajo	directo
Personal	SOPORTE CORPORATIVO ESPECIALIZADO EN SITIO	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		imposibilidad de concretar obligaciones	bajo	directo
Personal	SOPORTE CORPORATIVO ESPECIALIZADO REMOTO	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		imposibilidad de concretar obligaciones	medio	directo

Tabla 22 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Tipo	Activo	Criterio de Consecuencias	Valuación final	Valoración del impacto
Personal	SOPORTE CORPORATIVO ULTIMA MILLA	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		imposibilidad de concretar obligaciones	medio	directo
Personal	SOPORTE PERSONAL SUBCONTRATADO	Perdida de la reputación	alto	directo
		interrupción del servicio	alto	directo
		imposibilidad concretar	alto	directo

Tabla 23 Valoración del impacto (Julio, 2016) (Ing. Mayorga, 2014)

Identificación de amenazas

El origen de la amenaza está basado en la siguiente tabla.

A	Accidental
B	Usada por todos las acciones deliberadas dirigidas a los activos
C	(Del medio ambiente) es relevante

Tabla 24 Nomenclatura identificación amenazas (Julio, 2016)

TIPO	AMENAZA	ORIGEN
DAÑO FÍSICO	Fuego	A,D,E
	Accidente grave	A,D,E
	Destrucción de equipos o medios	A,D,E
	Polvo, corrosión, congelación	A,D,E
EVENTOS NATURALES	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundaciones	E
PERDIDA DE SERVICIOS ESENCIALES	Peligro del aire acondicionado o sistema de abastecimiento de agua	A,D
	Pérdida de energía eléctrica	A,D,E
	Falla equipos de telecomunicaciones	A,D
	Robo de los medios de comunicación o documentos	D
	Robo de equipos	D
	Recuperación de medios de comunicación reciclados	A,D
	Divulgación	A,D
	Datos de fuentes no confiables	D
	La manipulación del hardware	D
	La manipulación del software	A,D
FALLAS TÉCNICAS	Daño en el equipo	A
	Malfuncionamiento del equipo	A
	Saturación del sistema de información	A,D
	Malfuncionamiento del software	A
	Incumplimiento del mantenimiento del sistema de información	A,D

Tabla 25 Identificación de amenazas (Julio, 2016)

TIPO	AMENAZA	ORIGEN
ACCIONES NO AUTORIZADAS	Uso de equipo no autorizado	D
	Copia de software fraudulento	D
	Uso de falsificación o software copiado	A,D
FUNCIONES COMPROMETEDORAS	Errores en el uso	A
	Incumplimiento disponibilidad del personal	A,D,E
	Abuso de derechos	A,D,E

Tabla 26 Identificación de amenazas (Julio, 2016)

Identificación de amenazas origen humano

Origen de la amenaza	Motivación	Posibles consecuencias
Criminal Informático	Destrucción de la información	Crimen informático (acoso por intimidación, acoso para gratificación sexual, envío de fotos, videos, sonidos sin consentimiento, sexting,)
	Divulgación de información ilegal	Actos fraudulentos (reproducir, suplantación, interceptación)
	Ganancia de dinero	Soborno de información
	Alteración de datos no autorizados	Suplantación de identidad Intrusión
empleados (mal entrenados, descontentos, maliciosos, negligentes, deshonestos, o empleados que sean despedidos)	Curiosidad Ego Inteligencia Ganancia de dinero Venganza Errores no intencionales y omisiones (ejemplo errores al ingresar datos, errores de programación)	Asalto a un empleado, Correo negro, Navegación de la información confidencial, Abuso del computador, Fraude y robo Soborno de información, Entrada de falsificados, datos corruptos, Intercepción, Código malicioso (Ejemplo virus, bomba lógica, Troyanos La venta de información personal, Errores del sistema, Intrusión. Sabotaje, Acceso al sistema sin autorización,

Tabla 27 Identificación amenazas origen humano (Julio, 2016)

Identificación de controles existentes

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		ESTADO DE CONTROL			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENCIENTE	INJUSTIFICADO
Daño Físico	Fuego	A,D,E		extintores	X			
	inundación	A,D,E			X			
	vandalismo	A,D,E		guardia			X	

Tabla 28 Identificación de controles existentes (Julio, 2016) (Ing. Mayorga, 2014)

Identificación de Controles

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		ESTADO DE CONTROL			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENTE	INJUSTIFICADO
Daño Físico	Fuego	A,D,E		extintores	X			
	inundación	A,D,E			X			
	vandalismo	A,D,E		guardia			X	
	polvo, corrosión	A,D,E		mantenimiento anual			X	

Tabla 29 Identificación de controles (Julio, 2016)

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		TIPO			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENTE	INJUSTIFICADO
Eventos naturales	Fenómenos climáticos	E					X	
	Fenómenos sísmicos	E					X	
	Fenómenos volcánicos	E					X	
	Fenómenos meteorológicos	E					X	
	Inundaciones	E					X	

Tabla 30 Identificación de controles (Julio, 2016)

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		TIPO			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENTE	INJUSTIFICADO
PERDIDA DE SERVICIOS ESENCIALES	Aire acondicionado o sistema de abastecimiento agua	A,D					X	
	Pérdida de energía eléctrica	A,D, E		UPS			X	
	Falla en los equipos de telecomunicaciones	A,D		OPCIÓN A Y OPCIÓN B	X			
	Robo de los medios de comunicación o documentos	D					X	
	Robo de equipos	D		GUARDIA		X		
	Recuperación medio comunicación	A,D			X			
	Divulgación	A,D			X			
	Datos de fuentes no confiables	D			X			
	La manipulación del hardware	D		ACCESO EXCLUSIVO PERSONAL SOPORTE	X			
	La manipulación del software	A,D		ACCESO EXCLUSIVO PERSONAL SOPORTE	X			

Tabla 31 Identificación de controles (Julio, 2016)

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		TIPO			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENTE	INJUSTIFICADO
FALLAS TÉCNICAS	Daño en el equipo	A		EQUIPOS RESPALDO OPCIÓN B	X			
	Malfuncionamiento del equipo	A		EQUIPOS RESPALDO OPCIÓN B	X			
	Saturación del sistema de información	A,D		EQUIPOS RESPALDO OPCIÓN B	X			
	Malfuncionamiento del software	A		EQUIPOS RESPALDO OPCIÓN B	X			
	Incumplimiento del mantenimiento del sistema de información	A,D			X			
ACCIONES NO AUTORIZADAS	Uso de equipo no autorizado	D		RESTRINGIDO	X			
	Copia de software fraudulento	D					X	
	Uso de falsificación o software copiado	A,D					X	

Tabla 32 Identificación de controles (Julio, 2016)

TIPO	AMENAZA	ORIGEN	CONTROL					
			TIPO		TIPO			
			PLANEADO	EXISTENTE	SE JUSTIFICA	INEFICIENTE	NO SUFICIENTE	INJUSTIFICADO
FUNCIONES COMPROMETEDORAS	Errores en el uso	A					X	
	Incumplimiento de la disponibilidad del personal	A,D, E					X	
	Abuso de derechos	A,D, E					X	

Tabla 33 Identificación de controles (Julio, 2016)

Identificación de vulnerabilidades

Tipos	Vulnerabilidades	Amenazas
Hardware	insuficiente mantenimiento	falta de cumplimiento del cronograma de mantenimiento de equipos
	Susceptibilidad a la humedad, polvo, suciedad	daño de componentes electrónicos
	falta de parámetros de configuración de seguridad	personal no capacitado
	OS desactualizado	falta de upgrade sistema operativo equipos
Software	fechas incorrectas en los equipos	error de configuración de equipos
	mala gestión de contraseñas	claves con parámetros débiles presentan problemas de seguridad
	Defectos en el software	Uso indebido de software pirata
Red	Arquitectura de red insegura	falta de parámetros de seguridad
	daño en interfaz de red equipos	intermitencia en el servicio por daño físico de conectores
	cableado Ethernet deficiente	cables de red sin certificación
	problemas de acceso a equipos	dispositivos de red instalados inadecuadamente dificultan el soporte a los mismos e incrementan el tiempo de solución de problemas
	interferencia en la red inalámbrica	WLAN sin análisis previo o gestión deficiente

Tabla 34 Identificación de vulnerabilidades (Julio, 2016)

Tipos	Vulnerabilidades	Amenazas
Personal	ausencia de personal	incumplimiento del personal asignado
	procedimientos de gestión inadecuados	personal poco capacitado en el proceso
	tiempos altos de solución de problemas	personal con poca experticia técnica
	falta de conocimiento de procedimientos de seguridad	personal poco capacitado en el proceso
	Falta de mecanismos de monitoreo	personal poco capacitado en el proceso
Ubicación	localización en un área susceptible a fenómenos naturales intensos, lluvia excesiva, humedad excesiva, calor, demasiado polvo etc.	daño o malfuncionamiento de equipos electrónicos
	deficiente instalación eléctrica	instalaciones sin conexión a tierra, voltaje inadecuado, posibilidad de corto circuito
	poca seguridad de los bienes instalados	sitios sin la adecuada infraestructura para prevenir hurto de equipos
Organización	falta de control de entrega de claves de acceso wifi	difusión inadecuada de la contraseña de acceso a la red wifi
	falta de control de acceso a la rack de equipos	no se dispone de zona exclusiva de equipos en datacenter
	falta de registros de eventos por parte del responsable del servicio en sitio	error en los procedimientos
	falta de procedimientos posteriores a la detección de intrusos	usuarios no autorizados utilizando los recursos de la red
	falta de control para dispositivos que generan trafico inadecuado en la red	equipos con virus o uso inadecuado de los recursos de la red

Tabla 35 Identificación de vulnerabilidades (Julio, 2016)

Identificación de consecuencias

Las consecuencias son analizadas en términos de pérdida de confidencialidad, integridad y disponibilidad.

"**Disponibilidad** es la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9).

"**Confidencialidad** es la propiedad que esta información esté disponible y no sea divulgada a personas, entidades o procesos no – autorizados. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 9).

"**Integridad** es la propiedad de salvaguardar la exactitud e integridad de los activos. (ISO/IEC, 13335-1:2004)" (ISO/ICE, ITC, 2005, pág. 10).

A continuación se presenta una tabla con la identificación de consecuencias.

Identificación de consecuencias

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
Provisión de servicio de acceso Internet y Datos	Un caso grave de afectación al servicio que limite el acceso del cliente a la red LAN, WLAN o WAN seria critico ya que estaríamos imposibilitados de prestar el servicio para el cual fuimos contratados	X	X	X		X	X	X	

Tabla 36 Identificación de consecuencias (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
Computadoras	errores en el funcionamiento causaría afectación grave debido a que es la manera de interactuar el sistema	X	X	X		X	X		
Firewall	errores en el funcionamiento causaría afectación grave debido a que es la manera de proteger infraestructura lógica provisión del servicio	X	X	X	X	X	X	X	

Tabla 37 Identificación de consecuencias (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
Software son licencia (pirata)	Utilizar software pirata permite la intrusión de virus en el dispositivo lo que expone la seguridad y disponibilidad de la red informática	X	X	X	X	X	X	X	
control de contenido	evitar el acceso a páginas pornográficas y redes sociales, bloquear descarga de archivos multimedia	X	X		X		X	X	

Tabla 38 Identificación de consecuencias (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
Ethernet y Wireless 802.11 a/b/c/n/g	fallas en el funcionamiento ocasiona desconexión de los dispositivos a la red informática	X	X	X		X		X	
equipos de telecomunicaciones	fallas en los equipos causarían interrupción del servicio de datos o Internet significa afectación grave a la operación	X	X	X		X	X	X	

Tabla 39 Identificación de consecuencias (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
solicitudes del cliente sin tomar en cuenta sugerencias de seguridad informática	impacto directo debido a que las disposiciones del cliente comprometen el desempeño de la red				X	X	X		X

Tabla 40 Identificación de consecuencias (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIAS OPERACIONALES						NATURALEZA	
		TIEMPO DE REPARACIÓN	PERDIDA DE TIEMPO	PERDIDA DE OPORTUNIDADES	SALUD Y SEGURIDAD	COSTO FINANCIERO DE HABILIDADES ESPECIFICAS PARA REPARAR EL DAÑO O REEMPLAZO	IMAGEN REPUTACIÓN	TEMPORAL	PERMANENTE
energía eléctrica	Interrupción servicio de electricidad adicional al corte de servicio de telecomunicaciones ocasionado por apagado de los equipos de telecomunicaciones, puede ocasionar daño en la información de los clientes o afectación grabe al disco duro de los dispositivos.	X		X		X	X	X	

Tabla 41 Identificación de consecuencias (Julio, 2016)

Estimación del riesgo

Valoración de consecuencias

La valoración de consecuencias de un incumplimiento de seguridad de información se realiza en base a pérdida de confidencialidad, integridad o disponibilidad de los activos, para lo cual se ha establecido una escala del 0 al 3 como se puede observar en la siguiente tabla. (ISO 27001, 2013) (Ing. Mayorga, 2014)

Confidencialidad	Integridad	Disponibilidad
0 nada grave	0 nada grave	0 nada grave
1 poco grave	1 poco grave	1 poco grave
2 grave	2 grave	2 grave
3 muy grave	3 muy grave	3 muy grave

Tabla 42 Nomenclatura estimación del riesgo (Julio, 2016) (Ing. Mayorga, 2014)

Valoración de consecuencias

Mediante el análisis de los posibles casos de incidencias de afectación a la red podemos definir un criterio de impacto en nuestra infraestructura.

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIA OPERACIONAL	Criterio de Impacto			
			Valoración de reemplazo del activo	Consecuencias para la organización por la pérdida o compromiso de los activos		
Provisión de servicio de acceso Internet y Datos	Un caso grave de afectación al servicio que limite el acceso del cliente a la red LAN, WLAN o WAN seria critico ya que estaríamos imposibilitados de prestar el servicio para el cual fuimos contratados	imposibilidad de acceso a la red limita las actividades de la organización el tiempo de restablecimiento del servicio debe ser mínimo de acuerdo al plan de contingencia	no se tiene reemplazo	CONFIDENCIAL 3	INTEGRIDAD 3	DISPONIBILIDAD 3
Computadoras	errores en el funcionamiento causaría afectación grave debido a que es la manera de interactuar con el sistema	tiempo de soporte en sitio representan costos y no hay garantía que se pueda solucionar de forma inmediata	no se tiene reemplazo inmediato	CONFIDENCIAL 2	INTEGRIDAD 2	DISPONIBILIDAD 3

Tabla 43 Estimación del riesgo (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIA OPERACIONAL	Criterio de Impacto			
			Valoración de reemplazo del activo	Consecuencias para la organización por la pérdida o compromiso de los activos		
Firewall	error causaría afectación grave falla al de proteger infraestructura lógica y la provisión servicio	tiempo de soporte en sitio representan costos y no hay garantía que se pueda solucionar de forma inmediata	no se tiene reemplazo inmediato	CONFIDENCIAL 3	INTEGRIDAD 3	DISPONIBILIDAD 3
Software son licencia (pirata)	Utilizar software pirata permite la intrusión de virus en el dispositivo lo que expone la seguridad y disponibilidad de la red informática	afectación directa a la imagen, reputación y seguridad de la organización	no se tiene reemplazo inmediato	CONFIDENCIAL 3	INTEGRIDAD 3	DISPONIBILIDAD 3
control de contenido	evitar el acceso a páginas pornográficas y redes sociales, bloquear descarga archivo multimedia	afectación directa a la imagen, reputación y seguridad de la organización	no se tiene reemplazo inmediato	CONFIDENCIAL 3	INTEGRIDAD 3	DISPONIBILIDAD 3
Ethernet y Wireless 802.11 a/b/c/n/g	fallas en el funcionamiento ocasiona desconexión de los dispositivos a la red informática	tiempo de soporte en sitio representan costos y no hay garantía que se pueda solucionar de forma inmediata	30 minutos 500 USD	CONFIDENCIAL 2	INTEGRIDAD 2	DISPONIBILIDAD 3

Tabla 44 Estimación del riesgo (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIA OPERACIONAL	Criterio de Impacto			
			Valoración de reemplazo del activo	Consecuencias para la organización por la pérdida o compromiso de los activos		
equipos de telecomunicaciones	fallas en los equipos causarían interrupción del servicio de datos o Internet lo que significa afectación grabe a la operación de la organización	tiempo de soporte en sitio representan costos y no hay garantía que se pueda solucionar de forma inmediata	30 minutos 3500 USD	CONFIDENCIAL 2	INTEGRIDAD 2	DISPONIBILIDAD 3
solicitudes del cliente sin tomar en cuenta sugerencias de seguridad informática	impacto directo debido a que las disposiciones del cliente comprometen el desempeño de la red	Disposiciones del cliente que pongan en peligro la seguridad de la información deben ser documentadas con firma de responsabilidad haciendo constar las debidas sugerencias realizadas por el especialista de seguridad informática.	no se tiene reemplazo inmediato	CONFIDENCIAL 3	INTEGRIDAD 3	DISPONIBILIDAD 3

Tabla 45 Estimación del riesgo (Julio, 2016)

ACTIVOS	ESCENARIO DE INCIDENTE	CONSECUENCIA OPERACIONAL	Criterio de Impacto			
			Valoración de reemplazo del activo	Consecuencias para la organización por la pérdida o compromiso de los activos		
energía eléctrica	Interrupción del servicio de electricidad adicional al corte de servicio de telecomunicaciones ocasionado por apagado de los equipos de telecomunicaciones, puede ocasionar daño en la información del os clientes o afectación grabe al disco duro de los dispositivos.	corte de energía eléctrica comercial es una afectación directa debido a que a pesar de disponer de un UPS para afrontar estas contingencias el tiempo de respaldo para la cantidad de equipos es de 30 min máximo	no se tiene reemplazo inmediato	CONFIDENCIAL 1	INTEGRIDAD 1	DISPONIBILIDAD 3

Tabla 46 Estimación del riesgo (Julio, 2016)

Evaluación del riesgo

“Evaluación del riesgo es proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. (ISO/IEC Guía 73:2002)” (ISO/ICE, ITC, 2005, pág. 11). (Julio, 2016) (Ing. Mayorga, 2014)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Provisión de servicio de acceso Internet y Datos	Un caso grave de afectación al servicio que limite el acceso del cliente a la red LAN, WLAN o WAN seria critico ya que estaríamos imposibilitados de prestar el servicio para el cual fuimos contratados	imposibilidad de acceso a la red limita las actividades de la organización el tiempo de restablecimiento del servicio debe ser mínimo de acuerdo al plan de contingencia	5	3	15	1

Tabla 47 Evaluación del riesgo (Julio, 2016)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Computadoras	errores en el funcionamiento afectación grave a la operación	tiempo de soporte en sitio representa costos y no hay garantía que se pueda solucionar inmediatamente	5	3	15	7
Firewall	errores en el funcionamiento afectación grave a la operación	tiempo de soporte en sitio representa costos y no hay garantía que se pueda solucionar inmediatamente	5	3	15	3

Tabla 48 Evaluación del riesgo (Julio, 2016)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Software son licencia (pirata)	Utilizar software pirata permite la intrusión de virus en el dispositivo lo que expone la seguridad y disponibilidad de la red informática	afectación directa a la imagen, reputación y seguridad de la organización	4	5	20	9
control de contenido	evitar el acceso a páginas pornográficas y redes sociales, bloquear descarga de archivos multimedia	afectación directa a la imagen, reputación y seguridad de la organización	5	2	10	6

Tabla 49 Evaluación del riesgo (Julio, 2016)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
Ethernet y Wireless 802.11 a/b/c/n/g	errores en el funcionamiento afectación grave a la operación	tiempo de soporte en sitio representa costos y no hay garantía que se pueda solucionar inmediatamente	5	2	10	4
equipos de telecomunicaciones	errores en el funcionamiento afectación grave a la operación	tiempo de soporte en sitio representa costos y no hay garantía que se pueda solucionar inmediatamente	5	2	10	2

Tabla 50 Evaluación del riesgo (Julio, 2016)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
solicitudes del cliente sin tomar en cuenta sugerencias de seguridad informática	impacto directo debido a que las disposiciones del cliente comprometen el desempeño de la red	Disposiciones del cliente que pongan en peligro la seguridad de la información deben ser documentadas con firma de responsabilidad y haciendo constar sugerencias realizadas	4	2	8	8

Tabla 51 Evaluación del riesgo (Julio, 2016)

ACTIVOS	Escenario de Incidente		Impacto de la amenaza	Probabilidad	Medición de riesgo	Priorización
	Amenaza	Vulnerabilidad	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta	1 Muy baja 2 Baja 3 Media 4 Alta 5 Muy alta		
energía eléctrica	Interrupción del servicio de electricidad ocasiona corte de servicio de telecomunicaciones apagado de equipos telecomunicaciones, puede ocasionar daño en la información o afectación grave al disco duro de los dispositivos.	corte de energía eléctrica comercial es una afectación directa debido a que a pesar de disponer de un UPS para afrontar contingencias el tiempo de respaldo para la cantidad de equipos es de 30 min máximo	5	2	10	5

Tabla 52 Evaluación del riesgo **(Julio, 2016)**

Tratamiento de riesgo

"Tratamiento del riesgo es el proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE 27001, 2005, pág. 11).

"Aceptación de riesgo es la decisión de aceptar el riesgo (ISO/IEC Guía 73:2002)" (ISO/ICE, ITC, 2005, pág. 11)

"Reducción del riesgo son las acciones tomadas para reducir la probabilidad de los riesgos asociados con las consecuencias negativas (ISO/IEC Guía 73:2002)" (IEC/ITC 27005, 2008, pág. 2).

"Retener el riesgo es aceptar el peso de perder o beneficiarse de la ganancia de un riesgo particular (ISO/IEC Guía 73:2002)". (IEC/ITC 27005, 2008, pág. 2).

"Transferir el riesgo es compartir con otra parte el peso de perder o beneficiarse de la ganancia de un riesgo" (IEC/ITC 27005, 2008, pág. 2). (Ing. Mayorga, 2014)

A continuación se presenta la tabla en la que se toma la decisión del tratamiento de riesgo.

Tabla de decisión de tratamiento de riesgo

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Política de seguridad informática	Documento de política de seguridad informática	X		Elaboración de las políticas de seguridad para procesos
	Revisión de la política de seguridad informática		X	
Organización interna	Compromiso de los directivos con la seguridad informática	X		La organización interna estructurada permite realizar un adecuado seguimiento monitoreo y control enfocado a la seguridad informática y de la información
	Coordinación de la seguridad informática	X		
	Asignación de responsabilidades de la seguridad informática	X		
	Proceso de autorización para los medios de procesamiento de información	X		
	Acuerdos de confidencialidad	X		
	información de políticas de seguridad disponible para personal autorizado	X		
	Contacto con grupos de interés especial	X		
	Documento de políticas de Seguridad Informática	X		

Tabla 53 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Entidades externas	Identificación de riesgos relacionados con entidades externas	X		mantener un control en las actividades de las entidades externas relacionadas con nuestros procesos es importante ya que sus acciones generan consecuencias positivas o negativas sobre nuestra organización
	Tratamiento de la seguridad cuando se trabaja con contratistas	X		
Responsabilidad por los activos	Inventario de activos	X		Se debe precautelar la seguridad de los bienes de la organización
	Propiedad de los activos	X		
	Uso aceptable de los activos	X		
Clasificación de la información	Lineamientos de clasificación	X		La adecuada organización de la organización es fundamental
	Etiquetado y manejo de la información	X		

Tabla 54 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Seguridad de los Recursos Humanos antes de funciones	Roles y responsabilidades	X		Los colaboradores internos y externos de la empresa son potenciales riesgos para la información de la organización de manera consiente o por desconocimiento pueden afectar los sistemas informáticos es por esto que la seguridad informática debe ser difundida de manera suficiente con TODOS los individuos que se relacionen de cualquier manera con las actividades de la organización
	Selección	X		
	Términos y condiciones de empleo	X		
Seguridad de los Recursos Humanos durante las funciones	Gestión de responsabilidades	X		
	Capacitación y educación en seguridad de la información	X		
	Proceso disciplinario	X		
Seguridad de los Recursos Humanos al finalizar funciones relacionadas con la organización	Responsabilidades en terminación	X		
	Devolución de activos informáticos y de la información	X		
	Eliminación de derechos de acceso	X		

Tabla 55 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Áreas seguras	Perímetro de seguridad física	X		Los activos informáticos son indispensables para el desarrollo de las actividades de toda organización moderna, el control y seguridad de los mismos está directamente relacionada con el área física en la que estos dispositivos funcionan, el sitio de implementación debe disponer de todas las características estándar que brinden seguridad.
	Controles de entrada físicos	X		
	Seguridad de oficinas, centros de control y medios	X		
	Protección contra amenazas externas y ambientales	X		
	Trabajo en áreas seguras	X		
Seguridad del equipo	Ubicación y protección del equipo	X		Los activos informáticos son indispensables para el desarrollo de las actividades de toda organización moderna, el control y seguridad de los mismos es una prioridad para la organización
	Servicios públicos	X		
	Seguridad en el cableado	X		
	Mantenimiento de equipo	X		

Tabla 56 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Gestión de la seguridad en redes	Controles de red	X		La disponibilidad de conexión a la red es la razón de ser de la organización
	Seguridad de los servicios de red	X		
Gestión de medios	Gestión de los servicios removibles	X		todos los medios de manejo de la información deben ser auditados y controlados ya que representan una amenaza importante a la seguridad
	Eliminación de los medios	X		
	Procedimientos de manejo de información	X		
	Seguridad de documentación del sistema	X		
Monitoreo	Uso del sistema de monitoreo	X		El monitoreo de las actividades de la red y del ancho de banda utilizado por las diferentes subredes es un aspecto fundamental de la solución técnica debido a que el análisis de estos datos obtenidos mediante el monitoreo nos permiten generar acciones en función de la óptima provisión del servicio
	Protección de la información del registro	X		
	Registros del administrador y operador	X		
	Registro de fallas	X		

Tabla 57 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Control de acceso	Política de Control de acceso	X		actividad fundamental el control de acceso a la red
Gestión del acceso del usuario de sistemas de información	Inscripción del usuario	X		la gestión de acceso al usuario principio básico de la red
	Gestión de privilegios	X		
	Gestión de la clave de usuario	X		
	Revisión de los derechos de acceso del usuario	X		
Responsabilidades del usuario	Uso de clave	X		definir responsabilidades básicas del usuario ante la utilización de sus dispositivos debe ser una práctica muy clara dentro de la organización
	Equipo de usuario desatendido	X		
Control de acceso a redes	Política sobre el uso de servicios de red	X		Parte fundamental de la Seguridad informática es el control de acceso a la red
	Autenticación del usuario para conexiones externas	X		
	Identificación del equipo en la red	X		
	subnetting de redes	X		
	Protección de acceso remoto	X		

Tabla 58 Tratamiento del riesgo (Julio, 2016)

Objetivos de Control	Controles	Aplicabilidad		Justificación
		Si	No	
Gestión de incidentes de seguridad de información	Reporte de eventos de seguridad de información	X		El registro de los eventos que se suceden en la red es indispensable para el análisis de desempeño y toma de decisiones de controles a implementarse
	Reporte de debilidades de seguridad de la información	X		

Tabla 59 Tratamiento del riesgo **(Julio, 2016)**

Rediseño de la Red

Análisis de Requerimientos

- Detallar los materiales y equipos necesarios que permitan brindar un servicio garantizado con un 100% de disponibilidad.
- Establecer configuraciones básicas en los equipos sugeridos, de manera que sirvan de guía mínima de implementación de la solución planteada.
- Detallar políticas de seguridad informática que orienten al profesional acerca de que debe proteger en su red y de qué manera debe hacerlo.
- Enumerar los posibles problemas que podría afrontar la red, tanto en su infraestructura lógica como física, y plantear las soluciones para cada caso.
- Plantear procedimientos de documentación y registro que nos permitan evidenciar la oportuna y eficaz entrega del servicio y equipos mediante actas de entrega recepción.
- Análisis de diferentes escenarios de operación y las posibles soluciones que se pueden proponer, basados en implementaciones reales, concluyendo en cada caso el desempeño de la red.
- Evidenciar en campo el desempeño de cada una de las soluciones y emitir conclusiones una vez analizados los resultados obtenidos con cada solución.
- Promover el uso de tecnologías que provean alto grado de confiabilidad pero en el formato de licencia gratuita y bajos costos de infraestructura.

En la tabla a continuación detallamos las características técnicas de cada uno de los routers que se utilizan para la implementación de manera que podamos realizar una comparativa de las características de hardware y software disponibles en estos equipos esto nos permitirá evaluar si realmente el precio del os equipos representa su efectividad o se relaciona más con la marca de los mismos. (Cisco Systems C. , 2015) (Mikrotik, 2016) (Julio, 2016)

Resumen comparativo Cisco y Mikrotik

	CISCO 1941-K9	**MIKROTIK RB951Ui-**
PRECIO ROUTER	703 USD	105 USD
Gigabit Ethernet 10/100/1000	2	0
Fast Ethernet 10/100 ports	0	5
SFP-Based Ports	0	1
Memory Default	512 MB	128 MB
procesador	x86	CPU 1 core 650 MHz
External USB slots	2 NO ACTIVOS	1 (multipropósito)
based crypto acceleration (IPSec)	SI (NO INCLUIDA precio **630 usd**)	SI (INCLUIDA)
LICENCIA DATA AVANZADA	SI (NO INCLUIDA)	SI (INCLUIDA)
LICENCIA SEGURIDADES	SI (NO INCLUIDA)	SI (INCLUIDA)
wireless	NO DISPONIBLE	SI
PoE in	NO	SI (un puerto)
PoE out	NO	SI (un puerto)
Voltage Monitor	NO	SI
Antenna gain DBI	NO DISPONIBLE	2
Max Power consumption	35 W	19 W
SFP ports	0	1
Antenna gain DBI	2	2
Operating temperature range	- 40C to +70C	- 35C to +65C
Wifi	NO DISPONIBLE	2.4 Ghz
Wireless Access point antena	NO DISPONIBLE	802.11b/g/n

Tabla 60 comparativo routers **(Julio, 2016)**

4. Teoría de las herramientas

1.1. Aplicación práctica 1

Primera aplicación práctica de solución, se plantea la utilización de infraestructura basada en equipos marca Cisco, obviamente todo en versiones corporativas, que el fabricante asegura son equipos que soportan un alto backplane y adicionalmente poseen características de seguridad y operatividad sumamente eficientes.

En la práctica realizada por el investigador se ha verificado que son equipos muy solventes y confiables en su desempeño, se puede contar con un alto grado de garantía al momento de implementar soluciones basadas en esta tecnología, importante estos equipos para su adecuado desempeño requieren un operador especializado.

La provisión de infraestructura de acceso a conexiones para redes de datos e internet dirigidas a entornos corporativos que se desarrollen fuera de su centro habitual de trabajo, deben disponer de parámetros básicos de conexión y seguridades, el correcto dimensionamiento permitirá a los proveedores de estos servicios implementar redes confiables y que cumplan con las expectativas del cliente, para disponer de una referencia comprobada se realiza esta investigación. (Cisco Systems C. , 2015)

La solución planteada por el investigador tiene dos opciones de implementación, las dos opciones son 100% efectivas y han sido probadas en el entorno real, consiguiendo el estándar requerido de disponibilidad, la ingeniería lógica de implementación es la misma en las dos soluciones, lo que las diferencia son los equipos utilizados en cada una, en el primer caso se utilizan equipos corporativos de gama alta y de una marca posicionada en el mercado misma que el costo de equipos son altos y la configuración de los mismos exige un altísimo grado de especialización lo que encarece la solución, pero brinda tranquilidad en la operatividad del sistema. En el segundo caso los equipos sugeridos son versiones corporativas de alta gama, pero la marca es todavía nueva en el mercado por lo que su costo es mucho menor a la primera solución, se puede considerar que la configuración de estos equipos es de menor complejidad, pero

en base al alto grado de exigencia en seguridad y eficiencia que requiere la solución el costo de la configuración es de costo medio y requiere de igual manera un especialista. (S.A.S., 2014)

Para las dos aplicaciones prácticas se considerara un ancho de banda troncal 15 Mbps, distribuido en redes inalámbricas con diferentes SSID de acuerdo al usuario para el cual está dirigida la red, conexión mediante cableado estructurado, dirigido a servers y equipos críticos, el control de ancho de banda se lo realiza bajo demanda privilegiando los procesos propios de la empresa o institución.

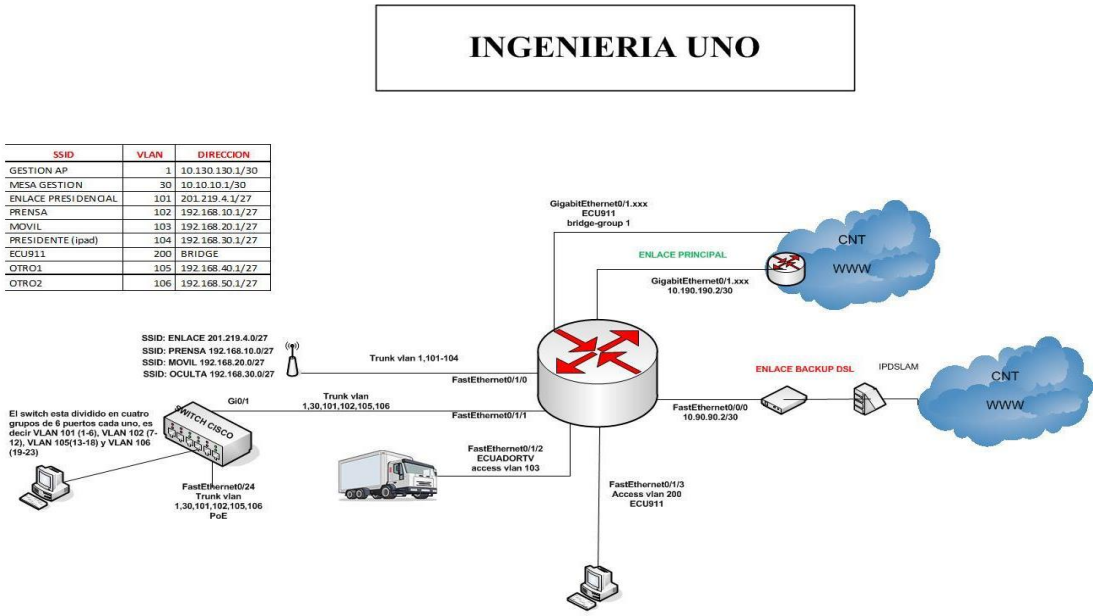


Ilustración 37 Ingeniería solución infraestructura uno **(Julio, 2016)**

A continuación se ilustra el equipamiento propuesto.

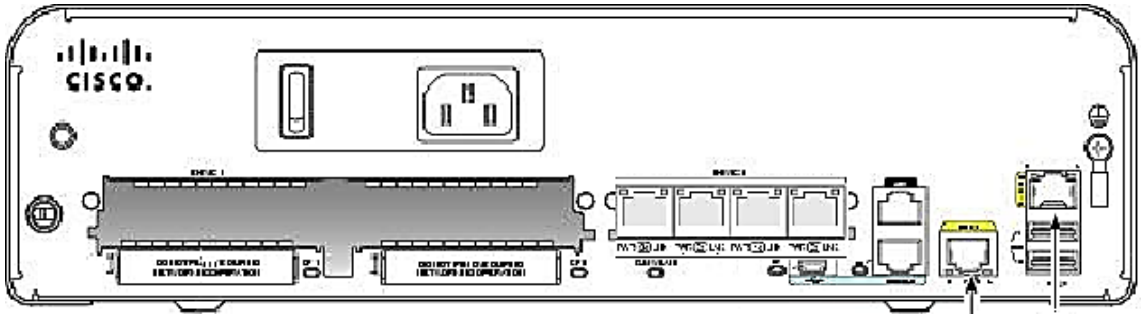


Ilustración 38 Cisco router 1900 k9 **(Cisco Systems C. , 2015)**

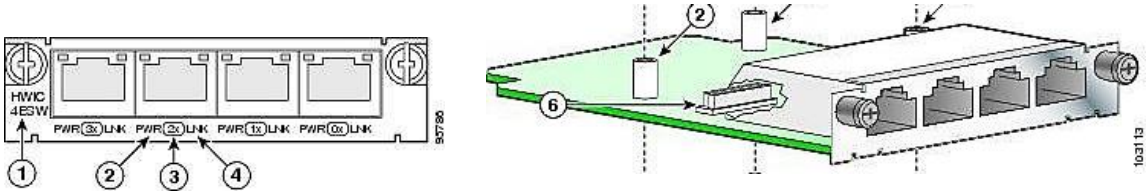


Ilustración 39 Cisco HWIC-4ESW **(Cisco Systems C. , 2015)**

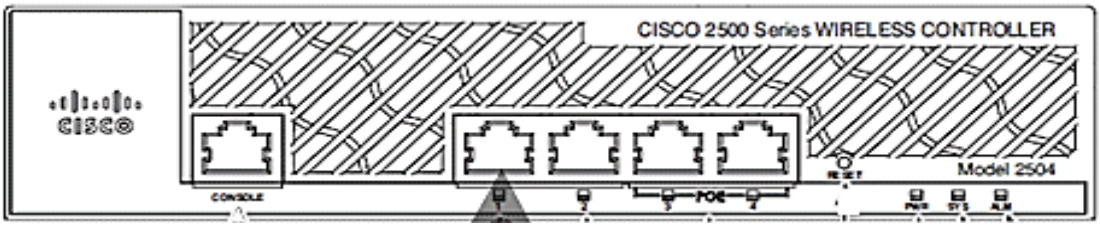


Ilustración 40 Cisco Wireless LAN controller **(Cisco Systems C. , 2015)**

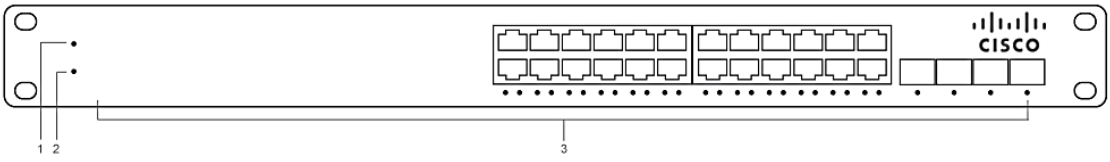


Ilustración 41 Cisco switch 24 port POE **(Cisco Systems C. , 2015)**

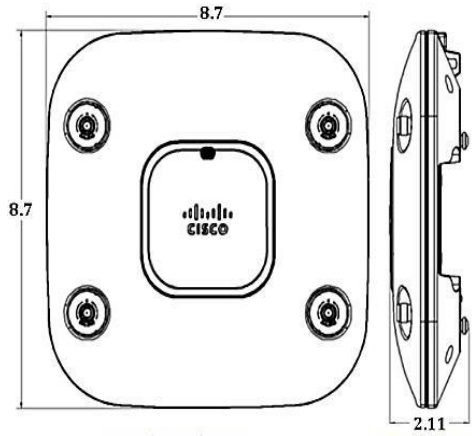


Ilustración 42 Cisco Aironet access point **(Cisco Systems C. , 2015)**

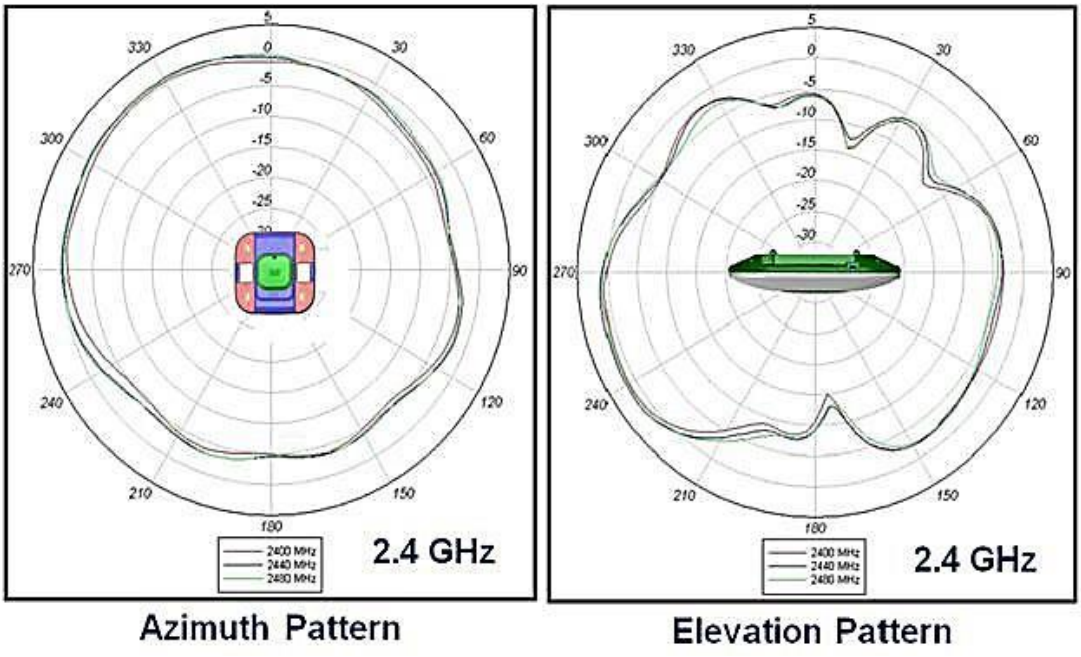


Ilustración 43 cobertura AP Cisco Aironet **(Cisco Systems C. ,**

Rack móvil: Es indispensable para la solución planteada disponer de un rack que permita movilizar los equipos y materiales utilizados para la implementación de la infraestructura, la ilustración corresponde al equipamiento óptimo ya que cumple con características específicas de transporte de equipos de telecomunicaciones. En los link a continuación se amplía la información de opciones y verificar las características del equipamiento. Este rack se considera activo informático indispensable para las dos soluciones planteadas.

http://www.ecscase.com/

https://www.youtube.com/watch?v=0OxOT-98mqY

4.2. Aplicación Práctica 2

Ilustración 44 Case rack reforzado móvil

Para nuestra segunda aplicación práctica, se plantea la utilización de infraestructura basada en equipos varias marcas Mikrotik para ruteo y seguridades, Ruckus para acceso wifi, y cisco para acceso alámbrico y POE, obviamente todo en versiones corporativas, que el fabricante asegura son equipos que soportan un alto backplane y adicionalmente poseen características de seguridad y operatividad sumamente eficientes.

La aplicación práctica dos, es mucho más económica, en cifras representa el 40% del costo de la primera opción, aplicaciones prácticas en equipamiento, sin embargo con esta segunda aplicaciones prácticas además del menor costo, ganamos opciones adicionales de configuración en varios aspectos que serán evidenciados en el desarrollo de la solución.

En la práctica he verificado que son equipos muy solventes y confiables en su desempeño, se puede contar con un alto grado de garantía al momento de implementar soluciones basadas en esta tecnología. (Mikrotik, 2016)

La provisión de infraestructura de acceso a conexiones para redes de datos e internet dirigidas a entornos corporativos que se desarrollen fuera de su centro habitual de trabajo, deben disponer de parámetros básicos de conexión y seguridades, el correcto dimensionamiento permitirá a los proveedores de estos servicios implementar redes confiables y que cumplan con las exceptivas del cliente, para disponer de una referencia comprobada se realiza esta investigación.

INGENIERIA DOS

SSID	VLAN	DIRECCION
GESTION AP	1	10.130.130.1/30
MESA GESTION	30	10.10.10.1/30
ENLACE PRESIDENCIAL	101	201.219.4.1/27
PRENSA	102	192.168.10.1/27
MOVIL	103	192.168.20.1/27
PRESIDENTE (ipad)	104	192.168.30.1/27
ECU911	200	BRIDGE
OTRO1	105	192.168.40.1/27
OTRO2	106	192.168.50.1/27

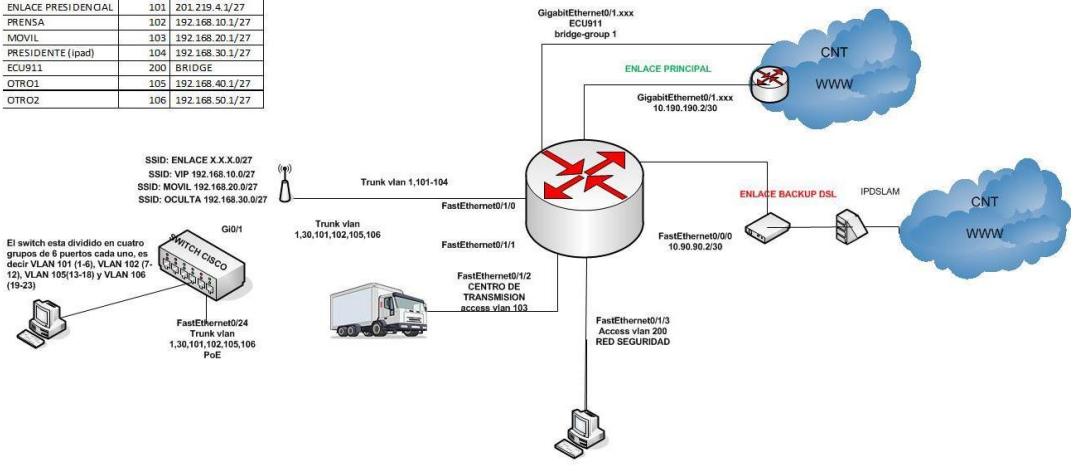


Ilustración 45 Ingeniería dos solución infraestructura **(Julio, 2016)**

A continuación se ilustra el equipamiento propuesto.

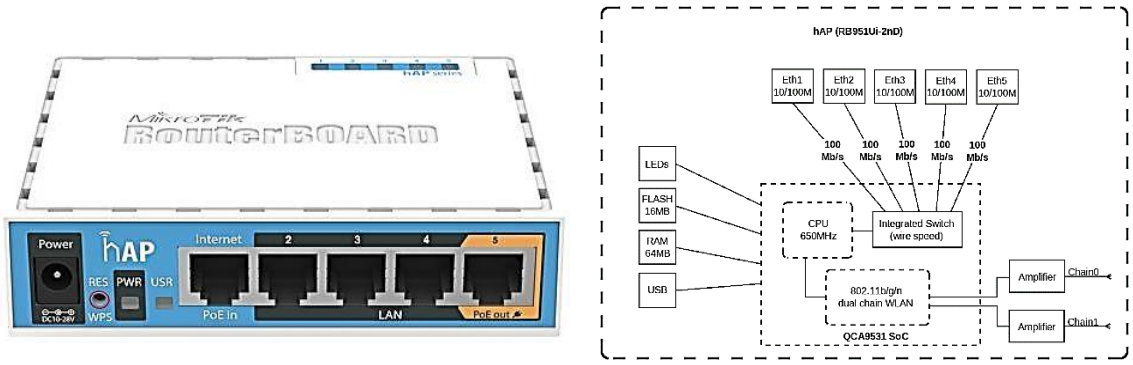


Ilustración 46 Mikrotik routerboard RB951Ui-2nD **(Mikrotik, 2016)**

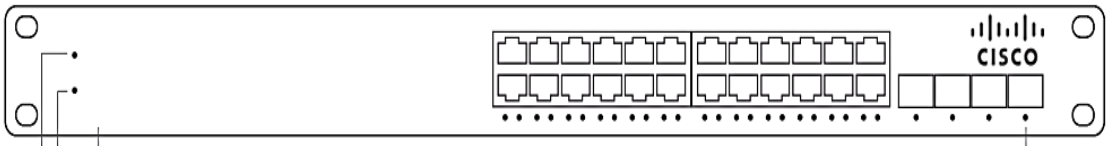


Ilustración 47 Cisco switch 24 port POE **(Cisco Systems C. , 2015)**

Ilustración 48 Ruckus Wirelles LAN controller **(RUCKUS, 2016)**

Ilustración 49 Ruckus Access Point **(RUCKUS, 2016)**

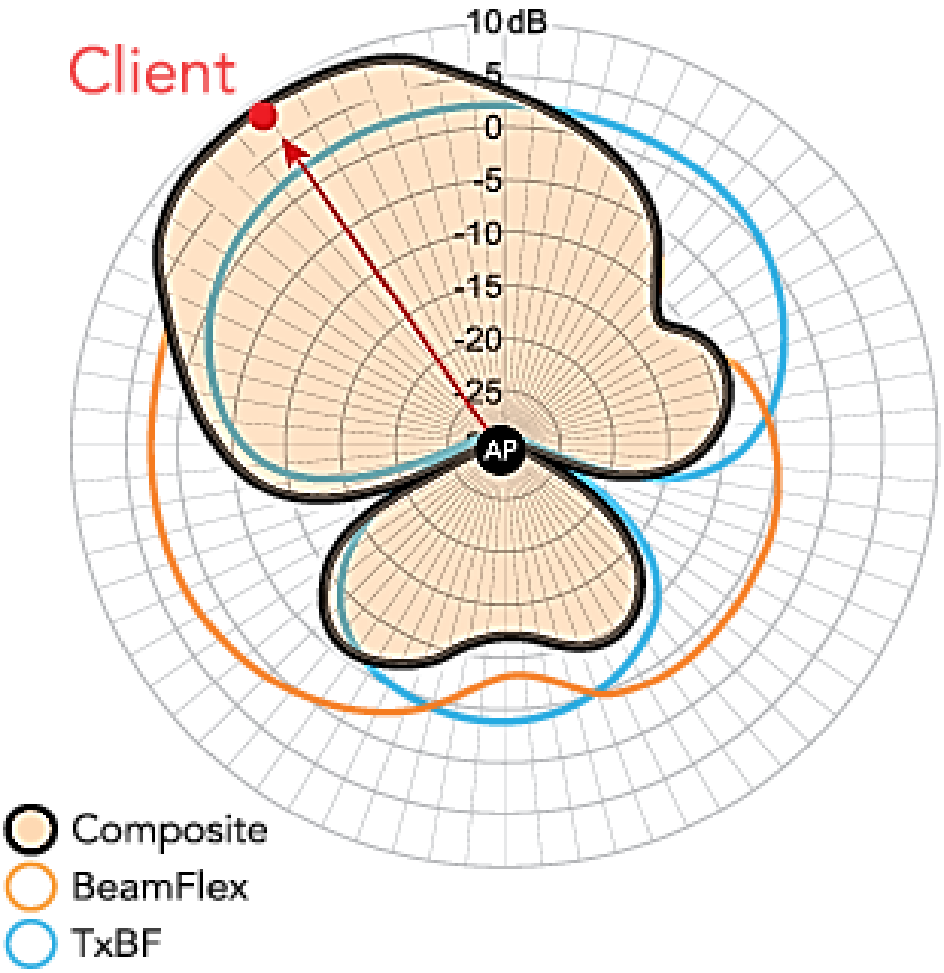


Ilustración 50 Cobertura AP Ruckus **(RUCKUS, 2016)**

Asignación y configuración de recursos tecnológicos.

Para redes de alto desempeño los equipos asignados son versiones corporativas obviamente de alto desempeño, mismos que requieren de un especialista para la configuración, es por esto que el envío de estos equipos al sitio del evento se debe realizar desde el centro de operaciones de red de la empresa o institución, los equipos previamente configurados y probados, deben ser enviados con todos los cables y accesorios necesarios, ya que no podemos asumir que se tendrá acceso a recursos en el sitio de destino. Es indispensable el envío de equipos de respaldo para afrontar cualquier problema que pudiera presentarse en el sitio del evento. Para la asignación de personal en sitio no siempre se podrá ni es indispensable, enviar a un especialista de alto nivel, es por eso que se asigna para implementación en sitio, a personal con una capacitación técnica suficiente, que entienda muy bien la infraestructura implementada y que esté capacitado para habilitar el enlace en su interfaz WAN de esa manera el soporte de especialista se puede realizar remotamente.

Monitoreo y Gestión de enlaces.

Una vez que el enlace está operativo el monitoreo del mismo es indispensable, este monitoreo en línea nos permite prever problemas como saturación o comportamientos singulares de la red, con la finalidad de gestionar remotamente cambios en la red que permitan mantener el enlace con un 100% de disponibilidad.

Adicionalmente, mediante el análisis del monitoreo de varios eventos podemos mejorar el desempeño de la red, implementando cambios oportunos en base a los datos obtenidos, determinar si el equipamiento asignado es suficiente en procesamiento y memoria para atender la demanda de recursos, o analizar el trafico utilizado y tomar medidas oportunas de seguridad y calidad de servicio para procesos en la red. (Cisco Systems I. , 2015) (Mikrotik, 2016)

Soporte Técnico Troubleshooting

En la infraestructura de red, es muy importante conocer el modelo OSI y TCP IP de red, ya que mediante el análisis escalonado de las capas del modelo se logra determinar los problemas que pudieran presentarse en las redes de telecomunicaciones.

Es decir se inicia el análisis en las primeras capas del modelo OSI se va descartando posibles problemas de la red, iniciamos revisando dispositivos de la primera capa medios físicos como cableado conectores una vez descartados en la segunda capa debemos verificar visualización del equipo en la red mediante mac address en la tercera capa ya verificamos parámetros de red direcciones lógicas ruteo todo lo que tiene que ver con las subredes y su conectividad a nivel de IP. En las capas superiores ya se tiene conectividad de extremo a extremo ya se verifica hasta donde están llegando los paquetes, es importante anotar que networking trabaja hasta la cuarta capa del modelo OSI y tercer capa del modelo TCP/IP. (Cisco Systems I. , 2015) (Mikrotik, 2016)

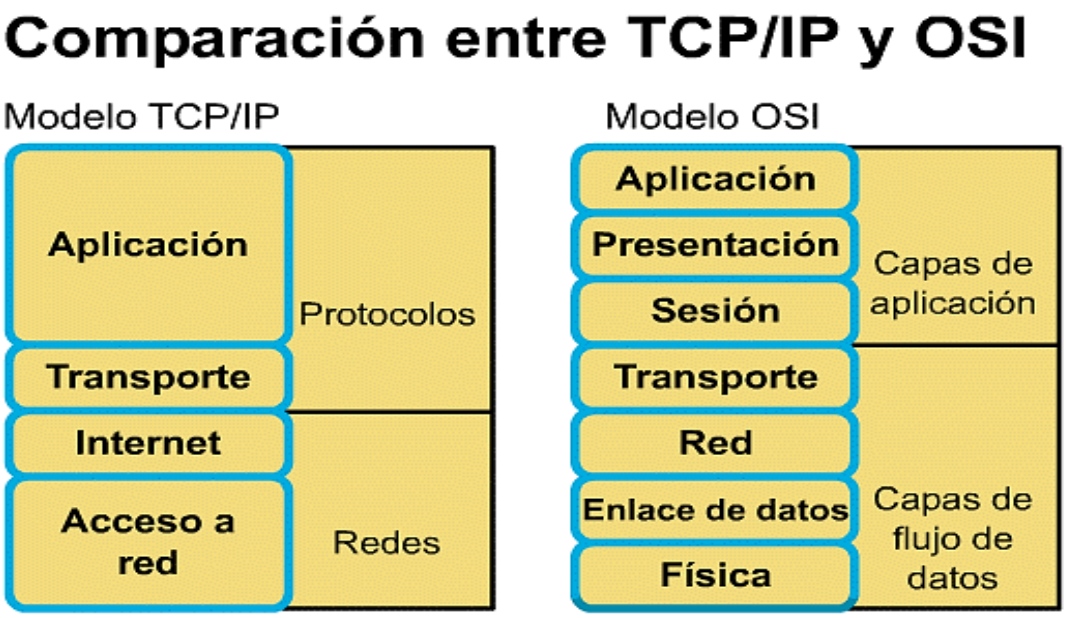


Ilustración 51 Troubleshooting modelo OSI y TCP/IP **(Cisco Systems C. , 2015)**

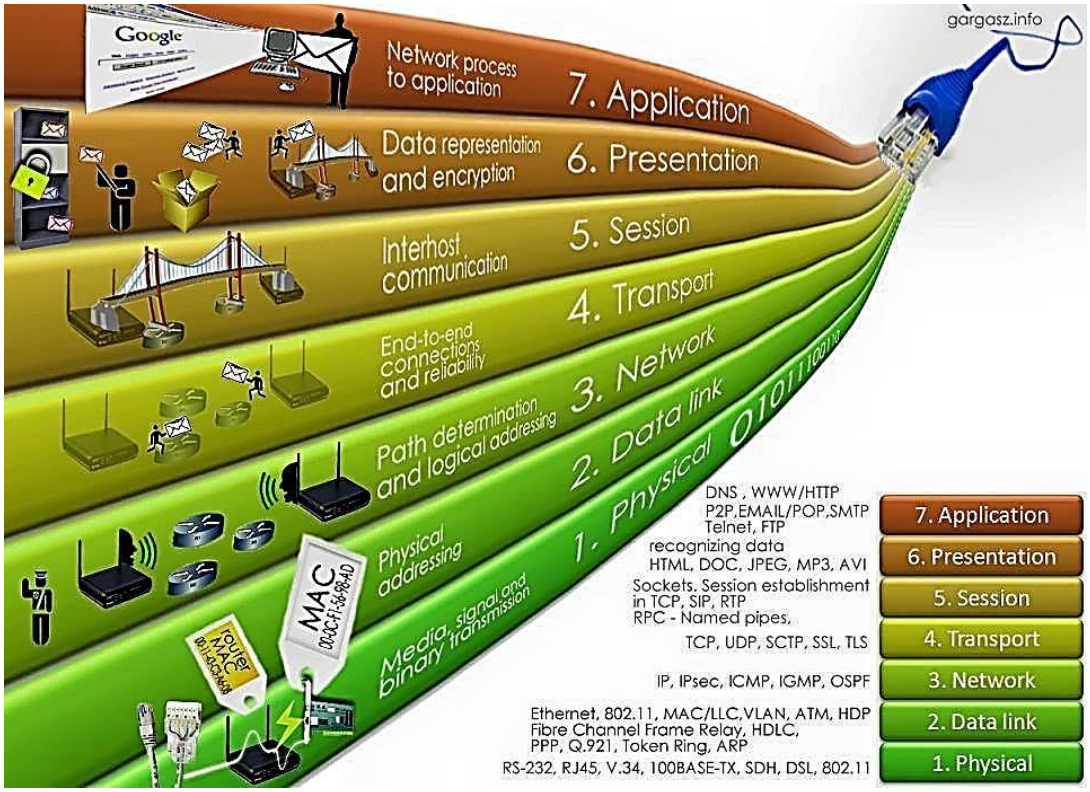


Ilustración 52 dispositivos Troubleshooting modelo OSI **(Cisco Systems C. , 2015)**

Conclusiones:

- Para cada evento AAA se enviara personal del equipo de expertos, con el fin de realizar análisis detallados en sitio de implementación de redes inalámbricas, buscando cumplir con los estándares más altos de calidad y disponibilidad de los servicios, de acuerdo a la realidad de cada localidad y ubicación física en la que se desarrolle cada evento.

- Se incrementara opciones en las políticas de monitoreo y logística de los servicios prestados para este tipo de eventos, incorporando nuevos parámetros de verificación, entregando al cliente una herramienta web que le permita conocer al cliente el consumo de Ancho de Banda del servicio entregado en tiempo real y agilitar la toma de decisiones sobre soluciones que permitan solventar inconvenientes fortuitos que se pudieran presentar en cada evento.

- Con la finalidad de incrementar los productos y servicios brindados al cliente, se ha considerado realizar la implementación de una nueva infraestructura inalámbrica para este tipo de eventos, considerando aspectos de redundancia de equipos de acceso.

- A fin de garantizar la disponibilidad del servicio ofrecido y de evitar cualquier intrusión de personas no autorizadas dentro de la red o mal uso de la misma, se implementará en conjunto con el personal de Sistemas, políticas de seguridad de la información, para lo cual se presentará una propuesta en la que se recomendarán las políticas específicas de seguridad para la aprobación del cliente.

- Con la finalidad de identificar de forma inmediata, requerimientos de upgrade o cualquier inconveniente de las conexiones, adicional al personal

de soporte en sitio, antes y durante el evento se intensificara el monitoreo proactivo desde el NOC de la empresa.

- La información de cualquier inconveniente detectado en el funcionamiento de la red, serán reportados de forma inmediata vía telefónica, al contacto que designe el cliente para este fin, como recomendación en caso que sea autorizado por el cliente se implementaría un grupo mediante la aplicación celular de Whats App y mantener informes periódicos del estado la red.
- Para elevar el nivel de seguridad de red, se implementaran diferentes pools de IPS públicas, en cada evento.
- Los inconvenientes de interferencias radican en el uso de equipos inalámbricos tales como microondas, teléfonos inalámbricos, fuentes de video inalámbrico, fugas de RF, que se encuentran usando el mismo canal dentro de la banda de 2.4 Gigas que al momento de llegar a saturar el AB del espectro provoca cortes e intermitencias en el servicio.
- El problema de interferencia por el número de ocupantes de un canal se puede resolver cambiando de frecuencia en forma manual o automática entre los canales del 1 al 13, en ciertos equipos es el Access Point quien realiza esta acción automáticamente, en otros casos se procederá a configurar de manera fija, en el caso del Access Point Cisco modelo APN1042N, tiene la opción para configurar manual y automáticamente.
- El número de clientes que usan el espectro de la banda 2.4 Gigas es grande, a tal punto que 14 canales no abastece siendo un problema común el de las interferencias entre equipo WIFI.
- La configuración de redes inalámbricas en la banda 5 Giga Hertzios puede ser una opción en caso de que la banda de 2.4 G se encuentre saturada, la relación entre las dos bandas es de 11 a 1, para entenderlo de la una mejor manera la banda de 2.4G sería una carretera de un carril mientras que la banda 5G sería una carretera de 11 carriles, es decir se tiene menos congestión, el único inconveniente seria que los equipos terminales dispongan de esta característica de hardware, al momento reservada para equipos de alto desempeño o tope de gama. De la misma manera se realizó una configuración similar a la 2.4G pero con 5G en equipos Cisco.

Recomendaciones:

- Se recomienda la configuración de las redes inalámbricas en canales de frecuencia 5G, tomando en cuenta que los dispositivos finales deben soportar dicha tecnología.

- Durante el trabajo en el sitio el Ingeniero de Soporte Técnico Corporativo, debe contar con el analizador de WIFI que permite conocer el estado del espectro de 2.4G y 5G, y detectar si existen fuentes de interferencia en el sitio. Otra opción que nos permitiría mitigar la interferencia por saturación de canal en la banda 2.4 Giga hertzios seria implementar dos SSID por cada Access Point, en tal caso se requeriría de dos Access Point, la finalidad sería el de configurar manualmente cada Access Point en diferentes canales evitando que estos se solapen, para lo cual la medición se realizara con el analizador de señales WIFI.

- El ingeniero de soporte corporativo en sitio o remoto tener un elevado nivel de conocimiento acerca de la operación de todos los dispositivos de la red Access Point, switch, routers, firewall, marca CISCO para obtener el mejor provecho de los beneficios que nos puede ofrecer dichos equipos y brindar soluciones rápidas y efectivas a cualquier problema que pueda presentarse

- Por seguridad de la red corporativa se recomienda cambiar el nombre de los SSIDs periódicamente y configurarlos en forma oculta.

- De la misma manera se recomienda que las claves deben ser enviadas ya cifradas y no en texto plano.
- Con la finalidad de precautelar el correcto funcionamiento de los equipos que forman parte de la solución tecnológica, observando las normas de cableado estructurado y en procura de brindar un excelente servicio al cliente, el investigador recomienda disponer de kits que contengan la solución planteada en una rack móvil y a su vez distribuir estos kit de

manera zonificada para atender cualquier requerimiento con excelentes tiempos de respuesta y cumpliendo con las normas de seguridad informática y seguridad de la información planteadas, estos kit al tener todo lo necesario para la implementación, requerirían cambios sencillos y mínimos en su configuración. En el siguiente gráfico el investigador propone una distribución de 5 kit a nivel nacional que puedan cubrir requerimientos de manera zonificada en el menor tiempo posible con opción a backup de equipos en caso de contingencia.

Ilustración 53 zonificación kit de infraestructura red corporativa mediana móvil **(ESPOCH, 2015)**

Bibliografía

bibliophile, e. (1993). *The Apis Embalming Ritual. P. Vindob. 3873, Lovaina: Peeters Press.* Obtenido de http://egyptologicalbibliophile.blogspot.com

Cisco Systems, C. (Agosto de 2015). *Cisco.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html

Cisco Systems, I. (2015). *Tendencias de seguridad Cisco Systems.* Obtenido de https://www.cisco.com/web/ES/campaigns/borderless/security/index.html

Cisco Wiki, d. (2017). Obtenido de http://docwiki.cisco.com/wiki/Main_Page

ESPOCH. (2015). *Escuela Politecnica del Chimborazo.* Obtenido de http://espoch.edu.ec/

Ing. Mayorga, T. (2014). *Maestria en redes de telecomunicaciones.* Ambato: Tesis.

ISO 27001, N.-I.-I. (2013). *ICONTEC.* Obtenido de http://www.icontec.org/

iso27000. (2013). *iso27000.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Julio, i. A. (2016). elaborado por Investigador. Quito.

Mikrotik. (2016). *Mikrotik.* Obtenido de https://www.mikrotik.com/

Mikrotik Wiki, d. (2015). *Mikrotik Wiki.* Obtenido de https://wiki.mikrotik.com/wiki/Tutorials_in_spanish_language

Mintel. (2016). *Ministerio de telecomunicaciones Ecuador.* Obtenido de https://www.telecomunicaciones.gob.ec

Museo Ejercito España, M. d. (2016). *Museo Ejercito Español.* Obtenido de http://www.museo.ejercito.es

Registro Oficial, E. (2017). *Registro Oficial gobierno Ecuador.* Obtenido de https://www.registroficial.gob.ec/

RUCKUS. (2016). *RUCKUS WIRELESS INC.* Obtenido de https://www.ruckuswireless.com/es

S.A.S., D. S. (2014). *Dragonjar.* Obtenido de https://www.dragonjar.org/blog

Trabajos citados

bibliophile, e. (1993). *The Apis Embalming Ritual. P. Vindob. 3873, Lovaina: Peeters Press.* Obtenido de http://egyptologicalbibliophile.blogspot.com

Cisco Systems, C. (Agosto de 2015). *Cisco.* Obtenido de http://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html

Cisco Systems, I. (2015). *Tendencias de seguridad Cisco Systems.* Obtenido de https://www.cisco.com/web/ES/campaigns/borderless/security/index.html

Cisco Wiki, d. (2017). Obtenido de http://docwiki.cisco.com/wiki/Main_Page

ESPOCH. (2015). *Escuela Politecnica del Chimborazo.* Obtenido de http://espoch.edu.ec/

Ing. Mayorga, T. (2014). *Maestria en redes de telecomunicaciones.* Ambato: Tesis.

ISO 27001, N.-I.-I. (2013). *ICONTEC.* Obtenido de http://www.icontec.org/

iso27000. (2013). *iso27000.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

Julio, i. A. (2016). elaborado por Investigador. Quito.

Mikrotik. (2016). *Mikrotik.* Obtenido de https://www.mikrotik.com/

Mikrotik Wiki, d. (2015). *Mikrotik Wiki.* Obtenido de https://wiki.mikrotik.com/wiki/Tutorials_in_spanish_language

Mintel. (2016). *Ministerio de telecomunicaciones Ecuador.* Obtenido de https://www.telecomunicaciones.gob.ec

Museo Ejercito España, M. d. (2016). *Museo Ejercito Español.* Obtenido de http://www.museo.ejercito.es

Registro Oficial, E. (2017). *Registro Oficial gobierno Ecuador.* Obtenido de https://www.registroficial.gob.ec/

RUCKUS. (2016). *RUCKUS WIRELESS INC.* Obtenido de https://www.ruckuswireless.com/es

S.A.S., D. S. (2014). *Dragonjar.* Obtenido de https://www.dragonjar.org/blog

ANEXOS

Anexo 1

Configuración lógica de equipos

En el detalle de configuración de los dispositivos de ruteo y acceso a la red se puede observar las técnicas y metodología utilizada para la puesta en marcha del enlace.

Tanto para Cisco como para Mikrotik se utiliza:

- protocolos de enrutamiento estático en atención a que la cantidad de subredes configuradas mismas que no justifican otro tipo de protocolo de enrutamiento.
- Para atender la convergencia de medios, el investigador utiliza una técnica básica, diferencia los diferentes usuarios mediante la creación de varias subredes que a su vez son asignadas a interfaces vlan lo que le permite aplicar diferente ancho de banda por subred dependiendo a quien o a que servicio este asignado el pool de IP
- Controlar los puertos disponibles en el router es indispensable para asegurar la disponibilidad del servicio es por esto que las políticas de seguridad deben ser acordadas previamente con el cliente.
- Debe procurar tener accesos enfocados exclusivamente a la operación de la organización, servicios o aplicaciones de ocio o que no guardan relación con la operación de la organización deben ser bloqueadas.
- Se debe crear un acceso con mayores privilegios a la menor cantidad posible de dispositivos, debiendo asegurarse que estos dispositivos cumplan con parámetros básicos de seguridad informática.
- La conexión de los dispositivos de usuario a la red debe tener un formato de contraseña que cumpla con parámetros básicos de seguridad y debe ser diferentes para cada subred o ssid disponible.
- Es altamente deseable que los dispositivos se conecten a la red mediante el registro de la mac address de esa manera identificamos que dispositivo realizó qué acción.

- Las paquetes de voip, ftp y video conferencia deberán ser marcados como trafico prioritario obviamente al ser un enlace de internet esta marcación se consigue únicamente en el tráfico interno del router al salir el paquete hacia el internet no tenemos control del mismo por lo que no podemos garantizar su desempeño.
- La solución para que las aplicaciones críticas de la organización sean atendidas prioritariamente antes que el ocio o gestiones menos importantes es priorizar el puerto de conexión en el que funciona esa aplicación, por ejemplo se debe atender primero el puerto 21 que corresponde a FTP en lugar del puerto 443 que corresponde a Facebook.

Script de programación equipos de telecomunicaciones aplicación Práctica 1

Router cisco 1941 k9 licencia ip services

```
GABINETE100#sh run
Building configuration...

Current configuration : 7558 bytes
!
! Last configuration change at 08:33:01 EC Fri May 29 2015 by cnt
!
version 15.0
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
hostname GABINETE100
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 5 $1$CzV4$DirSkjgpJXsAhW4PcFFpI/
!
aaa new-model
aaa local authentication attempts max-fail 3
!
!
aaa authentication login default local
aaa authentication login RG2 local enable
```

```
aaa authentication enable default enable
aaa authorization console
aaa authorization exec default local if-authenticated
aaa authorization commands 15 default local
!
!
!
!
!
aaa session-id common
clock timezone EC -5
!
no ipv6 cef
ip source-route
ip cef
!
!
ip dhcp bootp ignore
ip dhcp excluded-address 192.168.200.1
ip dhcp excluded-address 192.168.200.15
ip dhcp excluded-address 192.168.106.1
ip dhcp excluded-address 192.168.107.1
!
ip dhcp pool VICESNAP
  network 192.168.200.0 255.255.255.240
  domain-name VICESNAP_CNT
  default-router 192.168.200.1
  dns-server 200.107.10.100 201.219.1.19
!
ip dhcp pool SECOM_CNT
  network 192.168.100.0 255.255.255.240
  domain-name SECOM_CNT
  default-router 192.168.100.1
  dns-server 200.107.10.100 201.219.1.19
```

```
!
ip dhcp pool PRESIDENTE_CNT
  network 192.168.104.0 255.255.255.240
  domain-name PRESIDENTE_CNT
  default-router 192.168.104.1
  dns-server 200.107.10.100 201.219.1.19
!
ip dhcp pool MINISTROS_CNT
  network 192.168.105.0 255.255.255.0
  domain-name MINISTROS_CNT
  default-router 192.168.105.1
  dns-server 200.107.10.100 201.219.1.19
!
ip dhcp pool DESPACHO
  network 192.168.106.0 255.255.255.224
  domain-name SECOM_CNT
  default-router 192.168.106.1
  dns-server 200.107.10.100 201.219.1.19
!
ip dhcp pool MONITOREOCNT
  network 192.168.107.0 255.255.255.224
  domain-name SECOM_CNT
  default-router 192.168.107.1
  dns-server 200.107.10.100 201.219.1.19
!
!
no ip bootp server
no ip domain lookup
ip domain name sosnet.net
login block-for 60 attempts 2 within 30
login delay 5
login quiet-mode access-class 3
login on-failure log
login on-success log
```

```
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FTX142781LP
license boot module c1900 technology-package datak9
!
!
archive
log config
 logging enable
 logging size 200
 notify syslog contenttype plaintext
 hidekeys
path
scp://idtv_scorp:s8p4hTAa@200.107.60.53/INTERMINISTERIAL/GABINETE/N2_
DORAL_LAB
write-memory
time-period 21600
memory reserve console 512
!
no spanning-tree vlan 1
no spanning-tree vlan 100
no spanning-tree vlan 101
no spanning-tree vlan 102
no spanning-tree vlan 103
no spanning-tree vlan 106
no spanning-tree vlan 107
no spanning-tree vlan 110
no spanning-tree vlan 825
no spanning-tree vlan 1807
no spanning-tree vlan 1950
vtp mode transparent
username cnt privilege 15 secret 5 $1$..q9$zp4j23CPqHG3RoyFBWPXl1
```

```
!
redundancy
!
!
vlan 2
!
vlan 30
name gestion_switch
!
vlan 101
name CNT
!
vlan 102
name SECOM
!
vlan 103
name VICESNAP
!
vlan 104
name PRESIDENTE
!
vlan 105
name MINISTROS
!
vlan 106
name DESPACHO
!
vlan 107
name MONITOREO_CNT
!
vlan 4059
!
ip ssh time-out 30
ip ssh authentication-retries 2
```

```
ip ssh version 2
!
class-map match-all ICMP
match access-group name ICMP_SECURITY
!
!
policy-map ICMP-POLICY
class ICMP
   police 8000 conform-action transmit  exceed-action drop
!
bridge irb
!
!
!
!
interface GigabitEthernet0/0
description WAN_TRONCAL
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.526
description WAN_PRINCIPAL
encapsulation dot1Q 526
ip address 10.180.180.2 255.255.255.252
no ip redirects
ip nat outside
ip virtual-reassembly
no cdp enable
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
```

```
speed auto
!
interface FastEthernet0/0/0
description HACIA AP
switchport access vlan 102
switchport trunk allowed vlan 1,30,101-107,1002-1005
switchport mode trunk
!
interface FastEthernet0/0/1
description hacia AP
switchport trunk allowed vlan 1,30,101-107,1002-1005
switchport mode trunk
!
interface FastEthernet0/0/2
description SWITCH
switchport trunk allowed vlan 1,30,101-107,1002-1005
switchport mode trunk
!
interface FastEthernet0/0/3
description PUBLICA
switchport trunk allowed vlan 1,30,101-107,1002-1005
!
interface Vlan1
description GESTION_WLC
ip address 192.168.0.1 255.255.255.240
no ip redirects
no ip proxy-arp
!
interface Vlan30
description GESTION_SWITCH
ip address 10.10.10.1 255.255.255.248
!
interface Vlan101
description CNT
```

```
ip address 201.219.4.33 255.255.255.248
no ip redirects
no ip proxy-arp
!
interface Vlan102
description SECOM
ip address 192.168.100.1 255.255.255.224
no ip redirects
no ip proxy-arp
ip nat inside
ip virtual-reassembly
!
interface Vlan103
description VICESNAP
ip address 192.168.200.1 255.255.255.240
no ip redirects
no ip proxy-arp
ip nat inside
ip virtual-reassembly
!
interface Vlan104
description PRESIDENTE
ip address 192.168.104.1 255.255.255.240
no ip redirects
no ip proxy-arp
ip nat inside
ip virtual-reassembly
!
interface Vlan105
description MINISTROS
ip address 192.168.105.1 255.255.255.0
no ip redirects
no ip proxy-arp
ip nat inside
```

```
ip virtual-reassembly
!
interface Vlan106
description DESPACHO
ip address 192.168.106.1 255.255.255.0
no ip redirects
no ip proxy-arp
ip nat inside
ip virtual-reassembly
rate-limit input access-group 106 4096000 768000 1536000 conform-action continue exceed-action drop
rate-limit output access-group 106 4096000 768000 1536000 conform-action continue exceed-action drop
!
interface Vlan107
description MONITOREO_CNT
ip address 192.168.107.1 255.255.255.0
no ip redirects
no ip proxy-arp
ip nat inside
ip virtual-reassembly
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool PUBLICA 201.219.4.34 201.219.4.34 netmask 255.255.255.248
ip nat inside source list 1 pool PUBLICA overload
ip route 0.0.0.0 0.0.0.0 10.180.180.1
!
ip access-list extended ICMP_SECURITY
permit icmp any any
!
```

```
logging trap debugging
access-list 1 permit 192.168.200.0 0.0.0.15
access-list 1 permit 192.168.100.0 0.0.0.31
access-list 1 permit 192.168.104.0 0.0.0.15
access-list 1 permit 192.168.105.0 0.0.0.255
access-list 1 permit 192.168.106.0 0.0.0.31
access-list 1 permit 192.168.107.0 0.0.0.31
access-list 106 permit ip 192.168.106.0 0.0.0.31 any
access-list 106 permit ip any 192.168.106.0 0.0.0.31
!
no cdp run

!
!
!
!
snmp-server community sopCORPn2PB RO
snmp-server ifindex persist
snmp mib persist cbqos
!
control-plane
service-policy input ICMP-POLICY
!
bridge 1 protocol ieee
bridge 2 protocol ieee
banner                                                                  motd
^CCC**************************************************************************
EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO.
Usted debe tener permiso explicito para acceder y/o
Configurar este dispositivo. Todas las actividades realizadas
en el dispositivo son almacenadas.

UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
You must have explicit permission to access or
```

Configure this device. All activities performed on this device
are logged.
**^C
!
line con 0
exec-timeout 5 0
logging synchronous
login authentication RG2
line aux 0
login authentication RG2
line vty 0 4
exec-timeout 5 0
logging synchronous
login authentication RG2
transport input ssh
!
scheduler allocate 20000 1000
end

GABINETE100# (Julio, 2016)

Switch cisco sf-300 srw224g4p-k9 sb

System Description:
24-port 10/100 PoE Managed Switch
System Uptime: 4 days, 18 hr., 29 min. and 57 sec.
System Location:
QUITO - ECUADOR
Current Time: 08:03:52;2010-May-03

System Contact:
JULIO AGUIRRE 096183927
Base MAC Address: 68:bc:0c:77:db:06
Host Name: ENLACE
Jumbo Frames: Disabled
System Object ID: 1.3.6.1.4.1.9.6.1.82.24.2
Model Description: 24-port 10/100 PoE Managed Switch
Firmware Version (Active Image): 1.0.0.27
Serial Number: DNI15390377
Firmware MD5 Checksum (Active Image): 1987292110f5657e74308dde30c03dc4
PID VID: SRW224G4P-K9 V01 Firmware Version (Non-active): 1.0.0.27
Maximum Available Power(W): 180 Firmware MD5 Checksum (Non-active): 1987292110f5657e74308dde30c03dc4
Main Power Consumption(W): 8 Boot Version: 1.0.0.4
System Operation Status: Port Limit Boot MD5 Checksum: 4c9a0b6a9f1346736646d08ab94ae2ac
Locale: en-US
Language version: 1.0.0.27
Language MD5 Checksum: N/A

GABINETESW#show run
vlan database
vlan 30,101-106
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_____
interface vlan 30

```
ip address 10.10.10.2 255.255.255.252
exit
interface vlan 30
no ip address dhcp
exit
hostname GABINETESW
username cisco password Cnts0t@da
lege 15
no snmp-server server
ip telnet server
interface fastethernet1
switchport trunk allowed vlan add 30,101-106
exit
interface fastethernet2
switchport mode access
switchport access vlan 102
exit
interface fastethernet3
switchport mode access
switchport access vlan 102
exit
interface fastethernet4
switchport mode access
switchport access vlan 102
exit
interface fastethernet5
switchport mode access
switchport access vlan 102
exit
interface fastethernet6
switchport mode access
switchport access vlan 102
exit
interface fastethernet7
```

```
switchport trunk allowed vlan add 30,101-106
exit
interface fastethernet8
switchport mode access
switchport access vlan 104
exit
interface fastethernet9
switchport mode access
switchport access vlan 104
exit
interface fastethernet10
switchport mode access
switchport access vlan 104
exit
interface fastethernet11
switchport mode access
switchport access vlan 104
exit
interface fastethernet12
switchport mode access
switchport access vlan 104
exit
interface fastethernet13
switchport mode access
switchport access vlan 105
exit
interface fastethernet14
switchport mode access
switchport access vlan 105
exit
interface fastethernet15
switchport mode access
switchport access vlan 105
exit
```

```
interface fastethernet16
switchport mode access
switchport access vlan 105
exit
interface fastethernet17
switchport mode access
switchport access vlan 105
exit
interface fastethernet18
switchport mode access
switchport access vlan 105
exit
interface fastethernet19
switchport mode access
switchport access vlan 106
exit
interface fastethernet20
switchport mode access
switchport access vlan 106
exit
interface fastethernet21
switchport mode access
switchport access vlan 106
exit
interface fastethernet22
switchport mode access
switchport access vlan 106
exit
interface fastethernet23
switchport mode access
switchport access vlan 106
exit
interface fastethernet24
switchport mode access
```

switchport access vlan 106
exit
interface gigabitethernet1
switchport trunk allowed vlan add 30,101-106
exit
GABINETESW#
(Julio, 2016)

Access point cisco 1042 k9

AP_MINISTROS#show run
Building configuration...
Current configuration : 2248 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP_MINISTROS
!
logging rate-limit console 9
enable secret 5 1ks0O$3vpXGOWm4240/3/mknx.M.
enable password 7 030752180500
!
no aaa new-model
!
!
dot11 syslog
!
dot11 ssid MINISTROS
 vlan 102
 authentication open

```
  authentication key-management wpa version 2
  mbssid guest-mode
  wpa-psk ascii 7 082C4540000A11051D185D5679
!
!
!
username Cisco password 7 1531021F0725
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 102 mode ciphers aes-ccm
!
ssid MINISTROS
!
antenna gain 3
mbssid
packet retries 128 drop-packet
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
```

```
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
antenna gain 0
dfs band 3 block
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0.102
encapsulation dot1Q 102
```

```
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
interface BVI1
ip address 10.130.130.3 255.255.255.248
no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

bridge 1 protocol ieee
bridge 1 route ip
!
!
!
line con 0
password 7 02050D480809
login
line vty 0 4
password 7 14141B180F0B
login
!
end



AP_ENLACE#sh run
Building configuration...
Current configuration : 4070 bytes
!
version 12.4
```

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AP_ENLACE
!
logging rate-limit console 9
enable secret 5 $1$pdQd$U.OmosFkxTNDVhmWEJLUP0
!
no aaa new-model
!
!
dot11 syslog
!
dot11 ssid ENLACE
  vlan 101
  authentication open
  authentication key-management wpa version 2
  mbssid guest-mode
  wpa-psk ascii 7 0102323E5F1B514968
!
dot11 ssid MOVIL
  vlan 103
  authentication open
  authentication key-management wpa version 2
  mbssid guest-mode
  wpa-psk ascii 7 094F450D4944351F2B
!
dot11 ssid PRENSA
  vlan 102
  authentication open
  authentication key-management wpa version 2
  mbssid guest-mode
```

```
  wpa-psk ascii 7 08751C1D4F50481A21
!
dot11 ssid oculta
  vlan 104
  authentication open
  authentication key-management wpa version 2
  wpa-psk ascii 7 1406050E1E10337A75
!
username Cisco password 7 13261E010803
username cnt privilege 15 secret 5 $1$HoJP$h2c6ALGx7aq232f9.aYFl0
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 102 mode ciphers aes-ccm
!
encryption vlan 103 mode ciphers aes-ccm
!
encryption vlan 104 mode ciphers aes-ccm
!
encryption vlan 101 mode ciphers aes-ccm
!
ssid ENLACE
!
ssid MOVIL
!
ssid PRENSA
!
ssid oculta
!
antenna gain 0
```

```
mbssid
station-role root
!
interface Dot11Radio0.101
encapsulation dot1Q 101 native
no ip route-cache
bridge-group 101
bridge-group 101 subscriber-loop-control
bridge-group 101 block-unknown-source
no bridge-group 101 source-learning
no bridge-group 101 unicast-flooding
bridge-group 101 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface Dot11Radio0.103
encapsulation dot1Q 103
no ip route-cache
bridge-group 103
bridge-group 103 subscriber-loop-control
bridge-group 103 block-unknown-source
no bridge-group 103 source-learning
no bridge-group 103 unicast-flooding
bridge-group 103 spanning-disabled
!
interface Dot11Radio0.104
```

```
encapsulation dot1Q 104
no ip route-cache
bridge-group 104
bridge-group 104 subscriber-loop-control
bridge-group 104 block-unknown-source
no bridge-group 104 source-learning
no bridge-group 104 unicast-flooding
bridge-group 104 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
antenna gain 0
dfs band 3 block
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
```

```
interface GigabitEthernet0.101
encapsulation dot1Q 101
no ip route-cache
bridge-group 101
no bridge-group 101 source-learning
bridge-group 101 spanning-disabled
!
interface GigabitEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
interface GigabitEthernet0.103
encapsulation dot1Q 103
no ip route-cache
bridge-group 103
no bridge-group 103 source-learning
bridge-group 103 spanning-disabled
!
interface GigabitEthernet0.104
encapsulation dot1Q 104
no ip route-cache
bridge-group 104
no bridge-group 104 source-learning
bridge-group 104 spanning-disabled
!
interface BVI1
ip address 10.130.130.2 255.255.255.252
no ip route-cache
!
ip http server
no ip http secure-server
```

ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
password 7 00174312055F0A
login
line vty 0 4
privilege level 15
password 7 011C40094906
login local
!
end
AP_ENLACE#
(Julio, 2016)

Script de programación equipos de telecomunicaciones aplicación práctica 2

Router Mikrotik

/ip firewall filter
add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist action=drop \ comment="drop ftp brute forcers"
add chain=output action=accept protocol=tcp content="530 Login incorrect" dst-limit=1/1m,9,dst-address/1m
add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorrect" \ address-list=ftp_blacklist address-list-timeout=3h
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \ comment="drop ssh brute forcers" disabled=no
add chain=input protocol=tcp dst-port=22 connection-state=new \ src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist \ address-list-timeout=10d comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new \ src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 \ address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 \ action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="" disabled=no

add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list \ address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no

add chain=forward protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop \ comment="drop ssh brute downstream" disabled=no

add action=accept chain=input comment="Aceptar conexiones establecidas" \ connection-state=established disabled=no

add action=accept chain=input comment="Aceptar related conexiones" \ connection-state=related disabled=no

add action=drop chain=input comment="Rechazar conexiones invalidas" \ connection-state=invalid disabled=no

add action=drop chain=input comment="Bloquear Lista SSH" disabled=no \ src-address=!192.168.1.0/24 src-address-list=SSH

add action=drop chain=input comment="Bloquea Lista Telnet" disabled=no \ src-address=!192.168.1.0/24 src-address-list=Telnet

add action=drop chain=forward comment="Bloqueo Lista P2P" disabled=no \ src-address=!192.168.1.0/24 src-address-list="Bloqueo de P2P"

add action=accept chain=input comment="Conexiones desde la red Local" disabled=\ no src-address=192.168.1.0/24

add action=drop chain=input disabled=no src-address-list="Bloqueo de P2P"

add action=drop chain=output disabled=no src-address-list="Bloqueo de P2P"

add action=add-src-to-address-list address-list="Accesos Via Web" \ address-list-timeout=1d chain=input comment="Conexion WebBox" disabled=no \ dst-port=80 protocol=tcp

add action=accept chain=input disabled=no dst-port=80 protocol=tcp

add action=add-src-to-address-list address-list="Winbox Aceptado" \ address-list-timeout=1d chain=input comment=\ "Agrega IPs Que entran por Winbox" disabled=no dst-port=8291 protocol=tcp

add action=accept chain=input disabled=no dst-port=8291 protocol=tcp
add action=log chain=input disabled=no dst-port=8291 log-prefix=\ "Entrada por Winbox" protocol=tcp
add action=accept chain=input comment="Aceptar pings limitados" disabled=no \ protocol=icmp
add action=add-src-to-address-list address-list="Entradas por FTP" \ address-list-timeout=2d chain=input comment=\ "Crea Lista de IPs que entran al FTP" disabled=yes dst-port=21 protocol=tcp
add action=accept chain=input disabled=yes dst-port=21 protocol=tcp
add action=add-src-to-address-list address-list=SSH address-list-timeout=2d \ chain=input comment="Crea Lista de Entradas SSH" disabled=no dst-port=22 \ protocol=tcp
add action=accept chain=input disabled=no dst-port=22 protocol=tcp
add action=add-src-to-address-list address-list=Telnet address-list-timeout=2d \ chain=input comment=ListaTelnet disabled=no dst-port=23 protocol=tcp
add action=accept chain=input disabled=no dst-port=23 protocol=tcp
add action=add-src-to-address-list address-list="Bloqueo de P2P" \ address-list-timeout=1d chain=forward comment=P2P disabled=no p2p=all-p2p \ protocol=tcp
add action=drop chain=forward disabled=no p2p=all-p2p protocol=tcp
add action=drop chain=input disabled=no p2p=all-p2p protocol=tcp
add action=drop chain=output disabled=no p2p=all-p2p protocol=tcp
add action=drop chain=input comment="Bloqueo ATAQUE DNS cache externo" disabled=no dst-port=53 in-interface=WAN protocol=udp

(Julio, 2016)

Monitoreo consumo real de ancho de banda interfaces router.

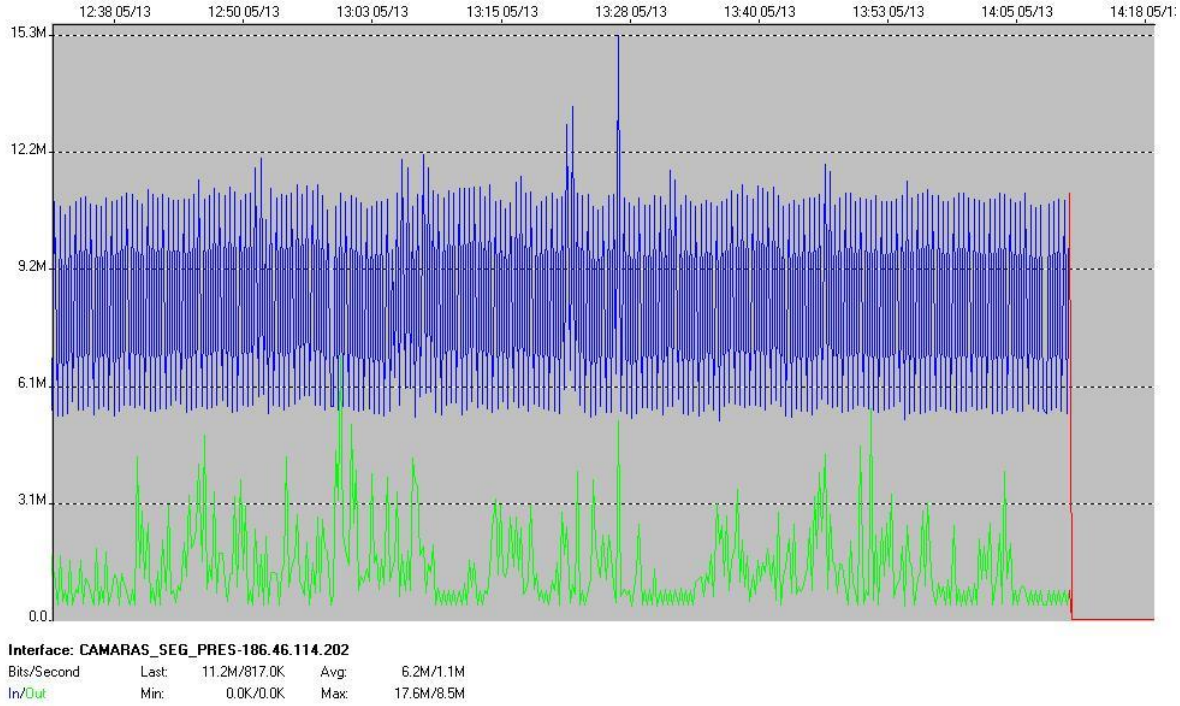


Ilustración 54 monitoreo interfaz video **(Julio, 2016)**

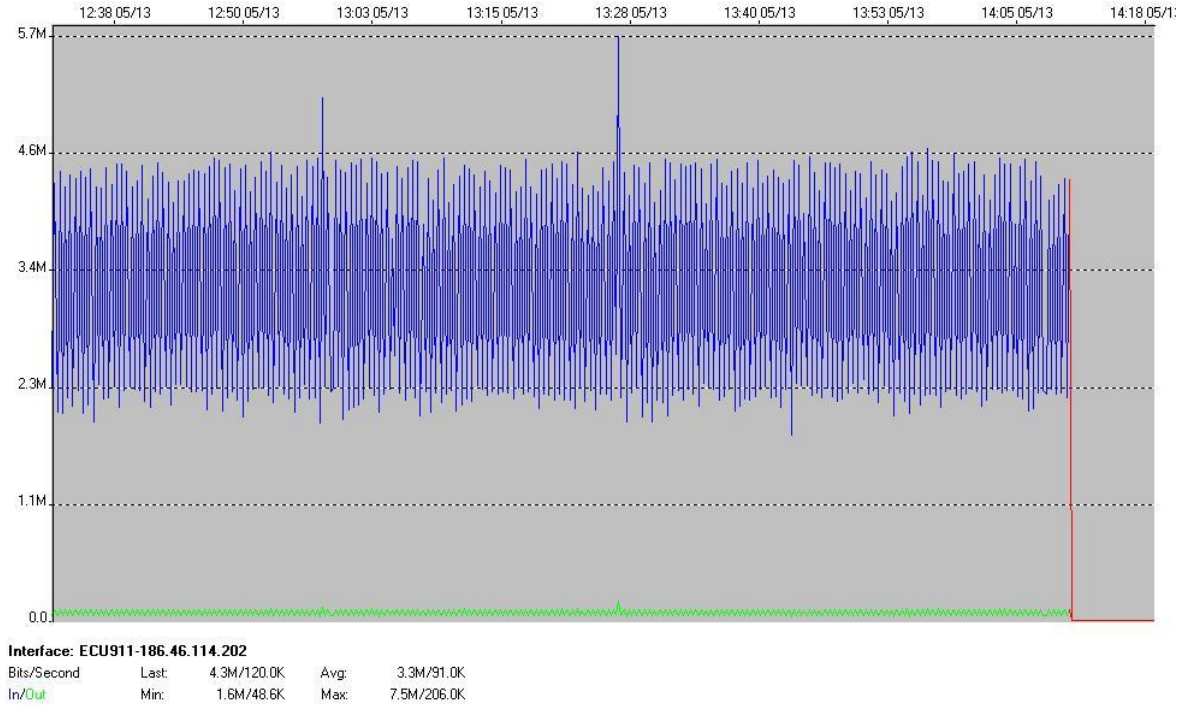


Ilustración 55 monitoreo interfaz vigilancia **(Julio, 2016)**

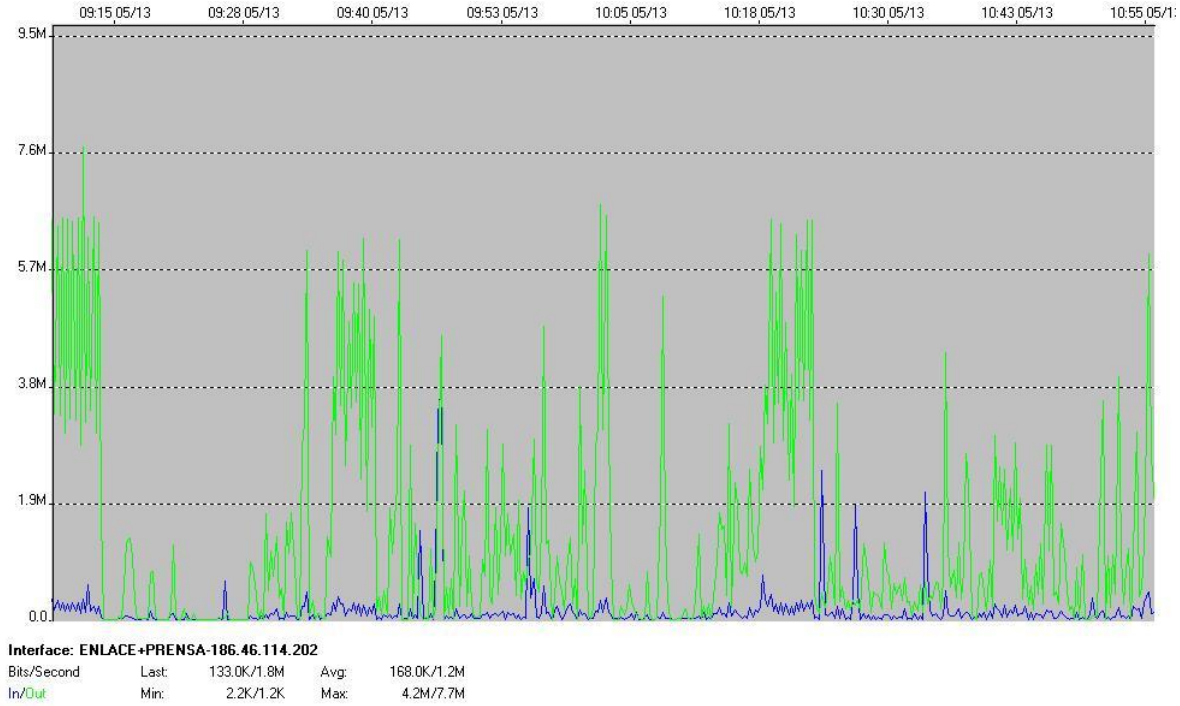


Ilustración 56 monitoreo interfaz prensa **(Julio, 2016)**

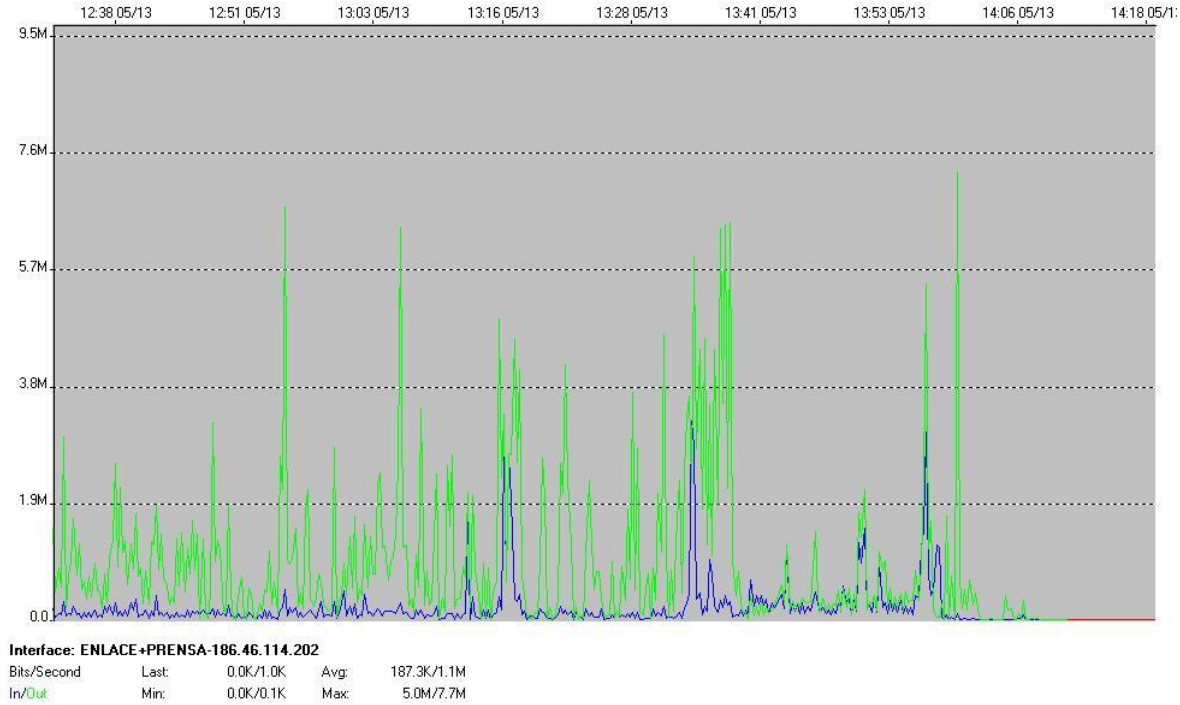


Ilustración 57 monitoreo interfaz prensa dos **(Julio, 2016)**

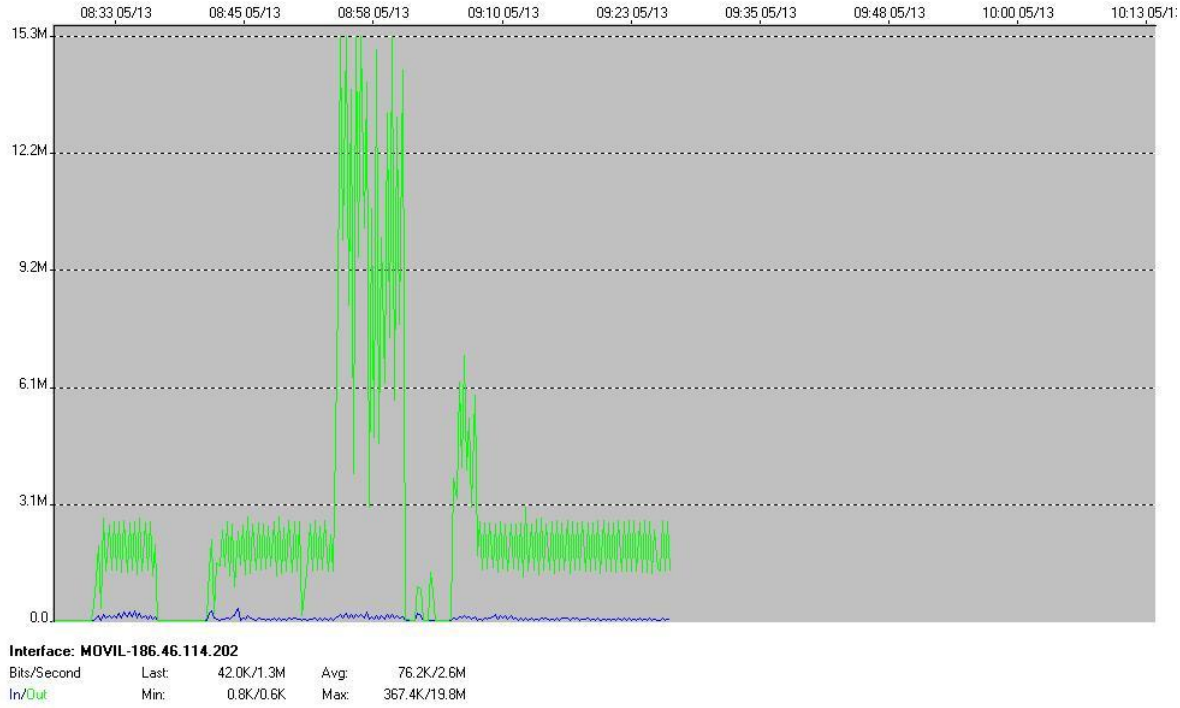


Ilustración 58 monitoreo interfaz móvil **(Julio, 2016)**

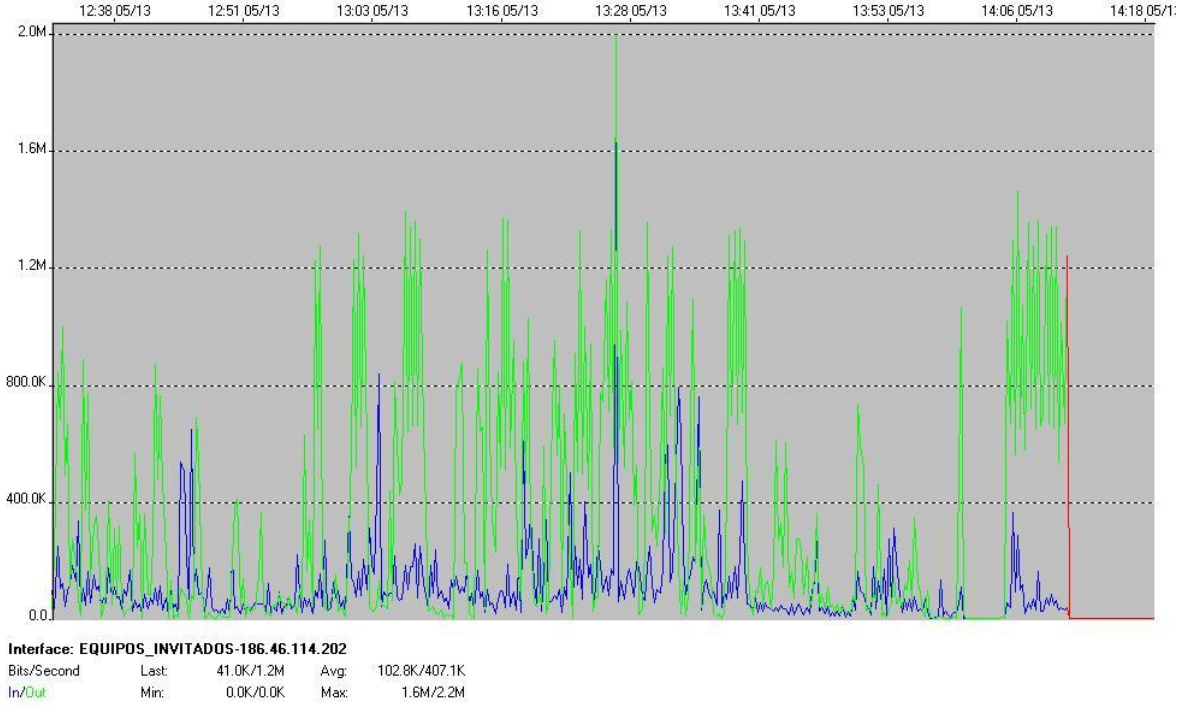


Ilustración 59 monitoreo interfaz dispositivos **(Julio, 2016)**

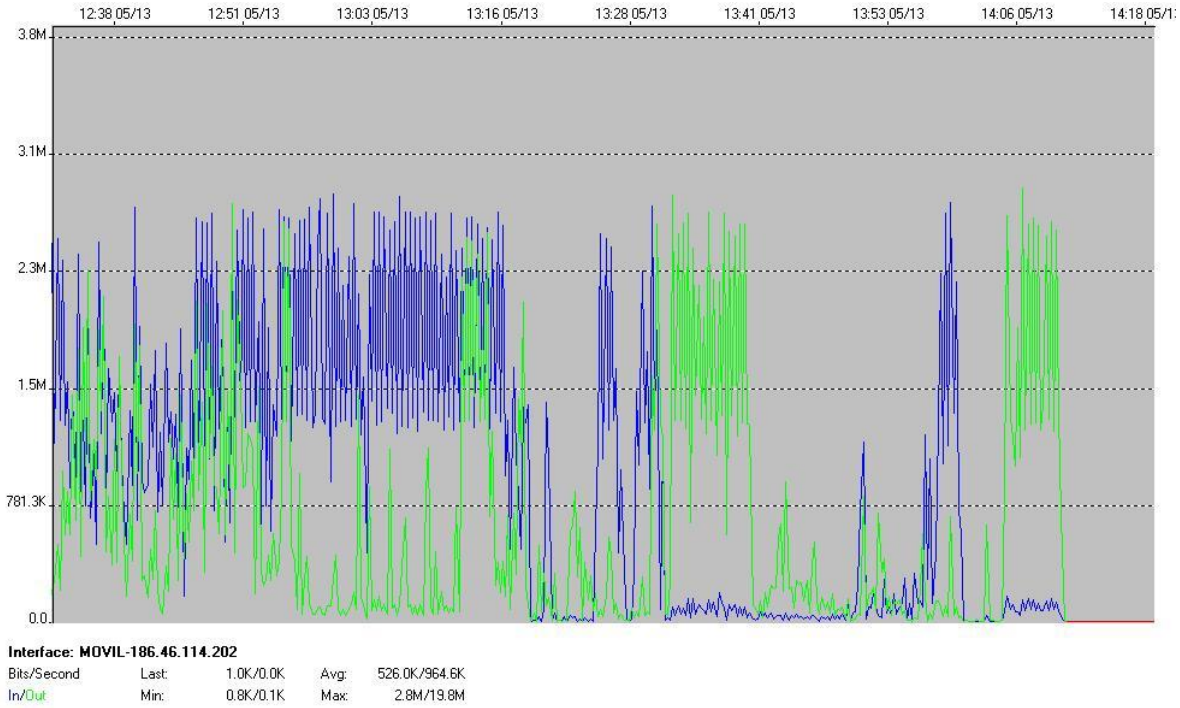


Ilustración 60 monitoreo interfaz móvil dos **(Julio, 2016)**

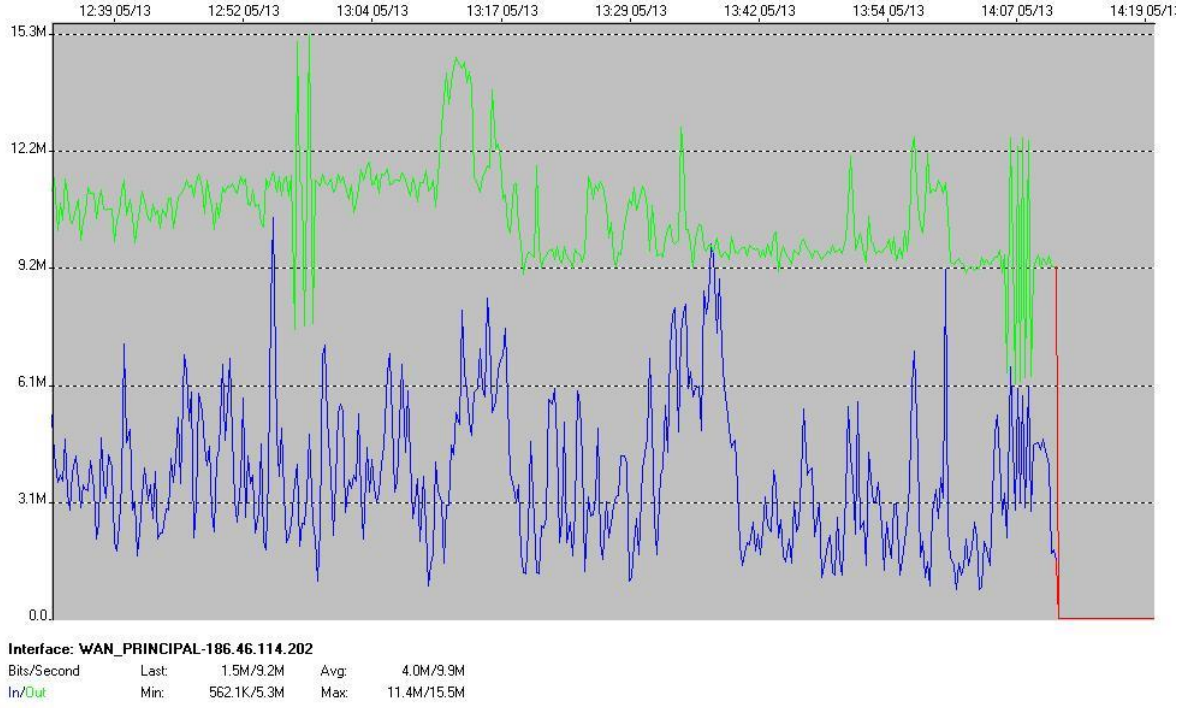


Ilustración 61 monitoreo interfaz wan (Julio, 2016)

Anexo 2

Fotografías de laboratorio soluciones propuestas.

Aplicación práctica 1 implementación infraestructura cisco

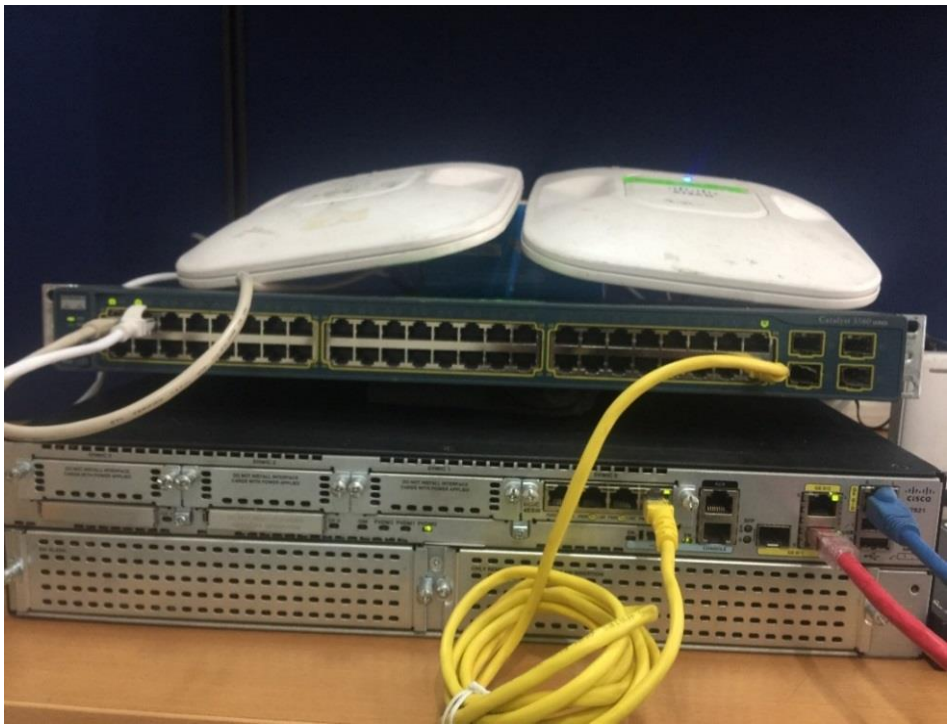


Ilustración 62 Infraestructura uno foto uno **(Julio, 2016)**

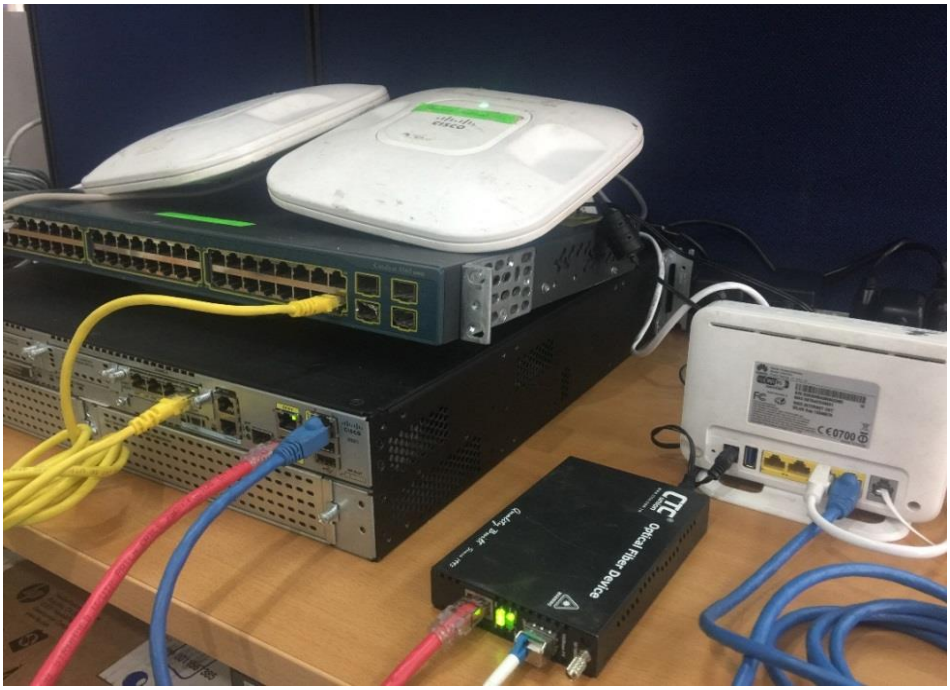


Ilustración 63 Infraestructura uno foto dos **(Julio, 2016)**

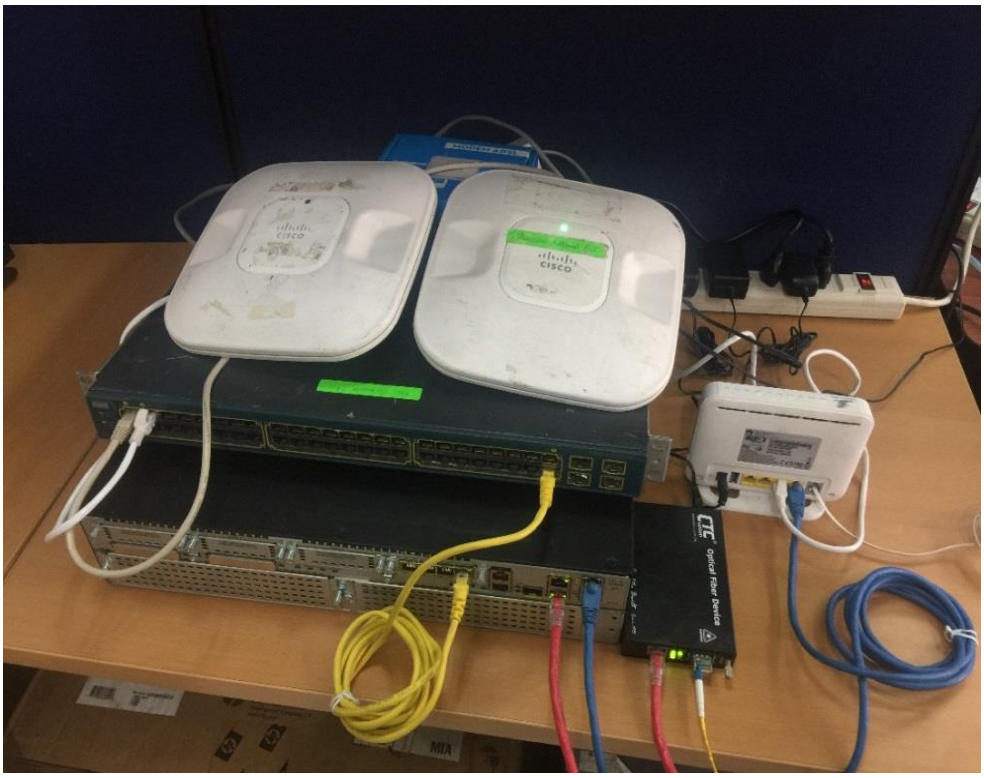


Ilustración 64 infraestructura uno foto tres **(Julio, 2016)**

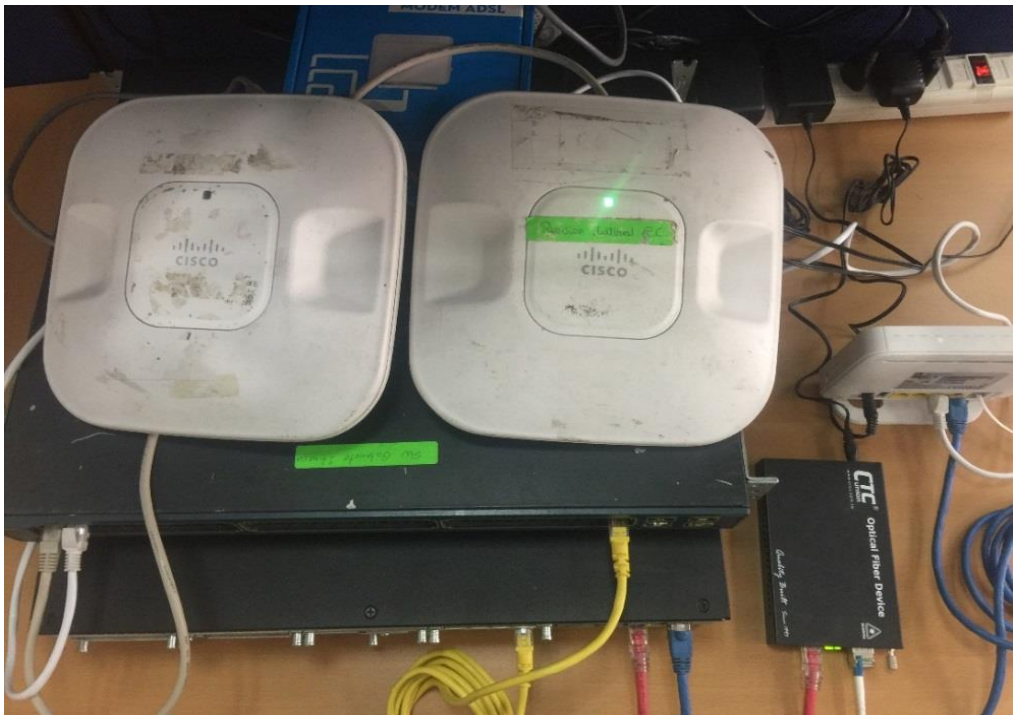


Ilustración 65 infraestructura uno foto cuatro **(Julio, 2016)**

Aplicación práctica 2 implementación alternativa (backup)

Fotografías de laboratorio soluciones propuestas.

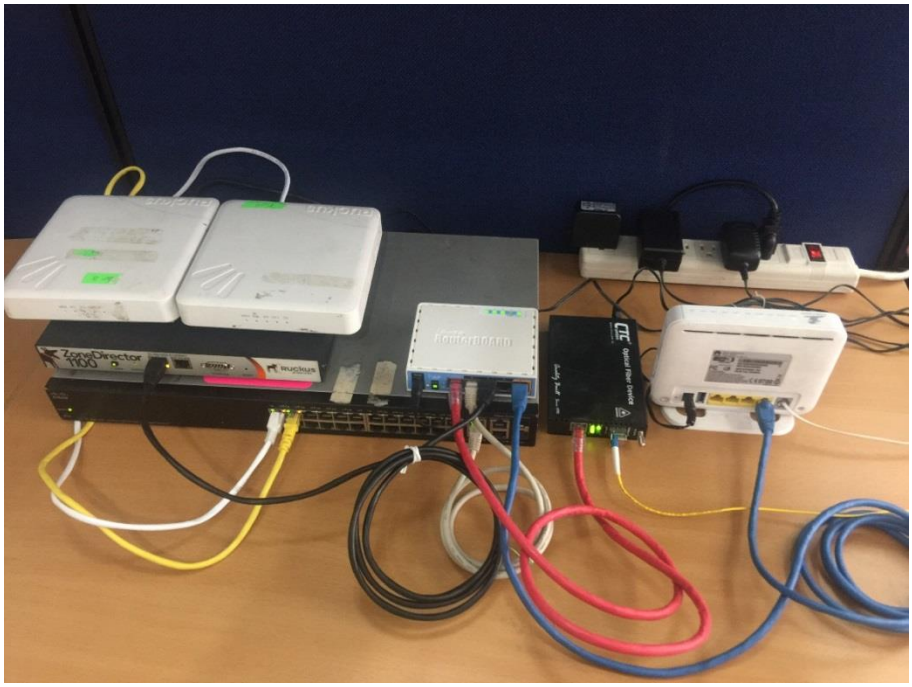


Ilustración 66 infraestructura dos foto uno **(Julio, 2016)**

Ilustración 67 infraestructura dos foto dos **(Julio, 2016)**

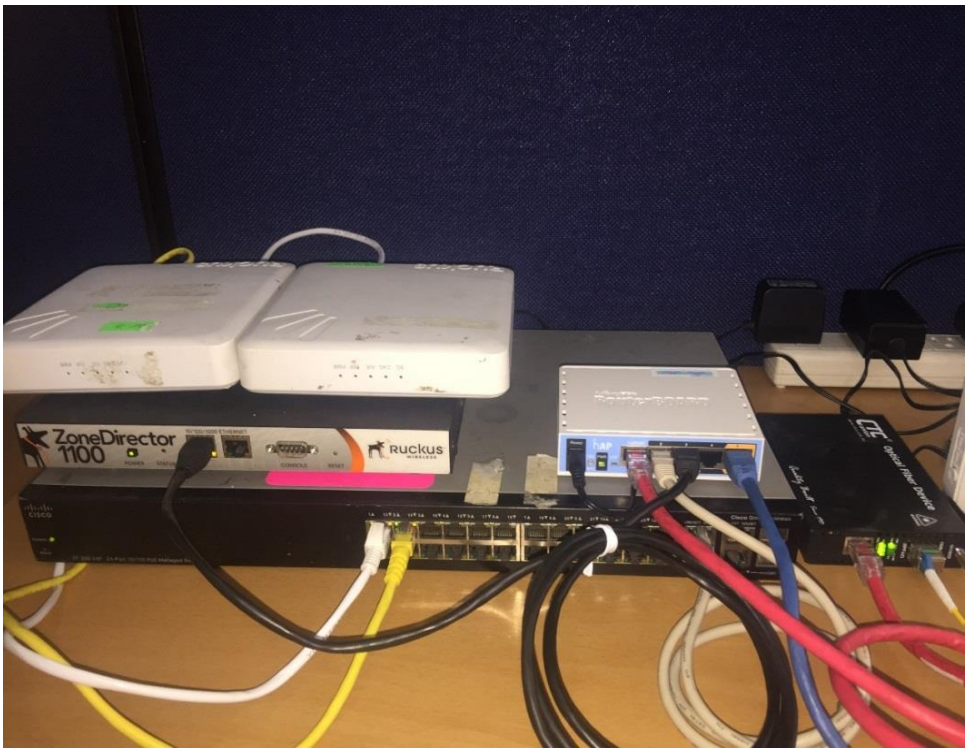


Ilustración 68 infraestructura dos foto tres **(Julio, 2016)**

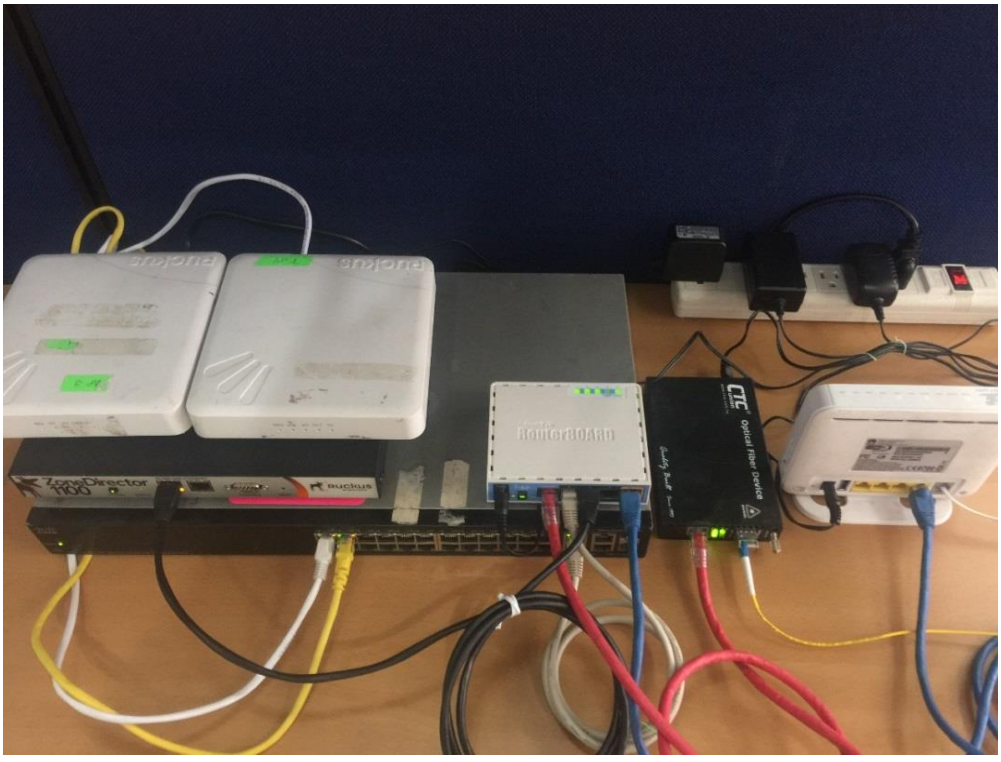
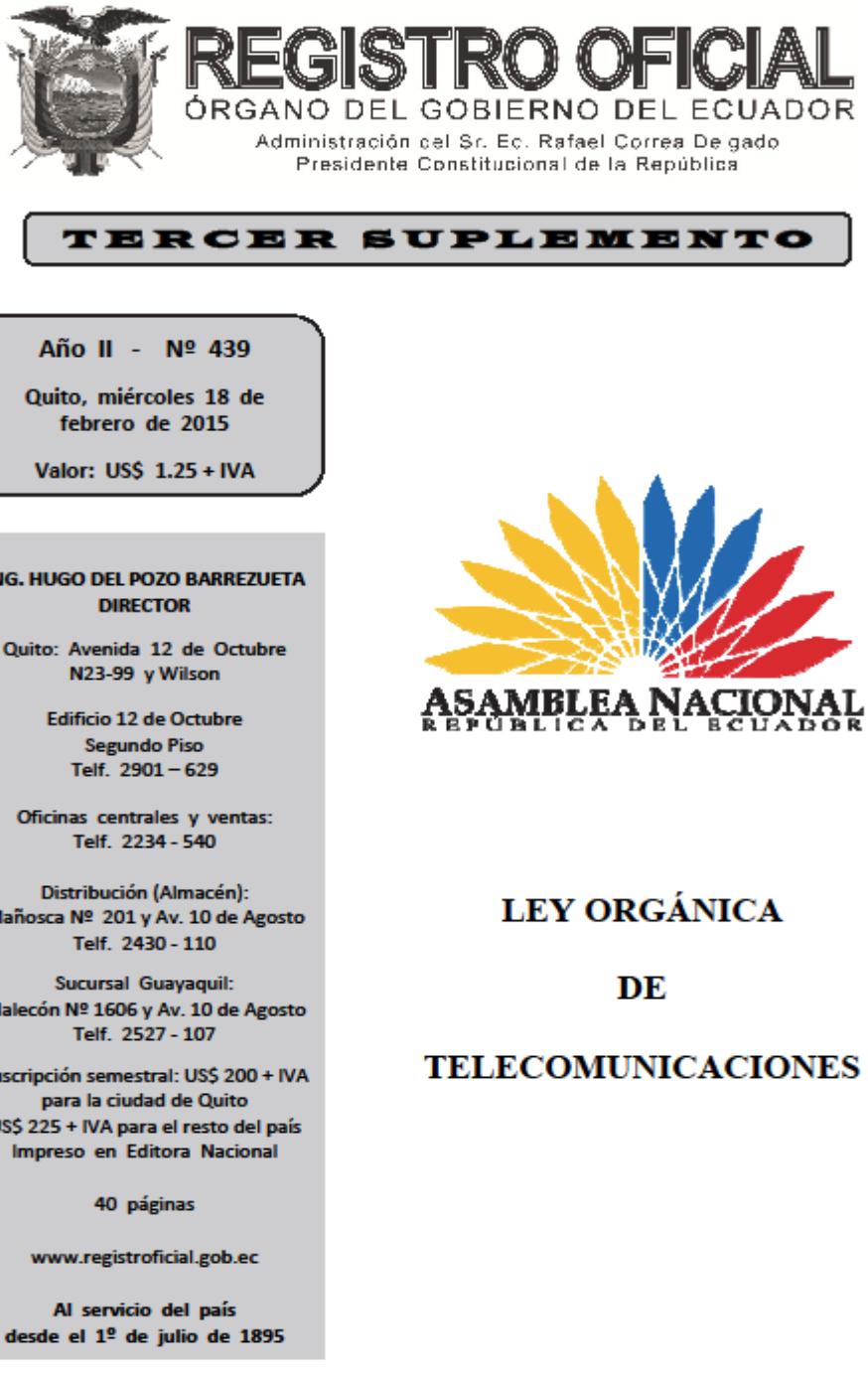


Ilustración 69 infraestructura dos foto cuatro **(Julio, 2016)**

Anexo 3

Ley orgánica de telecomunicaciones Ecuador



REGISTRO OFICIAL
ÓRGANO DEL GOBIERNO DEL ECUADOR
Administración del Sr. Ec. Rafael Correa Delgado
Presidente Constitucional de la República

TERCER SUPLEMENTO

Año II - Nº 439
Quito, miércoles 18 de febrero de 2015
Valor: US$ 1.25 + IVA

ING. HUGO DEL POZO BARREZUETA
DIRECTOR

Quito: Avenida 12 de Octubre N23-99 y Wilson
Edificio 12 de Octubre
Segundo Piso
Telf. 2901 – 629

Oficinas centrales y ventas:
Telf. 2234 - 540

Distribución (Almacén):
Mañosca Nº 201 y Av. 10 de Agosto
Telf. 2430 - 110

Sucursal Guayaquil:
Malecón Nº 1606 y Av. 10 de Agosto
Telf. 2527 - 107

Suscripción semestral: US$ 200 + IVA para la ciudad de Quito
US$ 225 + IVA para el resto del país
Impreso en Editora Nacional

40 páginas

www.registroficial.gob.ec

Al servicio del país
desde el 1º de julio de 1895

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

LEY ORGÁNICA
DE
TELECOMUNICACIONES

(Registro Oficial, 2017)

Anexo 4

Código orgánico integral penal

SUPLEMENTO

Año I - Nº 180

Quito, lunes 10 de febrero de 2014

Valor: US$ 5.00 + IVA

ING. HUGO ENRIQUE DEL POZO BARREZUETA
DIRECTOR

Quito: Avenida 12 de Octubre N 23-990 y Wilson

Edificio 12 de Octubre
Segundo Piso

Dirección: Telf. 2901 - 629
Oficinas centrales y ventas:
Telf. 2234 - 540

Distribución (Almacén):
Mañosca Nº 201 y Av. 10 de Agosto
Telf. 2430 - 110

Sucursal Guayaquil:
Malecón Nº 1606 y Av. 10 de Agosto
Telf. 2527 - 107

Suscripción anual: US$ 400 + IVA
para la ciudad de Quito
US$ 450 + IVA para el resto del país
Impreso en Editora Nacional

144 páginas

www.registroficial.gob.ec

Al servicio del país
desde el 1º de julio de 1895

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

CÓDIGO ORGÁNICO INTEGRAL PENAL

(Registro Oficial, 2017)

PlagScan Resultados del Análisis de los plagios del 2017-08-31 01:12

8.6%

TESIS METODOLOGÍA ISO 27000 PARA OPTIMIZAR RENDIMIENTO DE REDES CORPORATIVAS MEDIANAS MÓVILES MANTENIENDO ESTÁNDARES .docx

Fecha: 2017-08-31 00:55

✱ Todas las fuentes 100 | Fuentes de internet 100

☑	[0]	docplayer.es/2701064-Universidad-tecnica-de-ambato.html 0.0% 69 resultados
☑	[1]	https://documents.mx/documents/cisco-networking-academy-563dc7e70cf59.html 3.0% 38 resultados
☑	[2]	https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf 2.2% 50 resultados
☑	[3]	https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf 0.6% 34 resultados
☑	[4]	https://www.slideshare.net/walterjosequinteroacevedo/cisco-capitulo-1 2.2% 25 resultados
☑	[5]	https://sontusdatos.org/wp-content/uploa...-personales_2014.pdf 0.3% 18 resultados
☑	[6]	https://www.xatakamovil.com/conectividad...jor-para-nuestra-red 0.8% 26 resultados ⊞ 2 documentos con coincidencias exactas
☑	[9]	wireless.cubava.cu/que-son-los-canales-w...or-para-nuestra-red/ 0.8% 26 resultados ⊞ 1 documento con coincidencias exactas
☑	[11]	hemisferio-creativo.blogspot.com/2014/12/que-son-los-canales-wifi-y-como-escoger.html 0.8% 26 resultados
☑	[12]	tesis.pucp.edu.pe/repositorio/bitstream/...NEXOS.pdf?sequence=2 0.1% 14 resultados
☑	[13]	docplayer.es/7705711-Anexo-6-metodologia-de-gestion-del-riesgo.html 0.5% 24 resultados
☑	[14]	www.itesa.edu.mx/netacad/introduccion/course/module1/1.3.2.6/1.3.2.6.html 1.7% 22 resultados ⊞ 1 documento con coincidencias exactas
☑	[16]	https://es.slideshare.net/marojaspe/curso-ai-iso-27001 0.9% 24 resultados
☑	[17]	www.ingenieriasystems.com/2016/07/Presta...NA1-V5-CISCO-C1.html 1.7% 20 resultados
☑	[18]	unpocodetodoqueesmucho.blogspot.com/2013/ 0.7% 20 resultados
☑	[19]	unpocodetodoqueesmucho.blogspot.com/2013/07/ 0.7% 19 resultados ⊞ 1 documento con coincidencias exactas
☑	[21]	www.slideserve.com/limei/iso-27001-2005 0.0% 16 resultados
☑	[22]	www.youblisher.com/p/1023591-Los-Estanda...emas-de-Informacion/ 0.6% 20 resultados
☑	[23]	miordenadorwindows.medaunerror.com/sopor...ecnico.html?start=30 0.3% 18 resultados ⊞ 1 documento con coincidencias exactas
☑	[25]	https://www.slideshare.net/marojaspe/curso-ai-iso-27001 0.7% 21 resultados
☑	[26]	docplayer.es/10616100-Taller-de-gestion-...o-e-informatica.html 0.3% 13 resultados
☑	[27]	docplayer.es/8686431-Anexo-1-glosario-pa...so-guide73-2002.html 0.4% 18 resultados

[28] slideplayer.es/slide/5461036/
0.7% 15 resultados

[29] https://sites.google.com/site/wikinternet666/red-confiable
1.1% 18 resultados

[30] https://itic12sistemasdecalidad.wordpress.com/ensayo-de-investigacion/
0.1% 22 resultados

[31] www.monografias.com/trabajos67/estandar-internacional/estandar-internacional2.shtml
0.4% 17 resultados

[32] https://prezi.com/kpn5ltlmebo_/untitled-prezi/
0.6% 20 resultados

[33] https://es.slideshare.net/ManuelGarcia52/inalambricosexteriores2012v1
0.6% 14 resultados

[34] gestioncalidadiso.blogspot.com/2012/05/sistema-de-gestion-de-la-seguridad-de.html
0.4% 15 resultados

[35] https://interpolados.wordpress.com/tag/calidad/
0.7% 15 resultados

[36] mwndoinformatico.blogspot.com/2016/10/configurar-mi-wifi-en-el-modem-huawei.html
0.0% 12 resultados

[37] https://prezi.com/d7nhosssce5v/interferencias-electromagneticas/
0.4% 12 resultados

[38] 2016redes5cp2g1.blogspot.com/
0.5% 13 resultados

[39] https://interpolados.wordpress.com/tag/arquitectura-de-red/
0.6% 14 resultados

[40] docplayer.es/15522282-Diseno-de-una-rect...lectromagnetica.html
0.6% 12 resultados

[41] www.academia.edu/17289794/240464014-CCNA-1-V5-Resumen-capitulo-1
0.7% 11 resultados

[42] https://prezi.com/doxf6u1mptu-/terminos-y-definiciones-iso-27001/
0.0% 16 resultados

[43] soporteysistemas-amizba.blogspot.com/2015/04/3-que-son-los-canales-wifi.html
0.3% 10 resultados

[44] www.lawebdelyuyo.eu/2014/10/tutorial-elegir-el-canal-wifi-mas.html
0.5% 11 resultados

[45] https://eniacauditorias.wordpress.com/norma-isoiec-17799/
0.4% 13 resultados

[46] www.scd.com.ar/servicios/auditoria_informatica.php
0.4% 12 resultados

[47] https://es.slideshare.net/julian067/glosario-configuracin-router
0.4% 11 resultados

[48] https://tutandem.com/wifi-plus-a-300-mbps-en-nuestra-oficina-compartida-en-las-rozas/
0.4% 9 resultados

[49] arduinoamuete.blogspot.com/2016/
0.4% 10 resultados

[50] https://www.clubensayos.com/Tecnolog%C3%...I-BANCO/1210191.html
0.3% 16 resultados

[51] mastersinfo.weebly.com/uploads/7/5/3/9/7539117/arquitectura_de_la_red.pdf
0.7% 10 resultados

[52] arduinoamuete.blogspot.com/2016/11/esp8266-diagnostico-wifi-y-direccion-mac.html
0.4% 10 resultados
⊞ 1 documento con coincidencias exactas

[54] www.ingenieriasystems.com/2016/06/
0.6% 6 resultados

[55] https://es.slideshare.net/mvum/elba-reyes-16244700
0.2% 12 resultados
⊞ 1 documento con coincidencias exactas

[57] https://prezi.com/1ssnsslzgeb3/agroz-sa/
0.4% 12 resultados

[58] www.ingenieriasystems.com/2016/07/
0.6% 9 resultados

[59] https://sites.google.com/site/cursoenlin...-de-seguridad-de-red
0.6% 8 resultados

[60] https://prezi.com/yny_-d1bsjax/11-dominios-de-la-norma-iso-27001/
0.2% 11 resultados

[61] https://www.slideshare.net/groberth/clase-3-lan-wan-e-internet-redes-convergentes
0.6% 5 resultados

[62] slideplayer.es/slide/10335085/
0.6% 5 resultados

[63] https://www.coursehero.com/file/p2u44kj/...dad-de-los-datos-de/
0.5% 9 resultados

[64] https://www.scribd.com/document/233728460/CAPT-1
0.5% 8 resultados

[65] www.itc.edu.co/es/nosotros/seguridad-informacion
0.1% 13 resultados

[66] https://sites.google.com/site/internet1215/cap-1/otros-conceptos-que-se-deben-conocer
0.5% 5 resultados

[67] https://albinogoncalves.files.wordpress.com/2011/03/05_iso_27001.pdf
0.1% 12 resultados

[68] https://stemesio.files.wordpress.com/2008/09/normas-de-seguridad-gm.pdf
0.2% 10 resultados

[69] https://www.certifiedinfosec.com/es/cyber-security/iso-27001
0.2% 11 resultados

[70] www.ingenieriasystems.com/2016/06/Diagra...NA1-V5-CISCO-C1.html
0.5% 5 resultados

[71] https://smr.iesharia.org/wiki/doku.php/src:ut7:proyectos:tipos
0.3% 8 resultados

[72] ciscobgl.blogspot.com/p/arquitectura-de-internet-ccna.html
0.5% 8 resultados

[73] docplayer.es/32291567-Limitaciones-de-una-conexion-wifi.html
0.3% 8 resultados

[74] https://prezi.com/dnrmo5s_vyel/los-canales-y-frecuencias-en/
0.3% 8 resultados

[75] www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152009000100004
0.1% 10 resultados

[76] https://prezi.com/nndmshfgn6yc/estandare...d-de-la-informacion/
0.2% 7 resultados

[77] https://prezi.com/3tax7xvm23xe/propuesta...gias-de-informacion/
0.1% 10 resultados

[78] https://www.movistar.es/rpmm/estaticos/a...onexion_wifi_440.pdf
0.3% 7 resultados

[79] https://prezi.com/c9c3sob1tixi/analisis-de-riesgo/
0.2% 11 resultados

[80] https://www.csirt.gob.cl/media/2017/05/CSIRT-RCE-2017-FEA.pdf
0.2% 9 resultados

[81] https://sites.google.com/site/vmendillo/tesis_presentadas
0.1% 9 resultados

[82] www.animalpolitico.com/2017/02/corte-auditoria-scjn-informacion/
0.2% 9 resultados

[83] docplayer.es/1054853-Introduccion-a-la-seguridad-informatica.html
0.1% 9 resultados

[84] https://sites.google.com/site/wikinternet666/lan-y-wan
0.4% 4 resultados

[85] https://malwareantivirus.files.wordpress.com/2015/04/iso27001.pdf
0.1% 11 resultados

[86] www.ingenieriasystems.com/2016/07/Amenaz...NA1-V5-CISCO-C1.html
0.4% 6 resultados

[87] docplayer.es/36198380-Trabajo-de-grado-especializacion-gestion-integrada-qhse.html
0.1% 6 resultados

[88] www.buenastareas.com/ensayos/Iso-27001/32611597.html
0.1% 7 resultados

[89] www.youblisher.com/p/171883-Metodologia-...s-de-Bases-de-Datos/
0.3% 6 resultados

[90] https://interpolados.wordpress.com/tag/firewall/
0.4% 6 resultados
⊞ 1 documento con coincidencias exactas

[92] www.iso27000.es/download/doc_otros_estandar_all.pdf
0.1% 6 resultados

[93] https://prezi.com/_7oglhz-z57m/diseno-de-la-antena-yagi-uda/
0.1% 4 resultados

[94] https://sites.google.com/site/wikinternet666/seguridad-de-red
0.3% 6 resultados

[95] https://microfulio.wordpress.com/2011/02/25/interntet-seguridad/
0.3% 6 resultados

[96] https://prezi.com/evekqxuwnqsh/manual-de...d-de-la-informacion/
0.0% 9 resultados

[97] docplayer.es/15177537-Ley-organica-de-telecomunicaciones.html
0.4% 11 resultados

[98] www.mallafre-consultors.cat/es
0.1% 6 resultados

[99] www.telsur.cl/internet/wifi/servicio-wifi
0.1% 3 resultados

[100] grupoelemclase.blogspot.com/
0.3% 5 resultados
⊞ 1 documento con coincidencias exactas

[102] https://nandyromero.wordpress.com/
0.4% 9 resultados

[103] https://prezi.com/kstf6dclgqhi/copy-of-magerit/
0.1% 8 resultados

[104] https://www.clubensayos.com/Temas-Variados/Seguridad-De-La-Informacion/377683.html
0.0% 7 resultados

[105] https://www.slideshare.net/VinnyPaute/ley-organica-de-telecomunicaciones
0.4% 9 resultados

[106] tecno-actualidad.blogspot.com/2010/02/auditoria-de-sistemas-interna-externa.html
0.3% 4 resultados

[107] https://prezi.com/tzrofeovqrbp/estandar-internacional-27001/
0.1% 7 resultados

[108] https://artzeizdeandres.wordpress.com/2013/02/05/redes-inalambricas-wlan/
0.2% 6 resultados
⊞ 2 documentos con coincidencias exactas

[111] https://sites.google.com/site/internet1215/cap-1/tendencias-de-red
0.3% 5 resultados

141 páginas, 19723 palabras

⚠ Se detectó un color de texto muy claro que podría ocultar caracteres utilizados para combinar palabras.

Nivel del plagio: 8.6%

208 resultados de 112 fuentes, de ellos 112 fuentes son en linea.

Configuración

Directiva de data: *Comparar con fuentes de internet, Comparar con documentos propios*
Sensibilidad: *Media*
Bibliografia: *Considerar Texto*
Deteción de citas: *Reducir PlagLevel*
Lista blanca: --

Ilustración 70 Análisis PLAGSCAN