# PROPUESTA DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL DE ACCESO UTILIZANDO LA PLATAFORMA DE CISCO – CNAC (CISCO NETWORK ADMISSION CONTROL) EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA (COLOMBIA)

**ALEXA MARÍA RAMÍREZ ARDILA**

**Ingeniera de Sistemas – Especialista en Telecomunicaciones**


**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB**
**FACULTAD DE INGENIERÍA**
**MAESTRÍA EN TELEMÁTICA - MODALIDAD INVESTIGACIÓN**
**GRUPO DE INVESTIGACIÓN - TECNOLOGÍAS DE INFORMACIÓN (GTI)**
**LÍNEA EN TELEMÁTICA**
**BUCARAMANGA, SANTANDER, COLOMBIA**
**JULIO DE 2016**

# PROPUESTA DE UNA GUÍAMETODOLÓGICA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL DE ACCESO UTILIZANDO LA PLATAFORMA DE CISCO – CNAC (CISCO NETWORK ADMISSION CONTROL) EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA (COLOMBIA)

**ALEXA MARÍA RAMÍREZ ARDILA**
**Ingeniera de Sistemas – Especialista en Telecomunicaciones**

**Trabajo de grado para optar al título de Maestría en Telemática, en modalidad Investigación**

**Director:**
**Magíster José Gregorio Hernández Sánchez**

**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB**
**FACULTAD DE INGENIERÍA**
**MAESTRÍA EN TELEMÁTICA - MODALIDAD INVESTIGACIÓN**
**GRUPO DE INVESTIGACIÓN - TECNOLOGÍAS DE INFORMACIÓN (GTI)**
**LÍNEA EN TELEMÁTICA**
**BUCARAMANGA, SANTANDER, COLOMBIA**
**JULIO DE 2016**

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

**Bucaramanga, Julio 2016**

## AGRADECIMIENTOS

Agradezco a Dios, por haberme permitido culminar esta etapa profesional de mi vida, sin EL, nada de esto hubiera sido posible.

A la Universidad Autónoma de Bucaramanga por haberme brindado las instalaciones para llevar a cabo mi proyecto de grado

A mi director, el Ingeniero José Gregorio Hernández, quien con su amplio conocimiento en el área, fue pilar fundamental en la realización de cada una de las etapas de éste proyecto. Infinitas gracias “Jose”.

A mis asesores pedagógicos, ingenieros Jorge Andrick Parra y José Daniel Cabrera, por haberme orientado, corregido y apoyado en mi labor científica con un interés y una entrega que sobrepasaron las expectativas que como alumna pude tener. A ellos, mi más grande admiración por una vida dedicada a la investigación.

A la Ingeniera Johana Manrique, por haberme brindado sus orientaciones en el campo de los motores de búsqueda. Joa, mil gracias.

A Todos, Muchas Gracias por haber hecho parte de este gran proceso llamado Proyecto de Grado.

# DEDICATORIA

Dedico este proyecto, inicialmente a mi hija María Angélica, quien con su ternura y amor me apoyó durante cada uno de los momentos difíciles que tuve que pasar en la realización de este proyecto, sin su apoyo nada de esto hubiera sido posible.

A mi madre, quien por su dedicación y entrega incondicional ha sido uno mis mayores motores en todas las realizaciones profesionales de mi vida.

A Robert, por su amor incondicional, quien siempre estuvo allí apoyándome no solo emocionalmente sino profesionalmente.

A mis hermanos y hermanas, quienes siempre estuvieron allí para animarme a continuar y de los cuales siempre recibí palabras de aliento y satisfacción.

A todos y cada uno, mil gracias y los amo con todo mi corazón.

# PROPUESTA DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL DE ACCESO UTILIZANDO LA PLATAFORMA DE CISCO – CNAC (CISCO NETWORK ADMISSION CONTROL) EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA (COLOMBIA)

Alexa María Ramírez Ardila
José Gregorio Hernández Sánchez (Director)
Grupo de Investigación en Tecnologías de Información - GTI
Línea de Investigación Telemática
Programa de Maestría en Telemática
Universidad Autónoma de Bucaramanga – UNAB (Colombia)

## RESUMEN

Uno de los principales problemas que enfrentan las organizaciones hoy en día son los diversos ataques que sufren sus infraestructuras de red, por motivos tales como, conexiones de equipos infectados, robos de identidad, de información, entre otros. Las redes modernas deben contar con software y hardware especializado que garantice seguridad en la conexión cableada e inalámbrica de los usuarios, almacenamiento y a su vez recuperación de la información que se requiera.

El propósito de este proyecto era proponer una guía metodológica para la implementación de políticas de control de acceso en los equipos cisco de la UNAB mediante el análisis e identificación que se realizó a la arquitectura CNAC. Esta guía lleva por nombre **Guía Metodológica para implementar políticas de seguridad en una infraestructura de red Cisco basada en la solución propietaria *Cisco Network Asset Collector* (CNAC)** y su contenido se puede verificar en el anexo 7.

El presente proyecto presenta un enfoque cualitativo inductivo por la diversidad en su contenido. Para realizar la guía de implementación, el proceso se dividió en etapas sucesivas y sistemáticas; en cada una de ellas se trató de establecer objetivos y metas claras con productos entregables, donde los productos resultado de la primera etapa, sirvieron para adelantar la segunda y los de la segunda sirvieron para proseguir con la tercera etapa y así sucesivamente.

Finalmente, en este proyecto se realizó una síntesis de trabajos similares hechos en Colombia y otras partes del mundo, en donde se pudo evidenciar que son pocos los trabajos de grado que muestran una guía para implementar políticas de control de acceso, adicional, se realizó un diagnóstico de los equipos cisco de la UNAB y por último se describieron las orientaciones y el proceso de implementación de la guía.

**PALABRAS CLAVE:**
Redes de Computadores, Seguridad, Telemática, Redes Informáticas, Políticas de Seguridad, Protocolos, Tecnología de la información, Telecomunicaciones, Diagnóstico, Guías Metodológicas, Control de Acceso a Redes, Análisis y evaluación de riesgos, Estándar ISO.

# OFFER ABOUT A METHODOLOGICAL GUIDE FOR SETTING ACCESS CONTROL POLITICS BY USING CISCO PLATFORM CNAC AT AUTONOMA DE BUCARAMANGA UNIVERSITY (COLOMBIA)

Alexa María Ramírez Ardila
José Gregorio Hernández Sánchez (Director)
Research Group in Information Technology - GTI
Telematics Research Line
Autónoma de Bucaramanga University – UNAB (Colombia)

## ABSTRACT

Nowadays; one of the most difficult problems Organizations must face are the different attacks they suffer into their own infrastructures on nets; for diverse reasons such as infected equipment's connections, identity thefts, information and more the modern nets must have a specialized software and hardware to guarantee all kind of security (wire or wireless) and also the storage and recuperation of data and information the user can need at any time.

The intention of this project is to offer a Methodological guide for setting access control in cisco equipments at UNAB University by means of the analysis made on CNAC architecture where this guide has the name of: Methodological guide to set security politics on cisco net infrastructure based on the owner solution **Cisco Network Asset Collector (CNAC)** its content can be verified on annexe number seven (7).

This project presents a qualitative inductive approach because of the diversity of its content. To elaborate the implementation guide all the process was divided into systematic stages each one was directed to set clear skills to reach with deliverable products where in this exact process the result of the products generated on first stage were used to develop the second step and these ones were used to continue to the third stage and it was a continuous process of progress.

Finally in this project it was made a synthesis about similar works made in Colombia and other parts of the world; where we realized that there are so few thesis that show and offer a guide to set an Access control guide. Additional it was made a diagnose on cisco UNAB equipments and finally it was described the orientations and horizon on how to set the guide to get the results of protection.
.

KEYWORDS:
Computer Networks, Security, Telematics, Networking, Security Policies, Protocols, Information Technology, Telecommunications, Diagnosis, Methodological Guide, Network Access Control, Analysis and Risk Assessment, ISO Standard.

**CONTENIDO**

**pág.**

## LISTA DE FIGURAS

**pág.**

## LISTA DE CUADROS

**pág.**

## LISTA DE ANEXOS

**pág.**

## LISTA DE ACRÓNIMOS

| | |
|---|---|
| **AAA Server:** | Authentication, Authorization, and Accounting Server) |
| **ACL:** | Access Control List |
| **ACS:** | Access Control Server |
| **AD:** | Active Directory |
| **APT:** | Advanced Persistent Threats |
| **AS:** | Auditory Server |
| **AVS:** | Posture Validation Server |
| **BYOD:** | Bring Your Own Device |
| **CNAC:** | Cisco Network Asset Collector |
| **CTA:** | Cisco Trust Agent |
| **DHCP:** | Dinamic Host Configuration Protocol |
| **DNS:** | Domain Name Server |
| **DoS:** | Denial of Service |
| **FTP:** | File Transfer Protocol |
| **IP:** | Internet Protocol |
| **ISE:** | Identity Services Engine |
| **ISO:** | International Organization for Standardization |
| **LAN:** | Local Area Network |
| **MDM:** | Mobile Device Management |
| **NAC:** | Network Access Control |
| **NAD:** | Network Access Device |
| **NAT:** | Network Address Translation |
| **QoS:** | Quality of Service |
| **SMTP:** | Simple Mail Transfer Protocol |
| **WAN:** | Wide Area Network |

# INTRODUCCIÓN

En la actualidad, las empresas y organizaciones requieren cada vez más la actualización de su infraestructura de red para proporcionar y soportar servicios de misión crítica de manera rápida y efectiva (Kim, Ahn, Lim, & Mun, 2005). A medida que las empresas crecen y evolucionan, contratan más empleados, abren sucursales y se expanden a los mercados globales, lo cual afecta directamente los requisitos de la red empresarial. Así mismo, aumentan los requerimientos de los usuarios en cuanto al uso y aprovechamiento de los recursos de la red y las expectativas que se tienen de la misma, y para cumplir con ello, las arquitecturas subyacentes necesitan cumplir con cuatro características básicas e importantes (Cisco Academy Networking, 2012).

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

La seguridad es un aspecto primordial en la implementación y administración de red y se ha hecho evidente que con la evolución de las empresas y el acceso mediante dispositivos móviles y no-móviles de los diferentes tipos de usuarios, cambiaron también los requerimientos de seguridad de la misma. La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes, los cuales podrían traer consecuencias graves si se pone en peligro su integridad, como las interrupciones de la red que impiden la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios; el robo de propiedad intelectual (ideas de investigación,

patentes y diseños) y uso por parte de la competencia; hacer pública la información personal o privada de los usuarios sin su consentimiento; mala orientación y pérdida de recursos personales y comerciales, la pérdida de datos importantes cuyo reemplazo requiere un gran trabajo y finalmente, la denegación del servicio (DoS) que son la forma más promocionada de ataques y también están entre los más difíciles de eliminar. Debido a su fácil implementación y al daño potencialmente significativo, los ataques de DoS merecen especial atención de los administradores de seguridad, los cuales pueden ser mitigados utilizando listas de control de acceso en la definición de políticas de seguridad.

Existen dos tipos de problemas de seguridad que deben tener en cuenta los administradores de una red: la seguridad de su infraestructura de red y la seguridad de la información.

La seguridad de una infraestructura de red, incluye el aseguramiento físico de los dispositivos que proporcionan conectividad de red tales como, *Switches y Routers* y a su vez la implementación de políticas de seguridad para prevenir el acceso no autorizado al software de administración que reside en ellos. La seguridad de la información se refiere a, proteger la información que contienen los paquetes que se transmiten por la red y la información almacenada en los dispositivos conectados a la red, aplicando barreras y procedimientos que resguarden los datos y solo se permita acceder a ellos a las personas que cumplan con los requisitos establecidos en dichas políticas.

Al analizar esta vulnerabilidad, es necesario implementar medidas y técnicas de seguridad en redes para proteger la información y recursos, éstas deben ser proporcionales a lo que se intenta proteger como son: servidores Web, servidores de correo, protocolos de transferencia de archivos (FTP), bases de datos o cualquier tipo de red, en donde también, se pretende crear manuales los cuales están encaminados al uso adecuado de estas nuevas tecnologías, con recomendaciones

para obtener las mejores ventajas y no realizar un mal uso de las nuevas tecnologías que se dispone.

Estas nuevas tecnologías permiten asegurar de manera lógica la información de una organización, la cual se almacena en dispositivos de la red y es movida a través de su infraestructura. Una de estas tecnologías es el control de acceso a la red; según Frias-Martínez, Stolfo y Keromytis (2008), tiene como objetivo, asegurar que todos los dispositivos que se conectan a las redes corporativas cumplan con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, entre otros problemas, mediante la implementación de una fase previa a la conexión a la red, en donde el estado del dispositivo final se comprueba por medio de la configuración de un conjunto de políticas establecidas antes de ser concedido el acceso a la red y una fase posterior a la conexión que examina si el dispositivo cumple con las políticas que corresponden a su papel dentro de la red.

La necesidad de implementar tecnologías de control de acceso para autenticar dispositivos y usuarios que requieren conectarse a redes corporativas, ha impulsado a diferentes organizaciones privadas y públicas a ofrecer soluciones para estas necesidades. Algunas de estas organizaciones son Cisco Systems y Microsoft.

La red de la Universidad Autónoma de Bucaramanga – UNAB ha tenido un crecimiento constante y acelerado, para cumplir con los requerimientos que demanda la organización, soportando tanto los procesos académicos y administrativos de misión crítica, como de acceso a recursos internos y externos (internet) para la comunidad universitaria en general, la cual utiliza para este acceso conexiones cableadas o inalámbricas, con dispositivos de la universidad o propios, lo que ha incrementado la posibilidad de presentarse diversos problemas de seguridad.

En vista de lo anterior, la UNAB requiere la implementación de políticas de seguridad robustas que le permitan tener un control más efectivo y eficiente en las conexiones de redes cableadas e inalámbricas, utilizando para ello tecnologías de control de acceso, particularizadas para el tipo de equipo que conforma su infraestructura. Para ello, se requiere inicialmente diseñar una metodología que permita la implementación de NAC en la infraestructura de red Cisco de la UNAB, en donde se realice un estado del arte actual de su infraestructura, se recopilen las políticas que se requieran implementar y se proponga la infraestructura requerida para lograr su implementación.

Para cumplir con lo anterior, el presente documento se organiza de la siguiente manera: En primer lugar se encuentra el problema, la pregunta y la hipótesis de investigación, en esta sección se habla sobre el problema que existe sobre las medidas de seguridad informática empleadas por las organizaciones, la formulación del problema y la hipótesis que podría dar solución al problema planteado. En segundo lugar se encuentran los objetivos planteados (uno general y tres específicos), en esta sección se habla sobre el objetivo general planteado y los objetivos específicos que darán cumplimiento al desarrollo efectivo del objetivo general. En tercer lugar se encuentra el Marco Referencial el cual contiene el Marco Conceptual, Marco Teórico, Estado del Arte y Marco Legal. En esta sección se habla sobre todos los conceptos y definiciones que tienen relación con los temas de seguridad informática, control de acceso y control de acceso a redes corporativas, de igual manera contiene los referentes legales requeridos para implementar estas tecnologías y las consultas bibliográficas que hicieron posible la realización del proyecto. En cuarto lugar se encuentra la Descripción del proceso investigativo; en esta sección se habla sobre la metodología implementada y los diferentes métodos utilizados. Como quinto lugar están los resultados; en esta sección se encuentran cada uno de los resultados obtenidos los cuales cumplen con los objetivos específicos planteados inicialmente, finalmente y como sexto lugar se encuentran las conclusiones y recomendaciones obtenidos a lo largo del trabajo de

investigación sobre la implementación de políticas de seguridad utilizando la plataforma de control de acceso a la red de Cisco.

# 1. PROBLEMA, PREGUNTA E HIPÓTESIS DE INVESTIGACIÓN

El presente capítulo tiene el propósito de describir el problema, pregunta e hipótesis de la investigación realizada.

## 1.1 PROBLEMA DE INVESTIGACIÓN

El aumento masivo de usuarios que se conectan a las redes corporativas y que buscan acceder a sus diversos servicios, es una de las causas por la cual las empresas se han visto en la obligación de actualizar sus infraestructuras de red, con el fin de garantizar calidad de servicio y seguridad para acceder a aplicaciones tales como el correo electrónico, mensajería instantánea, descarga y actualización de contenidos, juegos en línea, entre otros, ya sea por conexión cableada o inalámbrica. Las redes modernas deben contar con *software* y *hardware* especializado que garantice seguridad en la conexión de los usuarios, almacenamiento y recuperación de la información que se requiera. (Frias-Martinez, Stolfo, & Keromytis, 2008).

En cuanto a seguridad de las redes, se han desarrollado tecnologías de Control de Acceso a la Red – NAC (por sus siglas en inglés *Network Access Control*) que permiten a las empresas admitir o denegar el acceso de usuarios y reducir las amenazas en la red (Frias-Martinez, Stolfo, & Keromytis, 2008). Sin embargo, no todas las empresas cuentan con un sistema de seguridad robusto que les permita identificar las características de *hardware* y *software* de los dispositivos que intentan conectarse, controlar ataques maliciosos y proveer alta calidad de servicio para

obtener el máximo aprovechamiento de los recursos de la red (Ahn, Lim, Mun, & Kim, 2005).

A nivel regional, la Universidad Autónoma de Bucaramanga – UNAB como empresa de carácter privado, cuenta con un sistema de red cableada segmentado por medio de VLANs que permiten separar los dominios de Broadcast y ofrecer seguridad de acceso de tráfico entre VLANs, para las áreas académicas y administrativas. El direccionamiento es privado y se ofrece acceso a internet controlado por medio de Proxys implementados en sistemas SQUID sobre Linux. Por otra parte, el tráfico desde y hacia Internet se controla por medio de protocolos que permiten configurar Listas de control de acceso - ACLs (por sus siglas en inglés *Access Control List*) y la asignación de direcciones IP con *Network Access Translation* - NAT, gestionado a través del *Switch* Core. En el *router* se encuentran definidas algunas políticas que cierran los puertos 1 a 1024 dejando abiertos exclusivamente los puertos bien conocidos de aplicaciones.

La autenticación en la red a nivel de aplicativos se controla mediante un servidor OpenLDAP que se encarga de realizar las funciones de *Single Site On - SSO* de la mayoría de aplicativos que requieren autenticación, entre estos el acceso a la red inalámbrica. Además, la UNAB cuenta con un servidor WSUS Windows que permite la actualización de los parches de seguridad críticos de los sistemas operacionales *Windows* de los PCs de forma centralizada, y consolas que permiten la actualización de Antivirus de escritorio evitando la consulta de los agentes de actualización a través de Internet.

Sin embargo, la UNAB requiere la implementación de políticas de seguridad robustas que le permitan tener un control más efectivo y eficiente en las conexiones de redes cableadas e inalámbricas. Por otra parte, requiere de un sistema de gestión que permita la administración de políticas de forma centralizada de tal forma que se puedan distribuir dentro de la infraestructura Cisco.

De lo anterior, nace el planteamiento del presente proyecto, el cual tiene como objetivo principal diseñar una guía metodológica para implementar políticas de control de acceso basadas en la arquitectura de Cisco, *Network Access Control* - CNAC en la infraestructura de red de la UNAB.

## 1.2 PREGUNTA DE INVESTIGACIÓN

Es por esto que surge la pregunta investigativa: ¿Puede y cómo puede una guía metodológica para implementar políticas de control de acceso a la red contribuir a reducir la vulnerabilidad en cuanto a la negación de los servicios de red tales como DNS, Proxys, DHCP, HTTP, Canales Internet y manejar perfilamiento de usuarios a través de la infraestructura de red de la UNAB?

## 1.3 HIPÓTESIS

El diseño de una guía metodológica para la implementación de políticas de control de acceso a la red ayudaría a reducir el nivel de vulnerabilidad en cuanto a la negación de los servicios de red, Canales Internet, perfilamiento en la infraestructura de red de la UNAB ya que se podría controlar el acceso de los dispositivos mediante una autenticación y diagnóstico inicial el cual permitiría detectar si el equipo que requiere acceso a la red cumple o no con las condiciones requeridas en las políticas implementadas.

# 2. OBJETIVOS

El presente capítulo tiene el propósito de describir el objetivo general y específicos de la investigación realizada.

## 2.1 OBJETIVO GENERAL

Proponer una guía metodológica que permita la implementación de NAC (Network Access Control) en la infraestructura de red de la Universidad Autónoma de Bucaramanga como una contribución para reducir el nivel de vulnerabilidad de la red y manejo de perfilamiento de usuarios.

## 2.2 OBJETIVOS ESPECÍFICOS

- Elaborar un documento que contenga la revisión de la literatura sobre seguridad en redes empresariales y control de acceso a la red.
- Diagnosticar el estado de los equipos Cisco que tiene la UNAB en donde se implementará NAC.
- Diseñar una guía metodológica para la implementación de la solución NAC en los equipos Cisco de la UNAB.

# 3. MARCO REFERENCIAL

El presente marco referencial está constituido por: el marco conceptual en donde se describe los conceptos claves del proyecto; el marco teórico en donde se describen las teorías encontradas sobre guías metodológicas y control de acceso a la red; el estado del arte en donde se pueden identificar los diferentes autores que han realizados trabajos de investigación relacionados con el tema de estudio y por último el marco legal en donde se encuentran las leyes referentes a seguridad informática, protocolos de autenticación y *Network Access Control*.

## 3.1 MARCO CONCEPTUAL

Para poder comprender los diferentes alcances de este proyecto, se deben comprender los conceptos relacionados con el control de acceso a las redes y con seguridad informática.

**3.1.1 Red de Área Local (LAN).** Una red de área local es un grupo de equipos que se encuentran conectados entre sí y pertenecen a la misma ubicación geográfica la cual es de tamaño pequeño (Tanenbaum, 2003).

**3.1.2 Infraestructura de red.** El termino infraestructura de red está diseñado para nombrar a una organización que utiliza la informática y otros dispositivos electrónicos para facilitar el trabajo de red y la navegación de internet (Kurose, Ross, & Hierro, 2010).

**3.1.3 Seguridad Informática.** Es un estado de cualquier tipo de información (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo (Moya & Martínez, 2005).

**3.1.4 Denegación de servicios:** Se produce cuando una atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica o cableada, impidiendo a los usuarios legítimos de ésta, disponer de esos servicios (Pellejero, Andreu, & Lesta, 2006).

**3.1.5 Análisis de riesgos.** El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo (López, 2010).

**3.1.6 Vulnerabilidad informática.** De acuerdo a P.A. López (2010), las vulnerabilidades son las probabilidades que existen de que una amenaza se materialice contra un activo.

**3.1.7 Control de acceso.** Es el proceso de conceder permisos a usuarios o grupos y poder conocer quienes están autorizados para acceder a los sistemas de información y recursos. Su concepto se resume en tres pasos que son: identificación, autenticación y autorización, gracias a estos principios y con el buen uso de los mismos el administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema.

**3.1.8 Control de acceso a la red (NAC).** NAC es un concepto que controla el acceso a la red y el uso de recursos de red en función de autenticación del usuario,

el comportamiento del dispositivo final, y una evaluación de identidad y seguridad las propiedades del dispositivo (Maiwald, 2012).

**3.1.9 Servicio de Autenticación.** Son medidas dirigidas a garantizar que la persona o la maquina es quien dice ser. Por medio de este servicio se protege contra el ataque de suplantación de personalidad en la cual una entidad remota se hace pasar por alguien que no es (Comer & Suominen, 2002).

**3.1.10 Remediación.** Es un componente de una solución de gestión de recuperación que funciona en combinación con un servidor de recuperación para actualización de software cliente específico, tales como parches del sistema operativo.

**3.1.11 Cuarentena.** Es el estado que se coloca a un host cuando no cumple las políticas de control requeridas para su conexión a la red local.

**3.1.12 Cisco Network Asset Collector (CNAC).** Cisco NAC es una solución para el control de acceso a la red, cuya arquitectura es propietaria, que permite autenticar, autorizar, evaluar y remediar posibles vulnerabilidades, antes de permitir que los usuarios se conecten en la red, conexiones que pueden ser alámbricas, inalámbricas, accesos remotos, etc., es decir, se identifica a los dispositivos, computadores portátiles, computadores de escritorio y otros activos que sean autorizados, compatibles y que cumplan con la política, antes de permitir el acceso (Cisco Systems, Inc., 2009).

**3.1.13 Implementación.** Es el proceso que requiere de las unificaciones de fases previas a la elaboración del proyecto a ejecutar (Tur, 2009).

**3.1.14 Guía metodológica.** Es un documento estructurado que tiene un orden lógico consecutivo de fases y etapas para desarrollar o implementar un Sistema

Integral, en donde la terminación de una fase puede servir como insumo o entrada para poder desarrollar la siguiente fase (Vogt & Johnson, 2011).

**3.1.15 Diagnóstico.** Etimológicamente diagnóstico proviene de gnosis: conocer y a través: así entonces significa: conocer a través o conocer por medio de. Sin embargo, diversos autores que abordan este tema van más allá de su raíz etimológica, algunos entendiéndolo como resultado de una investigación, o como una explicación de una situación particular o como una descripción de un proceso, o como un juicio interpretativo, o bien sólo un listado de problemas con un orden de prioridades: así entonces, es necesario pasar a revisar algunas definiciones al respecto. Scarón de Quintero (1985) afirma que "el diagnóstico es un juicio comparativo de una situación dada con otra situación dada" ya que lo que se busca es llegar a la definición de una situación actual que se quiere transformar, la que se compara, valorativamente con otra situación que sirve de norma o pauta.

## 3.2 MARCO TEÓRICO

Con relación a las diferentes teorías que se han escrito sobre las implementaciones de la solución de control de acceso a las redes corporativas se pueden mencionar las siguientes:

Helfrich, D., Frazier, J., Ronnau, L., y Forbes, P. (2006), definen el proceso de implementación y configuración de cada uno de los componentes de la arquitectura NAC de Cisco, iniciando por la identificación de cada uno de ellos y finalizando con el proceso de configuración que se debe realizar en cada dispositivo, adicional a esto, muestra la importancia de implementar este tipo de soluciones para proteger las infraestructuras de red de las organizaciones. Helfrich muestra en detalle la

solución pero no menciona las políticas que se deben tener en cuenta al momento de su implementación.

Headquarters, C. (2005), proporciona una guía para la implementación de control de admisión a la red (NAC). Este documento es un trabajo en conjunto de todos los colaboradores de la industria y patrocinado por Cisco Systems. En él, se describen las consideraciones de implementación y procedimientos de configuración de dispositivos que actúan como NAD con software Cisco IOS. Proporciona directrices de instalación para el Cisco Trust Agent (CTA) en los equipos cliente de Microsoft Windows. También proporciona instrucciones de configuración de Cisco Secure ACS, incluyendo la configuración de los productos de software antivirus. De la misma manera se puede observar una vez analizado el documento no se mencionan las políticas de seguridad generales que se deben tener en cuenta al momento de implementar la solución.

Icontec (2007) define las normas que se deben tener en cuenta con respecto a la tecnología de la información, sus técnicas de seguridad y los códigos de práctica para la gestión de la seguridad de la información.

La Organización Internacional de Estandarización (2013) definió los siguientes estándares para la administración de la seguridad de información y las técnicas de seguridad que se deben considerar al momento de implementar soluciones de control de acceso a las redes internas de una organización. Estos estándares son: ISO/IEC 27001, ISO/IEC 27002 - ISO/IEC 27003 - ISO/IEC 27004 y ISO/IEC 27005. Estos estándares son mencionados en cada una de las literaturas que manejan como tema principal de investigación el Control de Acceso a Redes como soluciones propietarias o libres.

Acevedo, Castañeda, y Martínez (Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática.), presenta los avances de las

investigaciones adelantadas sobre el cálculo del retorno de la inversión en seguridad informática, para lo cual se ha revisado la evolución de la seguridad de la información, los conceptos generales de la seguridad informática y los elementos asociados con el retorno de la inversión, los cuales serán utilizados para plantear una alternativa para la estimación del ROI. Termina su investigación con una guía metodológica propuesta para el fin ya descrito anteriormente.

En la actualidad, la seguridad informática ha adquirido gran incremento, por las cambiantes condiciones y las nuevas plataformas de computación que se dispone.

La posibilidad de interconectarse a través de redes, ha abierto nuevos espacios que permiten investigar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados como son que las organizaciones dependen de la presencia de internet, que es uno de los principales motivos que provocan riesgos de seguridad, porque permite acceder a la información y a los recursos de manera no autorizada.

Al analizar esta vulnerabilidad es necesario implementar medidas y técnicas de seguridad en redes para proteger la información y recursos, estas deben ser proporcionales a lo que se intenta proteger como son: servidores web, servidores de correo, FTP, base de datos o cualquier tipo de red. En el presente marco de referencia se cita la literatura requerida para el estudio y posterior diseño de una guía metodológica para implementación de políticas de control de acceso a la red.

Los temas que se tuvieron en cuenta en la revisión de la literatura y que se presentan de manera detallada en el presente marco teórico son:

- Seguridad en Redes
- *Bring Your Own Device*
- Control de Acceso

- Control de Acceso a Redes
- *Cisco Network Admission Control* – CNAC

**3.2.1 Seguridad en redes.** Seguridad en redes es mantener bajo protección los recursos y la información con la que cuenta la red a través de procedimientos basados en políticas de seguridad de control de acceso para tener un control adecuado de acceso a la red (Manual de Seguridad en Redes).

La seguridad de la red se inicia con la autenticación del usuario, generalmente con un nombre de usuario y una contraseña para mantener bajo protección los recursos y la información con que se cuenta en la red, a través de una serie de procedimientos basados en una política de seguridad que permitan el control. Cabe recalcar que no existe una seguridad absoluta, lo que se intenta es minimizar el riesgo (Cisco Networking Academy, 2009).

Las tecnologías de seguridad ofrecen diversas soluciones con el fin de proteger la red contra robo o uso incorrecto de la información. Cuando no existe ningún tipo de seguridad implementada, la organización se enfrenta a accesos no autorizados que trae como consecuencia largos periodos de inactividad de red, interrupción del servicio, incumplimiento de las normativas e incluso a acciones legales (Manual de Seguridad en Redes).

Según la Organización Internacional para la Estandarización (ISO) (2013) y con respecto a la Seguridad de Información, en todas sus formas (automatizada o automatizada, formalizada o no formalizada, pública o reservada, etc.) es uno de los principales activos de cualquier organización, necesaria para el normal funcionamiento y el alcance de los objetivos tratados dentro de la misma.

El subcapítulo de seguridad en redes se divide en:

- Tipos de seguridad
- Principales servicios de seguridad
- Análisis de riesgos
- Vulnerabilidad
- Amenazas y
- Mecanismos de seguridad

**3.2.1.1 Tipos de Seguridad.** La seguridad informática se plantea desde dos enfoques distintos aunque complementarios:

**La Seguridad Física:** Puede asociarse a la protección del sistema ante las amenazas físicas mediante la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

**La Seguridad Lógica**: Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas mediante el enmascaramiento de la misma usando técnicas de criptografía. Igualmente, se realiza aplicación de barreras para resguardar el acceso a los datos y solo puedan acceder a ellas personas autorizadas. Con respecto a este tipo de seguridad son varias las técnicas aplicadas entre las que se en encuentran; el control de acceso, la autenticación, la encriptación, el *firewall* y el antivirus, entre otros.

***3.2.1.2 Principales Servicios de Seguridad.*** Los principales servicios básicos de seguridad y en los cuales mencionan en sus apartados Nakhjiri y Nakhjiri (2005)son: Autenticación, Confidencialidad, Integridad, Control de acceso, No repudio y Anonimato. Para poder entender un poco más este concepto y su importancia, se detallan a continuación cada uno de estos servicios.

- **Servicio de Autenticación de Datos**

De acuerdo a Carreño Gallardo (2004), el servicio de autenticación de datos, son medidas dirigidas a garantizar que la persona o la maquina es quien dice ser. Por medio de este servicio se protege contra el ataque de suplantación de personalidad donde una entidad remota se hace pasar por alguien que no es.

Teniendo en cuenta lo anterior, es considerable recalcar las distintas situaciones de autenticación:

**Autenticación de Entidad.** Es el proceso cuando una entidad se conecta al sistema y debe demostrar su identidad, esta autenticación se puede llevar a cabo en diferentes características tales como la entidad que verifica a través de una clave o con cualquier otro tipo de información que posea quien intenta comunicarse.

**Autenticación de Origen de Datos**. Se da cuando en una transferencia de datos como por ejemplo en correo electrónico, solamente se quiere demostrar que los datos han sido originados por una determinada entidad.

Estas teorías conllevan a que se diferencien dos tipos claros de autenticación, una simple y una fuerte; en la autenticación simple solo uno de los participantes está en obligación de demostrar su identificación basada en contraseñas o palabras claves. Un ejemplo de este tipo de autenticación podría ser el siguiente:

Ejemplo. La entidad A trata de probar su identidad, envía a la entidad B su nombre significativo y un testigo de autenticación T este testigo se construye a través de un nombre y una contraseña pass-A todo protegido mediante una función unidireccional f1. Para que el esquema funcione el nombre significativo debe ser “claro” y la entidad B conozca y tenga almacenada la contraseña de A en la base de datos. Para que la contraseña sea almacenada con seguridad se debe proteger

con una función unidireccional que lo que almacene sea una función del testigo de autenticación, es decir mientras no se comprueba que el valor recibido coincide con el valor almacenado no se dará valido el proceso de autenticación.

Con respecto a la autenticación fuerte, cada uno de los participantes en la conexión debe suministrar las respectivas credenciales de autenticación. Existen diferentes casos de autenticación fuerte entre los que se encuentran: Autenticación unidireccional, Autenticación mutua o bidireccional y Autenticación tridimensional. La Autenticación unidireccional consiste en que solo uno de los participantes que forman parte de la comunicación deben demostrar su identidad, la Autenticación bidireccional consiste en que en ambos sentidos deben demostrar su identidad y la Autenticación tridimensional ayuda a reforzar mediante mecanismos de seguridad la autenticación bidireccional.

- **Servicio de Confidencialidad de los datos**

Carreño Gallardo (2004), menciona que la confidencialidad de los datos, proporciona protección para evitar que los datos sean revelados a usuarios no autorizados, señala que este proceso garantiza que los datos sean entendidos solo por destinatarios autorizados, es decir, si la información es robada no sea posible entender su significado. Con este servicio, se puede garantizar que la información que circula a través de las redes esté disponible para usuarios legítimos.

- **Servicio de Integridad de los datos**

A diferencia del servicio de confidencialidad, este servicio garantiza que los datos recibidos por el receptor coincidan exactamente con los enviados por el emisor, garantiza que la información no sea modificada, añadida, sustraída, es decir, el receptor detectará si se ha producido un ataque a la información y podrá aceptar los datos recibidos o simplemente rechazarlos (Carreño Gallardo, 2004). Este servicio

debe garantizar que la información sea fiable y que no ha sido modificada, es decir que la información no ha sido copiada, modificada, borrada en su origen o durante su trayecto. Se debe tener en cuenta que es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida no sólo debe estar almacenada en el computador sino que se deben considerar elementos menos obvios como respaldos y documentación. Esto implica modificaciones causadas por errores de *hardware y/o software*, causadas de forma intencional y de forma accidental. Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

- **Servicio de no Repudio**

Otro de los principales servicios de seguridad, es el de no repudio, el cual proporciona garantías respecto a la emisión y recepción de la información y sirve para evitar que algún participante niegue haber formado parte de ésta (Aguilera López, 2010). Dentro de los casos de no repudio se mencionan los siguientes:

**No repudio con prueba de origen.** El receptor que envía el mensaje adquiere una prueba del origen de la información recibido, por tanto el emisor no puede negar que envió información porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío y esto evita que el emisor niegue el envío.

**No repudio con prueba de envío.** El receptor o emisor adquiere una prueba que no podrá negar que recibió el mensaje con la fecha y hora. Este servicio proporciona al emisor la prueba de que el destinatario del envío, realmente lo recibió, evitando que el receptor lo niegue.

**No repudio con prueba de entrega**. El emisor adquiere una prueba demostrando a terceras personas que el receptor adecuado recibió el mensaje sin inconvenientes.

- **Servicio de control de acceso**

Este tipo de servicio, sirve para evitar el uso no autorizado de los recursos de la red, es decir, permite que solo personas autorizadas puedan tener acceso a una máquina y que cada usuario tenga los permisos de acuerdo a sus funciones. Según Cisco Systems (2014), este servicio se implementa bajo la autenticación en la que el usuario demuestra quien dice ser para poder acceder a los privilegios y restricciones correspondientes. En el control de acceso se presenta en dos servicios que son: (1) El acceso a servidores de todo tipo base de datos, impresoras, servidores, es decir, el usuario accede de forma cliente – servidor y deben identificarse para acceder de acuerdo a los servicios que requiera, (2) El acceso a terminales desde lo que el usuario se conecta a la red. En algunos casos estos servicios se conectan utilizando el servicio de autenticación, teniendo en cuenta que al comprobar que el usuario es quien dice ser, se le aplican los privilegios que le fueron otorgados y las restricciones. Otros casos pueden ser por medio de credenciales que consiste en asignar privilegios independientes de la identidad.

- **Servicio de Anonimato**

Aguilera López (2010), define el servicio de anonimato, como aquel que se encarga de ocultar la identidad de la persona ante actores que forman parte de dichas operaciones. Menciona que de acuerdo a las características de la información, en algunas situaciones se recomienda mantener en anonimato dichos datos.

**3.2.1.3 Análisis de Riesgos.** Todas las organizaciones, ya sean públicas o privadas, formales e informales, se crean y se mantienen con unos objetivos determinados. Todos los posibles eventos que puedan afectar de manera negativa el cumplimiento de estos objetivos pueden considerarse infinitos. Estos eventos pueden tener origen interno y externo y tener diferentes naturalezas, entre las que

se encuentran, riesgo financiero, riesgo económico, riesgo tecnológico y de seguridad de la información.

De acuerdo al estándar 27005 (2011) el análisis de riesgo es una herramienta que permite identificar, clasificar y valorar los eventos que puedan interferir con la obtención de los objetivos propuestos y establecer las medidas necesarias para reducir el riesgo de amenaza que se pueda dar por cada una de las vulnerabilidades encontradas.

**3.2.1.4 Vulnerabilidad.** Son las posibilidades que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la presencia de un factor que pueda posibilitar una amenaza o un ataque. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización. De acuerdo a una de las clasificaciones, los tipos de vulnerabilidades que pueden presentarse a nivel informático son: Vulnerabilidad física, Vulnerabilidad natural, Vulnerabilidades del *hardware*, Vulnerabilidades del software, Vulnerabilidad Humana, entre otras. (International Organization for Standardization - ISO, 2013). La vulnerabilidad física se relaciona con el acceso físico al sistema, se refiere a las instalaciones de los equipos de cómputo que forman parte de la organización. La vulnerabilidad humana suele presentarse cuando el personal realiza malas prácticas de las políticas de acceso al sistema, utilizando medios de almacenamiento para extraer información. La vulnerabilidad natural se refiere al grado en el que el sistema se puede ver afectado por este tipo de desastres, la vulnerabilidad se presenta por deficiencias de medidas de seguridad para afrontar los desastres. Algunos ejemplos podrían ser: la baja ventilación y mala calefacción. La vulnerabilidad de hardware presenta la probabilidad de que las piezas del sistema fallen, dejando el sistema inoperable y

propenso a amenazas y ataques, es decir, trata de cómo las personas pueden utilizar el *hardware* para atacar y finalmente, la vulnerabilidad de *software* puede ocurrir por errores en la programación, o en el diseño.

**3.2.1.5 Amenazas.** Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento que puede producir un daño material o inmaterial sobre los elementos de un sistema, en el caso de la Seguridad Informática, son los elementos de información. Las amenazas pueden ser causadas por usuarios, programas maliciosos, errores de programación, intrusos, personal técnico interno, fallos electrónicos, catástrofes naturales, entre otros (SANS, 2000). En internet existen muchas personas que se dedican a robar información, pueden ser personas de la misma organización o externa, estas pueden robar información y los administradores pueden quizá darse cuenta luego de semanas o meses, esto trae como consecuencia perdidas de dinero, clientes.

Las amenazas pueden tener diferentes orígenes y su clasificación se realiza en 6 tipos diferentes: Amenazas humanas, Amenazas de *Hardware*, Amenazas de *Software*, Amenazas de Red, Amenazas de Seguridad y Amenazas de Desastres Naturales (Carreño Gallardo, 2004).

Con respecto a las amenazas humanas, las personas son la fuente principal de amenaza en las que se invierte más recursos para controlarlos y equilibrar sus consecuencias. En la siguiente tabla de pueden ver los diferentes tipos de amenazas humanas:

Cuadro 1. Tipos de amenazas humanas

| Amenaza | Descripción |
|---|---|
| Curiosos | Ingresan al sistema sin autorización, motivados por aprender, curiosidad, desafío personal, se debe tener bastante cuidado porque pueden causar daño no intencional, incluso, perdidas económicas. |
| Intrusos | Se encarga de ingresar al sistema con un objetivo fijo, se debe tener precaución porque estas personas tienen la experiencia, la capacidad y herramientas para ingresar al sistema sin importar el nivel de seguridad que posea. |
| Personal enterado | Personal que tiene acceso autorizado puede ser personal que labora en la actualidad o ex empleados que lo pueden hacer por rencores personales o motivados por el dinero. |
| Terrorista | Causar daño para diferentes fines. |
| Robo | Extraer información en alguna unidad de almacenamiento, robo físico de hardware para otros fines. |
| Sabotaje | Consiste en reducir la funcionalidad del sistema por medio de acciones que impidan el normal funcionamiento por tanto daño de los equipos, interrupción de los servicios, en algunos casos provocando la destrucción completa del sistema. |
| Fraude | Actividad que tiene como fin aprovechar los recursos para obtener beneficios ajenos a la organización. |
| Ingeniería social | Obtener información social a través de la manipulación a los usuarios legítimos impulsándolos a revelar información sensible. De esta manera los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra antes que aprovechar de los agujeros de seguridad de los sistemas. |

Fuente: Autor del proyecto

Otra de las principales amenazas y que hace parte de esta clasificación son las de *hardware*, las cuales se dan por las fallas físicas ya sea defectos de fabricación o mal diseño de *hardware* que forma parte del sistema de cómputo. En la Figura **1** se pueden observar los diferentes tipos de amenazas de *hardware*.

Figura 1. Tipos de amenazas de hardware

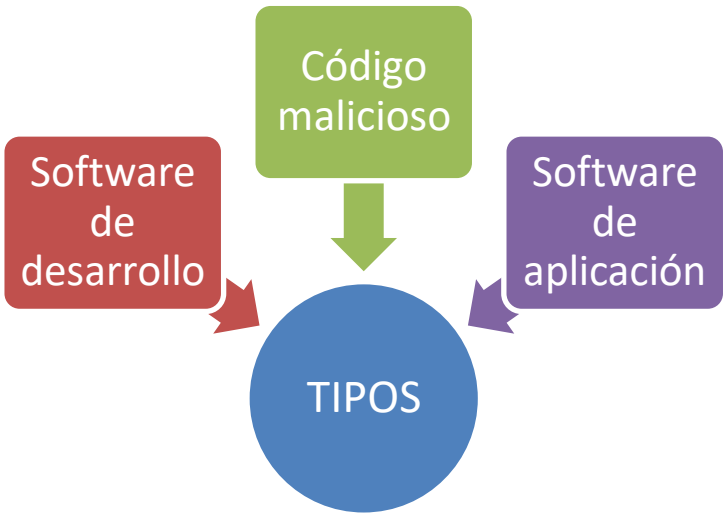

Fuente: Autor del proyecto

Cuando se habla de mal diseño, se dice que los componentes de *hardware* del sistema no cumplen con los requerimientos necesarios; en cuanto a los errores de fabricación, tiene imperfecciones de fabricación y fallas en el momento de usarse, esto trae consecuencias negativas a la organización y a los fabricantes. Las variaciones de voltaje en el suministro de energía provocan daños en los dispositivos, es por esta razón que se deben revisar las instalaciones de energía que proporcionan el voltaje que se requiere de acuerdo a la vida útil de los dispositivos. Con respecto al desgaste se debe tener en cuenta que debido al uso de los dispositivos, con el tiempo tienden a perder sus capacidades técnicas; finalmente, el descuido y el mal uso son factores de importancia los cuales consideran los parámetros establecidos por los fabricantes, tales como: tiempo de uso, periodos y procedimientos de mantenimiento.

Continuando con la clasificación de las amenazas, se encuentran las de software,

las cuales, dentro del sistema operativo, pueden ser por software mal desarrollado, diseñado e implantado. De acuerdo a (Tanenbaum, 2003), los tipos amenazas de software se clasifican como los que se muestran en la Figura **2**.

Figura 2. Tipos de amenazas de software




Fuente: Autor del proyecto

Las amenazas de red se presentan cuando la red no está disponible para su uso, esto puede ocurrir por un ataque o por un error físico o lógico del sistema. Las principales amenazas que se dan son cuando no hay disponibilidad de la red y cuando se produce extracción lógica de la información. La tabla a continuación muestra los tipos de amenazas.

Cuadro 2. Tipos de amenazas en la red

| Tipos de Amenaza | Características |
|---|---|
| Por Topología | La topología es la disposición física que conecta los nodos de una red, computadores o servidores, cada uno con sus ventajas y desventajas. Dependiendo del alcance, se puede implementar una topología sobre otra pero se debe tener en cuenta que se puede limitar la comunicación hasta dejar la red fuera de servicio. |
| Por Sistema Operativo | Cada sistema operativo tiene diferente nivel de protección que lo hace susceptible a ataques, a partir de esto los atacantes pueden tomar acciones contra los sistemas operativos con mayor seguridad. |

| | |
|---|---|
| Por Cableado Estructurado | Son normas y estándares que consisten en un tendido de cables en el interior de un edificio con el propósito de implantar una red, utiliza una serie de cables, canalizaciones, conectores, etiquetas y demás dispositivos que se necesitan para establecer una infraestructura de telecomunicación en un edificio, se deben tener limitaciones dependiendo de lo que se vaya a implementar. |
| Por Incumplimiento de las normas de instalación de la red. | Con respecto a las instalaciones, se deben seguir ciertas normas (ANSI/TIA/EIA-568) y estándares que se conoce como cableado estructurado. |

Fuente: Autor del proyecto

Las amenazas de desastres naturales, son eventos que tienen origen por la fuerzas de la naturaleza, éstas afectan a la información de los sistemas y a la amenaza de integridad del sistema completo, ocasionando un sistema inoperable. Entre los diferentes desastres naturales que afectan al sistema se encuentran: inundaciones, terremotos, incendios, huracanes, tormentas eléctricas, por esta razón se debe tener en cuenta la importancia de un cableado de red de datos, redes de energía, suministro de agua ya que una falla de estos podría dañar la información de la organización.

Una amenaza a la seguridad de acuerdo al estándar ISO 7498-2 (1989) significa un posible medio por el cual puede transgredirse una política de seguridad, como puede ser la pérdida de confidencialidad e integridad. Un servicio de seguridad es una medida que puede instaurarse para hacer frente a una amenaza, como la protección del servicio de confidencialidad utilizando cifrado robusto.

**3.2.1.5.1 Identificación de requisitos de seguridad.** Para poder comprender e interpretar los diferentes tipos de amenazas a la seguridad, se necesita disponer de una definición global de los requisitos de seguridad. Estos requisitos son los siguientes:

- Secreto, confidencialidad, privacidad, intimidad y anonimato. Se requiere que la formación del sistema sea solo accesible para su lectura por partes autorizadas. Este tipo de acceso incluye la impresión, visualización y otras

formas de revelación, incluyendo, simplemente la revelación de la existencia de un objeto.

- Integridad, exactitud, corrección y autenticación. Los factores estratégicos del sistema de computación solo serán modificables por partes autorizadas. La modificación incluye la escritura, el cambio de valor, el cambio de estado, el borrador y la creación.
- Disponibilidad y accesibilidad. Los factores estratégicos del sistema de computación van a estar siempre funcionales para las partes autorizadas. El servicio de disponibilidad requiere que una red asegure un mínimo nivel de continuidad de servicio especificado. Pueden identificarse tres tipos de servicios de disponibilidad. (1) Cuando una red detecta condiciones que degradarían al servicio por debajo de un nivel mínimo pre especificado e informa de esa degradación a sus operadores. (2) Cuando una red posee suficiente poder de recuperación para proporcionar suficiente capacidad de recuperación frente a todo tipo de acciones de personas y procesos no autorizados que alteren datos. Este tipo de disponibilidad supone una capacidad de recuperación que se debe proporcionar mediante redundancia, utilización de facilidades alternativas y otros medios afines. El servicio proporcionado puede degradarse y/o puede requerir implementación de prioridades del servicio, para asegurar que las aplicaciones críticas tengan soporte. (3) Cuando una red es capaz de proporcionar un servicio continuado, pero además cuenta con un sistema de adaptación y reconfiguración automática.

**3.2.1.5.2 Tipos de amenazas según el Estándar ISO 7498-2** (1989)**.** Los tipos de amenazas a la seguridad de un sistema o de red de computadores descritos en el estándar ISO 7498-2, se caracterizan de forma más sencilla y se considera la función del sistema de computación como proveedor de información. En general, existe un flujo de información desde una fuente, como por ejemplo, una región de

memoria principal a un destino, que puede ser otro usuario. Las cuatro categorías generales de amenaza son las siguientes:

- Interrupción: Cuando ocurre un factor estratégico del sistema se destruye o se hace no utilizable o no disponible. Esta es una amenaza a la disponibilidad. Algunos ejemplos de interrupción son la destrucción de un componente hardware, un disco duro, el corte de un enlace de comunicaciones o la inhabilitación del sistema de gestión de archivos.
- Interceptación. Se produce cuando una parte no autorizada obtiene acceso a un factor estratégico. Esto constituye una amenaza a la confidencialidad. La parte no autorizada puede ser una persona, un programa o un computador.
- Modificación. Se produce cuando una parte no autorizada, no solo tiene acceso, sino que modifica un factor estratégico. Los ejemplos de modificación son el cambio de valores en unos datos, la alteración de un programa para que opere de forma diferente y la modificación del contenido de los mensajes que se transmiten en una red.
- Fabricación. Se produce cuando una parte no autorizada inserta objetos falsificados en el sistema. También constituye una amenaza a la integridad. Ejemplos de fabricación son la inserción de mensajes falsos en una red y la adición no autorizada de registros.

**3.2.1.5.3 Clasificación de las amenazas.** Según la forma de producirse, las amenazas pueden ser accidentales, como el mal funcionamiento del sistema, los errores del software y los fallos operacionales e intencionales. La realización de una amenaza intencional se puede considerar un ataque. Según el efecto que producen y la forma en que operan también pueden clasificarse en pasivas y activas. Las amenazas pasivas, son aquellas en las que el objetivo del atacante es obtener la información que se transmite. Son revelaciones no autorizadas de información, que se efectúan sin cambiar de estado el sistema y que están relacionadas con la interceptación de un secreto. Se pueden identificar dos tipos

de amenazas pasivas. (1) Liberación del contenido del mensaje. Ocurre cuando un usuario no autorizado lee el contenido de una transmisión de datos. Son objeto de estas amenazas un mensaje de correo electrónico no cifrado, que puede contener información sensible o confidencial, (2) Análisis del tráfico. Consiste en la interceptación de la información a través de la observación del flujo de tráfico, en cuanto a presencia, ausencia, cantidad, dirección, tipo de protocolos, frecuencia, etc., es posible que un atacante observe el patrón de la secuencia de los mensajes, aunque se encuentren cifrados.

El atacante puede terminar la localización e identidad de los computadores que se comunican y que también, puede observar la frecuencia, el tipo de protocolos utilizados y la longitud de los mensajes intercambiados. Esta información puede ser útil para averiguar la naturaleza de la comunicación (International Organization for Standardization-ISO, 1989).

Las amenazas pasivas son muy difíciles de detectar, ya que no alteran los datos, el objetivo, a la hora de traer este tipo de amenazas, radica más en la prevención que en la detección. Las amenazas activas suponen alguna modificación de flujo de datos o la creación de un flujo de datos falso. Abarcan tres áreas fundamentales: La interrupción que afecta la disponibilidad, la modificación y repetición, que atacan a la integridad y a la fabricación, que actúa también contra la integridad. Se pueden identificar las siguientes categorías (Bertolín, 2008):

- Suplantación o mascarada. Tiene lugar cuando una entidad finge ser otra diferente. Una suplantación, normalmente, incluye algunas de las otras formas de ataque activo. Un ejemplo son las secuencias de autenticación que se pueden capturar y repetir después de que se haya producido una secuencia de autenticación válida. Puede tener como finalidad conseguir que una entidad autorizada con escasos privilegios obtenga privilegios extra, suplantando una entidad que los posea.

- Repetición. Implica la captura pasiva de unidades de datos de protocolos y su retransmisión, que conlleva a la producción de un efecto no autorizado, mediante la repetición de un mensaje o parte de él. Por ejemplo, un mensaje válido que contiene información de autenticación, puede replicarse por parte de una entidad para autentificarse como alguien que no es.
- Modificación de mensajes. Significa que alguna parte de un mensaje legítimo ha sido alterado, o retardado, sin que se pueda detectar para producir un efecto no autorizado. Ejemplos de modificación de mensajes son los borrados, los retardados y la reorganización de mensajes.
- Denegación de servicios. Impide o inhibe la utilización normal o la gestión de las actividades de comunicación. Este tipo de ataque tiene un objetivo específico, como en el caso de una entidad que se puede suprimir todos los mensajes direccionados a un destino determinado como el servicio de auditoría de seguridad.

**3.2.2 Bring Your Own Device (BYOD).** *BYOD* es la nueva tendencia en la industria la cual facilita a los empleados en la organización el uso de sus dispositivos móviles personales para acceder a los recursos de la compañía para el desarrollo de sus funciones laborales, así como para su uso personal. Los accesos pueden ir desde los e-mails de trabajo, documentos, aplicaciones y recursos de red como impresoras entre otros. Es una tendencia que se ha producido debido a la potencia y flexibilidad de dispositivos portátiles inteligentes, que permite tener acceso a la información corporativa y personal (Information Commisioner's Office-ICO, 2014).

Este fenómeno se inicia en el 2009 cuando los empleados de Intel empezaron a usar sus dispositivos móviles personales en su lugar de trabajo, esto fue bien recibido ya que los directivos de Intel visualizaron una forma de reducir costos y mejorar la productividad (Information Security Media Group, 2016). Fue sólo hasta el año 2011 cuando los proveedores de servicios de TI, como Unisys y proveedor de software como Citrix Systems compartieron sus puntos de vista y percepciones

acerca de esta tendencia emergente y las organizaciones empezaron a considerar su implementación (Spandas, 2012).

Existen muchos aspectos a considerar durante la implementación de esquema (*BYOD*) Traiga su propio dispositivo, dentro de los que se destacan los costos financieros, la seguridad y temas legales. Un gran número de organizaciones adoptan esta tendencia buscando un aumento de la productividad (Rege, 2011), hoy en día los empleados parecen ser completamente dependientes del uso de sus dispositivos portátiles (laptops, Smartphones y tablets) para el desarrollo de su trabajo esto simplemente porque lo encuentran mucho más fácil que los recursos asignados por la compañía los cuales reposan en sus escritorios. Esto deja ver que para lograr ser más competitivos en el mercado las organizaciones deben estar a la vanguardia de los avances tecnológicos para los usuarios finales que realmente son sus empleados, todo esto sin comprometer la seguridad de la información y la privacidad del usuario final (Johnson & Filkins, 2012).

David A. Willis argumenta (2013) que, la implementación de una estrategia de BYOD, puede presentar un cambio radical en la economía y cultura a nivel de tecnologías de la información para las organizaciones en el mundo. Sin embargo, muchas de estas, especialmente las pequeñas y las medianas empresas (PYME) son culpables de subestimar el potencial ya sea ignorándolo o tomando medidas insuficientes para incorporar correctamente este tipo de tecnologías a su organización.

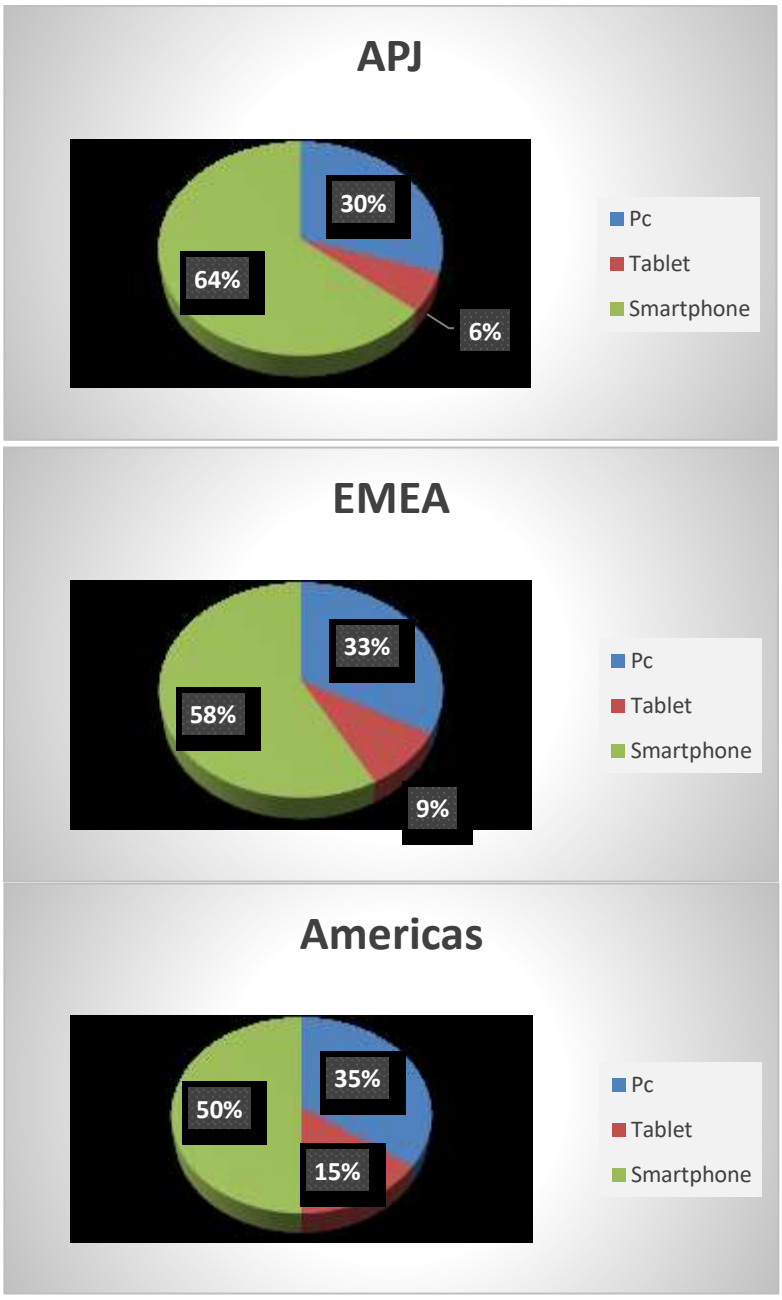
Un error que se presenta de manera frecuente en las organizaciones que tratan de incursionar en la tendencia BYOD es que las políticas de seguridad existentes son bastante cerradas con la finalidad de proteger la red, causando inconvenientes cuando los empleados traen sus dispositivos móviles para desarrollar sus labores diarias, incluso el no contar con el conocimiento suficiente y pretender desplegar un sistema BYOD, sin tener en cuenta el antivirus, programas anti-malware que se

encuentren instalados en los dispositivos móviles conduce a una gran cantidad de vulnerabilidades ocasionando inconvenientes con las políticas de seguridad existentes en ocasiones hasta comprometiendo la confidencialidad de la información. La aplicabilidad de esta tendencia BYOD podría funcionar dependiendo de la forma y el alcance con el que se realice su despliegue, aplicación y gestión, este es un esquema que cada vez más organizaciones sin importar su tamaño han venido adoptando, realizando asignación de presupuestos y recursos hacia esta nueva modalidad de trabajo. Se habla que en promedio el 61% de las organizaciones a nivel internacional indican que sus empleados utilizan sus dispositivos personales para efectuar sus labores en su lugar de trabajo. Las organizaciones que adoptan una tendencia BYOD se ha incrementado en 73%, se prevé que para el 2015 el 90% de las organizaciones incentive a los empleados al uso de sus dispositivos móviles con aplicaciones y software empresarial.

**La**

Figura **3** muestra el aumento del uso de dispositivos móviles en que se presenta en cada una de las regiones del mundo, el estudio realizado por Bussines Insider indica que los dispositivos más usados son las tablets presentando un crecimiento del 20% entre los años 2014 y 2015, mientras que el uso de computadores de escritorio y portátiles decae en un 24%.

Figura 3. Porcentaje de uso de dispositivos móviles a nivel América, Asia y Pacífico, Europa, Oriente Medio y África. Encuesta realizada por Global Connected Devices By Device Type




Fuente: Bort (2012)

Contar con una buena política de BYOD representa nuevas oportunidades en las organizaciones, pero no se pueden dejar de lado los riesgos que se encuentran asociados, tales como:

- Confidencialidad de la Información; El contar con diversos dispositivos móviles en los que se encuentren configuradas aplicaciones de la organización, pueden verse expuestos a pérdida o robo de los mismos, dejando de manera explícita información sensible.

- Virus y *Software* malicioso, El no tener el *software* ni el *hardware* estandarizado y brindar acceso a la red corporativa a una gran cantidad de dispositivos si conocer su estado en actualizaciones o nivel de seguridad pueden ocasionar muchos inconvenientes

Control de acceso e integridad de la información, Se genera una mayor necesidad de controlar el acceso de red y la privacidad de la información, en caso de la salida de un empleado de la organización o la perdida de alguno de sus dispositivos, se debe actuar de manera inmediata para interrumpir el acceso a la red corporativa y restringir el acceso a los datos de la organización que se encuentran en el dispositivo. Adicional debe existir segmentación sobre los datos de la organización y los datos personales almacenados en el dispositivo.

Las organizaciones pueden tener muchas razones por las que decidan implementar una política BYOD. Un aliciente importante es el ahorro en costos sobre los activos de TI al no tener que pagar por los dispositivos y planes de datos costosos.

Al permitir que los empleados asuman estos costos, la organización puede orientar un nuevo presupuesto para el desarrollo de la política buscando la seguridad conjunta tanto de los datos como de los dispositivos de los empelados También hay beneficios en la productividad. Si el empleado puede hacer su trabajo en su propio dispositivo móvil, hay menos tiempo de inactividad durante la capacitación de un nuevo dispositivo desde el cual puede ponerse al día en sus labores, revisar mensajes de correo electrónico fuera del horario laboral, se reduce el soporte tecnológico en la mayoría de casos el empleado se encuentra en la capacidad de

solucionar sus inconvenientes. Permitirle el uso de su propio dispositivo significa que tendría un mayor cuidado sobre el mismo, el contar con la información corporativa y personal de primera mano y en solo dispositivo mejoraría la forma de buscarla optimizando la comunicación e incrementando las oportunidades de negocio.

Las políticas BYOD en las organizaciones pueden presentar una cierta resistencia por parte de Tecnologías de la Información y de los empleados, sin embargo, son una realidad en los negocios hoy en día.

**3.2.3 Control de Acceso.** El control de acceso es el proceso de conceder permisos a usuarios o grupos y poder conocer quienes están autorizados para acceder a los sistemas de información y recursos. Su concepto se resume en tres pasos que son: identificación, autenticación y autorización, gracias a estos principios y con el buen uso de los mismos el administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema.

Para tener éxito en la protección de las redes internas, lo fundamental es poder contar con una política para el control de acceso con el objetivo de evitar o minimizar todos aquellos accesos que no son autorizados, por lo que se puede controlar mediante:

- Registros de usuarios
- Gestión de privilegios
- Autenticación por contraseñas o usuarios, etc.

Además de la autenticación, es necesario poder asegurar a los equipos que son descuidados por un lapso de tiempo determinado, es decir, se podría realizar una activación automática de un protector de pantalla después de cierto tiempo de inactividad, el mismo que impedirá el acceso mientras no se introduzca una

contraseña autorizada. Así mismo, son de vital importancia los controles de acceso a la red, al sistema operativo, a las aplicaciones y a la información, para ello, deben existir registros y bitácoras de acceso. Para el caso de existir comunicación móvil, redes inalámbricas, computadores portátiles, etc. también es necesario implementar políticas que contemplen cada uno de estos aspectos (Novenca Security Systems, 2015).

Se debe establecer, documentar y revisar una política de control de acceso con base a las necesidades de seguridad y de negocio de la organización. Las reglas para el control del acceso deben tener en cuenta las políticas de distribución y autorización de la información, es decir, establecer una serie de controles referidos de acuerdo con:

- Control de acceso a la información, análisis de requisitos necesarios para el control de acceso.
- Crear una Política de control de acceso. Control de accesos, únicamente a usuarios autorizados.
- Registro de usuario, gestión de privilegios, gestión de contraseñas de usuarios.
- Control de accesos a usuarios no autorizados, contribución y responsabilidad por parte de los usuarios.
- Uso de contraseña, equipo de usuario desatendido, Política de puesto despejado y mesa limpia.

Frias-Martínez, Stolfo y Keromytis (2008), definen los productos de seguridad como una táctica que resuelve muy bien problemas de seguridad. La seguridad de la información es un reto en escenarios como empleados regulares, empleados remotos, tele trabajadores, usuarios invitados, etc. El uso de estos escenarios afecta el contexto de la seguridad de la red, por lo tanto, en los dispositivos finales se hace más fácil la penetración de malvare.  Esta penetración se debe a:

- Antivirus vencido
- Sistema operativo sin parches
- Configuraciones defectuosas en el firewall
- Error en las firmas para detección de intrusos
- Productos de seguridad vencidos
- Equipos infectados

Se puede concluir que la seguridad informática está en juego, convirtiéndose en un requisito principal de las nuevas infraestructuras de seguridad que puedan controlar el acceso a la red de los dispositivos finales y asegurar que los dispositivos finales ya sea locales o remotos cumplan con las características de seguridad. Para seguridad se cuenta con que inicialmente, los usuarios se autentican en la red para ingresar pero verificar que los computadores cumplan el nivel exigido en la política de seguridad no es una práctica común. Estos dispositivos finales son amenazas latentes que pueden perjudicar la seguridad de la red.

El control de acceso es una visión que utiliza soluciones existentes y nuevas que ofrece garantías para que cualquier dispositivo que intente conectarse a la red se autentique mediante políticas definidas. Los dispositivos que no cumplan son aislados o colocados en cuarentana, no autorizando el ingreso cuando intentan conectarse. Dentro de las clasificaciones de control de acceso se encuentran las siguientes:

**3.2.3.1 Control de acceso por identificación.** Es una acción que el sistema realiza para reconocer la identidad de los usuarios, habitualmente se usa un identificador de usuarios, todas las acciones que se llevan a cabo en el sistema son de responsabilidad de los usuarios, entonces hablamos de la necesidad de registros de auditorías que permiten guardar las acciones realizadas dentro del sistema y

rastrearlas hasta el usuario autenticado, es decir es el medio por el cual los usuarios del sistema identifican quiénes son.

**3.2.3.2 Control de acceso por autenticación.** Autenticación es verificar que el usuario que trata de identificarse es válido, por lo general se implementa con una contraseña en el momento de iniciar una sección, es el segundo paso del proceso de control de acceso (Creative Commons Attribution Share-Alike 3.0 License, 2016).

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas: (1) algo que solamente el individuo conoce: ejemplo una contraseña, (2) algo que una persona posee: ejemplo una tarjeta magnética, tarjeta con circuito integrado, (3) algo que el individuo es y que lo identifica de manera única: ejemplo las huellas digitales, reconocimiento de voz, (4) algo que solamente el individuo es capaz de hacer: ejemplo los patrones de escritura.

**3.2.3.3 Control de acceso criptográfico.** Existen mecanismos de control de acceso criptográfico donde se combina algunas técnicas de la criptografía para desarrollar protocolos, modelos y mecanismos de autenticación para el control de acceso.

Es un protocolo de autentificación de red. Está diseñado para suministrar una autentificación poderosa para aplicaciones cliente/servidor usando criptografía secret-key. Una versión libre de este protocolo Internet es un lugar inseguro. Muchos de los protocolos usados en internet no proporcionan seguridad. Herramientas para "rastrear" contraseñas fuera de la red son usadas comúnmente por piratas informáticos maliciosos. Por lo tanto, aplicaciones que envían una contraseña no encriptado sobre la red son sumamente vulnerables. Peor aún, otras aplicaciones de cliente/servidor dependen de la honestidad sobre la identidad del usuario que lo está usando (Creative Commons Attribution Share-Alike 3.0 License,

2016). Algunos sitios intentan que cortafuegos (Firewall) solucionen sus problemas de seguridad de la red. Desafortunadamente, los cortafuegos suponen que "los villanos" están en el exterior, que es a menudo una suposición muy mala. La mayoría de los incidentes muy perjudiciales del delito informático son llevados por miembros. Los cortafuegos también tienen una desventaja importante, restringen cómo pueden usar Internet por sus usuarios. Después de todo, los cortafuegos son sólo un ejemplo menos extremista del dictamen de que no hay nada más seguro que una computadora que está desconectada de la red. En muchos lugares, estas restricciones son sólo irrealistas e inaceptables.

Kerberos fue creado por MIT como una solución para estos problemas de seguridad de la red. El protocolo de Kerberos usa criptografía fuerte con el propósito de que un cliente pueda demostrar su identidad a un servidor (y viceversa) al otro lado de una conexión de red insegura. Después de que un cliente/servidor ha conseguido que Kerberos demuestre su identidad, también pueden cifrar todas sus comunicaciones para garantizar la privacidad y la integridad de los datos cuando continúa en su empresa.

MIT provee el código fuente de Kerberos con el propósito de que alguien que desea usarlo pueda estudiar el código y así asegurarse que el código es digno de confianza. Además, para aquellos que prefieren depender de un producto soportado de manera profesional, Kerberos está disponible como un producto de muchos distribuidores diferentes.

La **¡Error! No se encuentra el origen de la referencia.** muestra el f
uncionamiento del protocolo de autenticación a través del protocolo Kerberos.

Fuente: Creative Commons Attribution Share-Alike 3.0 License (2016)

El protocolo de autenticación de Kerberos es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor que lo ofrece; este proceso se realiza en tres grandes etapas que a continuación se describen:

C: Cliente que solicita un servicio
S: Servidor que ofrece dicho servicio
A: Servidor de autenticación
T: Servidor de tickets
K: Clave secreta del cliente trasferencia
K: Clave secreta del servidor
K: Clave secreta del servidor de tickets
K: Clave de sesión entre el cliente y el servidor de tickets
K: Clave de sesión entre cliente y servidor

**3.2.3.4 Modelos de control de acceso.** Un modelo de control de acceso es un conjunto definido de criterios que un administrador del sistema utiliza para definir derechos/permisos de los usuarios del/al sistema.

Los modelos principales de control de acceso son:

- Control de Acceso Obligatorio *(Mandatory Access Control) (MAC)*
- Control de Acceso Discrecional *(Discretionary Access Control) (DAC)*
- Controles de Acceso Basado en Roles *(Rule Based Access Control) (RBAC)*

**3.2.3.5 Políticas de control de acceso.** La política definida para el control de acceso debe quedar basada en los requerimientos de seguridad, además de ser implantada, documentada y revisada.

En una política de accesos se debe establecer de manera detallada y clara las reglas y los derechos que son asignados a cada usuario o grupo de usuarios. Es importante que se considere de manera conjunta los controles de acceso lógicos y físicos. También es primordial dar a los usuarios y proveedores de servicios una explicación detallada y clara de cada uno de los requisitos de negocio protegidos por los controles de accesos. La política debería contemplar lo siguiente:

- Requerimientos de seguridad que serán analizados de manera individual para cada aplicación de negocio.
- Recopilación e identificación de la información con referencia a las aplicaciones y riesgos que la información está afrontando.
- Políticas para la distribución de la información y las autorizaciones (niveles de seguridad para la clasificación de la información).
- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes.
- Reglamentación aplicable y las obligaciones establecidas con respecto a la protección del acceso a los datos o servicios.
- Perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos.

- Administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión.
- Segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos.
- Requerimientos para la autorización formal de los pedidos de acceso.
- Requerimientos para la revisión periódica de controles de acceso.
- Retiro de los derechos de acceso.

**3.2.4 Control de Acceso A Redes (NAC).** NAC se puede clasificar en dos categorías, uno es el estándar abierto y otro es el propietario. Cada solución de NAC se limita a su proveedor y no cuenta con el apoyo técnico de otros proveedores para generar nuevas y mejores soluciones. La estandarización de la arquitectura NAC juega un papel importante y es la llave para el éxito.

**3.2.4.1 Funciones de NAC.** En el mercado actual, existen numerosas soluciones NAC disponibles. Las empresas tienen diferentes solicitudes para implementar esta solución ya que no hay un estándar unificado. NAC debe pasar por tres fases: Una fase de sensibilización, una de normas (propietario y no propietario) y la interoperabilidad de tales normas. Actualmente NAC se encuentra en la segunda fase denominada Normas.

Las funcionalidades que una solución NAC debe tener son las siguientes:

- Detección del nodo
- Autenticación
- Evaluación de seguridad del dispositivo final
- Autorización
- Cumplimento de la política
- Cuarentena
- Remediación

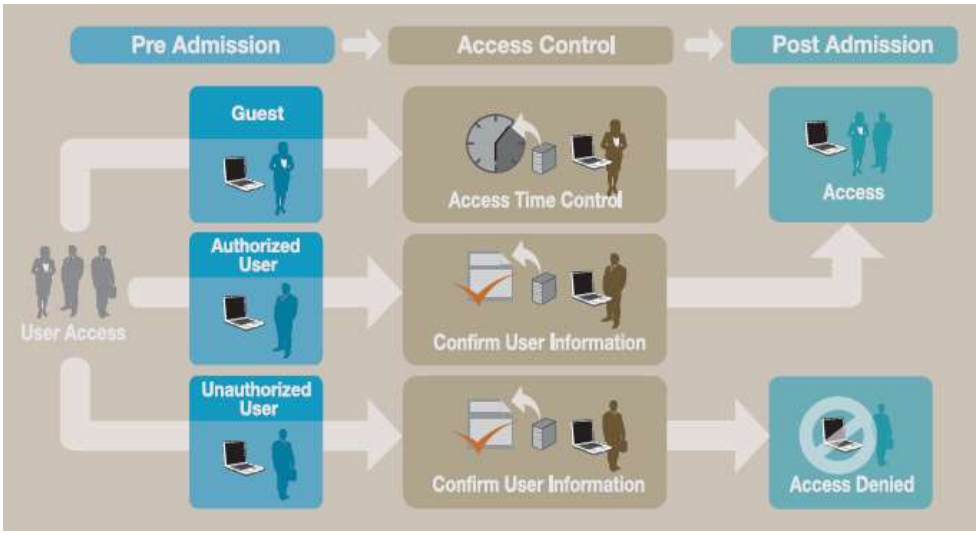
- Control post- admisión

**3.2.4.2 Elementos de un Control de Acceso a la Red.** Los elementos que integran el control de acceso a la red son los siguientes:

- Equipo cliente. En una red, los equipos clientes son empleados por los usuarios de una red tales como PC's, impresoras, servidores, entre otros.
- Autenticador. Entidad en un extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace.
- NAC *Gateway*. Es un dispositivo que se encuentra entre el servidor de autenticación y el equipo de usuario final. Este dispositivo permite controlar las acciones de autenticación y autorización mediante la manipulación de los atributos que entrega el servidor de autenticación, a fin de indicar al autenticador la acción a seguir.
- Servidor de autenticación. Entidad que facilita el servicio de autenticación al autenticador (Córdoba Téllez & Durán Martínez, 2010).

La Figura 4 muestra los elementos que hacen parte de la solución de control de acceso

Figura 4. Elementos de NAC




Fuente: Córdoba Téllez y Durán Martínez (2010)

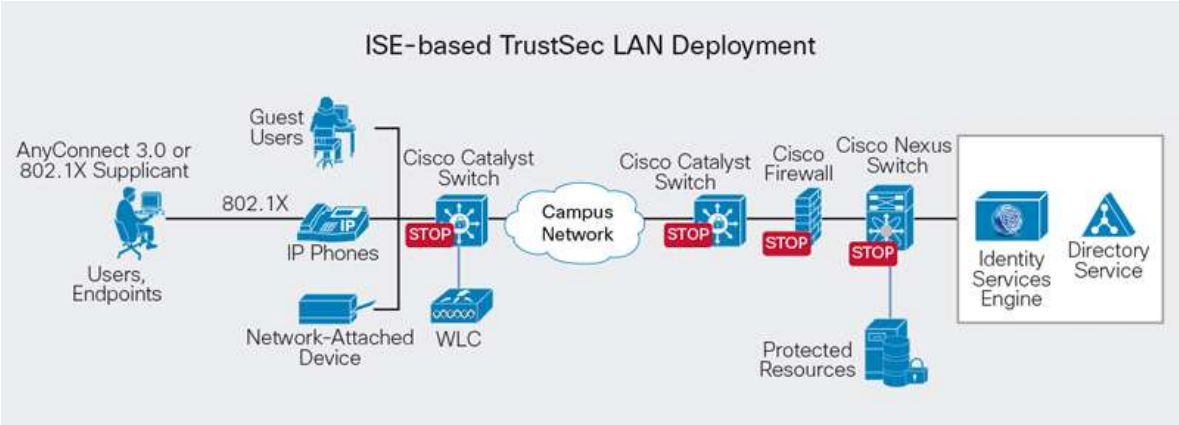
NAC impide el acceso de dispositivos no autorizados de forma automática y protege el riesgo de una falla en la red gracias a la política de administración integrada.

Por otra parte, *Cisco Identity Services Engine* (ISE) es una sofisticada plataforma de seguridad de tipo contextual cuyo trabajo es identificar a los usuarios que buscan acceder a los sistemas informáticos de la red de datos de un corporativo, provee un monitoreo completo, reporte y alarmas para todas sus funciones desde el panel de control NAC, evaluación por perfiles AAA, invitados BYOD y acceso *Mobile Device Management (MDM)* el cual es la gestión de los dispositivos móviles en el ámbito de las empresas. El servicio de alimentación dinámica de dispositivos es continuamente actualizado y si un servidor se ve comprometido y empieza a reenviar el tráfico como servidor de protocolo simple de transferencia de correo (SMTP) ilegitimo, el ISE puede reclasificar el dispositivo y cambiar su nivel de acceso a partir de los sondeos realizados por NetFlow.

La integración del ISE con la sensibilidad en el contexto ocurre cuando la visibilidad de un terminal se intersecta con señales de otra infraestructura de red, aplicaciones y defensas de seguridad. El ISE usa el contexto para centralizar y unificar el control

de acceso transmitido en la política de acceso a la red segmentándolo dinámicamente sin la complejidad de múltiples VLANs y sin cambiar la arquitectura de la red. Al contar con una plataforma robusta de acceso compartido pxGrid, se acelera la eficacia de la red y las soluciones de seguridad. La anterior plataforma también funciona para integrar el NAC con otras plataformas de seguridad para acelerar las características de sus soluciones e identificar, mitigar y remediar las amenazas en la red. Estas mejoras de seguridad expandidas ofrecen nuevas posibilidades como la detección avanzada de amenazas en la red, el fortalecimiento de los *Firewalls* y reforzar los antivirus. En la Figura **5** se puede identificar la implementación de una red LAN basada en ISE.

Figura 5. Red LAN basada en ISE




Fuente: (Cisco Systems, Inc, 2016)

**3.2.5 *Cisco Network Asset Collector* (CNAC).** Cisco CNAC es una solución para el control de acceso a la red, cuya arquitectura es propietaria, que permite autenticar, autorizar, evaluar y remediar posibles vulnerabilidades, antes de permitir que los usuarios se conecten en la red, conexiones que pueden ser alámbricas, inalámbricas, accesos remotos, etc., es decir, se identifican a los dispositivos, computadores portátiles, computadores de escritorio y otros activos que sean

autorizados, compatibles y que cumplan con la política, antes de permitir el acceso. El primer paso se produce en el punto de autenticación, antes de que el código malicioso pueda causar daños, entonces su tarea es evaluar si los equipos cumplen con las políticas de seguridad. Las políticas de seguridad pueden variar por el tipo de usuario, el tipo de dispositivo o sistema operativo, es así que cuando no se cumple la política, se toman las acciones de bloquear, aislar o reparar equipos que no cumplan. Los equipos son redirigidos a un área de cuarentena, donde se produce la remediación.

Cisco define a NAC como: El control de la admisión de la red de Cisco. Es una solución que utiliza la infraestructura en red para hacer cumplir políticas de seguridad en todos los dispositivos que intentan tener acceso a recursos de computación de la red, ayuda a asegurar que todos los hosts cumplan con las últimas políticas de seguridad corporativa, tales como antivirus, software de la seguridad, y parches (remiendo) del sistema operativo, antes de obtener el acceso de red normal (Cisco, 2013).

**3.2.5.1 Características y beneficios.** A continuación se muestran las características y beneficios que ofrece la solución de control de acceso propietaria de Cisco:

- Impide el acceso no autorizado a redes para proteger sus activos de información.
- Ayuda a mitigar proactivamente las amenazas de red tales como virus, gusanos y software espía.
- Identifica las vulnerabilidades en los equipos de los usuarios mediante la evaluación periódica y la remediación.
- Permite reducir costos mediante el seguimiento automático, reparación y actualización de equipos cliente.

- Reconoce y clasifica a los usuarios y sus dispositivos antes de que el código malicioso puede causar daños.
- Evalúa el cumplimiento de la política de seguridad basada en el tipo de usuario, tipo de dispositivo y sistema operativo.
- Aplica las políticas de seguridad mediante el bloqueo, aislamiento y reparación de máquinas no compatibles en un área de cuarentena sin necesidad de la atención del administrador.
- Aplica el servicio de evaluación y remediación a una variedad de dispositivos, sistemas operativos, dispositivos y métodos de acceso incluyendo LAN, WLAN, WAN y VPN.
- Aplica las políticas de todos los posibles escenarios de funcionamiento sin necesidad de productos independientes o módulos adicionales.

**3.2.5.2 Protocolo de autenticación extensible (EAP).** El Protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*) es una extensión del Protocolo punto a punto (PPP) que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información de longitudes arbitrarias. EAP se ha desarrollado como respuesta a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad, como las tarjetas inteligentes, tarjetas de identificación y calculadoras de cifrado. EAP proporciona una arquitectura estándar para aceptar métodos de autenticación adicionales junto con PPP.

Mediante EAP, se pueden admitir esquemas de autenticación adicionales, conocidos como tipos EAP. Entre estos esquemas, se incluyen las tarjetas de identificación, contraseñas de un solo uso, autenticación por clave pública mediante tarjetas inteligentes y certificados. EAP, junto con los tipos de EAP seguros, es un componente tecnológico crítico para las conexiones de red privada virtual (VPN) seguras. Los tipos EAP seguros, como los basados en certificados, ofrecen mayor seguridad frente a ataques físicos o de diccionario, y de investigación de

contraseñas, que otros métodos de autenticación basados en contraseña, como CHAP o MS-CHAP.

**3.2.5.3 Soporte 802.1X.** Cisco NAC ayuda a reducir la pérdida potencial de información sensible permitiendo a las organizaciones verificar el nivel de privilegios de un usuario antes de conceder el acceso a la red. Esto ayuda a prevenir el acceso no autorizado a través del cable, inalámbrica o red de acceso remoto. Cisco NAC proporciona una integración completa con la tecnología inalámbrica, VPN y 802.1X, y puede ser implementado en un *single-sign-on* (SSO) de manera de maximizar los beneficios y minimizar el impacto de seguridad del usuario (Cisco System, Inc, 2014).

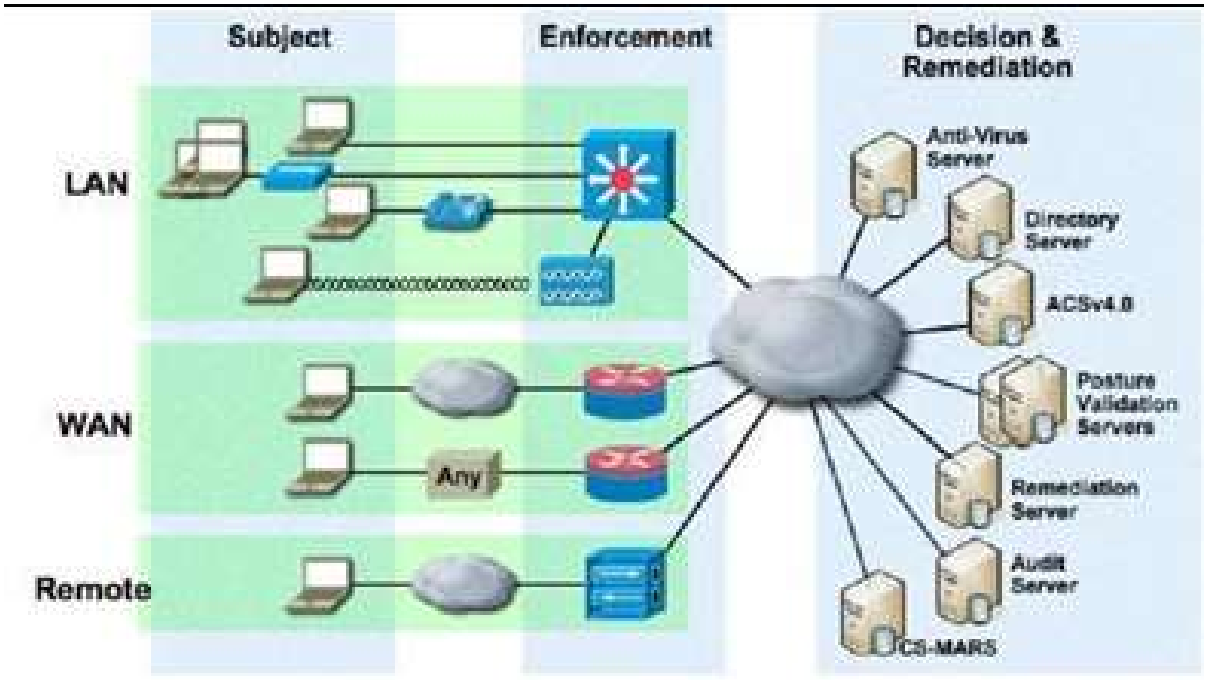
El estándar 802.1x es una solución de seguridad ratificada por el IEEE en junio de 2001 que puede autenticar (identificar) a un usuario que quiere acceder a la red ya sea por cable o inalámbrica. Esto se hace a través del uso de un servidor de autenticación. El 802.1x se basa en el protocolo EAP (Protocolo de autenticación extensible), definido por el Grupo de Trabajo de Ingeniería de Internet (IETF). Este protocolo se usa para transportar la información de identificación del usuario.

### 3.2.5.4 Descripción de la Arquitectura

La ¡Error! La autoreferencia al marcador no es válida. muestra la arquitectura propietaria de Cisco, que en el lado del cliente se compone de un agente denominado Cisco Trust Agent cuya función es la de recibir la información del estado de la seguridad del equipo a conectar a la red proporcionando toda la información recogida, para recopilar esta información pueden usarse aplicaciones de distintos fabricantes o una propietaria de Cisco, el Cisco Secure Access. Para el

Trust Agent, Cisco ha desarrollado un protocolo propietario, el EAP, en dos versiones: una sobre UDP y otra sobre 802.1x.

Figura 6. Descripción de la arquitectura CNAC




Fuente: Cisco Systems (2016)

La diferencia entre ambas es que sobre UDP se hace solo validación y en 802.1x se hace validación y autenticación. Además, no todos los equipos Cisco soportan todos los escenarios posibles a través del protocolo EAP, muchos *switches y routers* requieren de una actualización.

En cuanto a servidores Cisco, se utiliza el *Access Control Server* que se ha desarrollado para tal fin, completando con interfaces de verificación, auditoria y autenticación de otros fabricantes. Cisco también ofrece una solución basada en appliances permitiendo una más rápida implementación.

Cisco NAC está presente a través de todos los métodos de acceso a la red. La información de la situación puede ser recogida y la políticas de acceso aplicadas

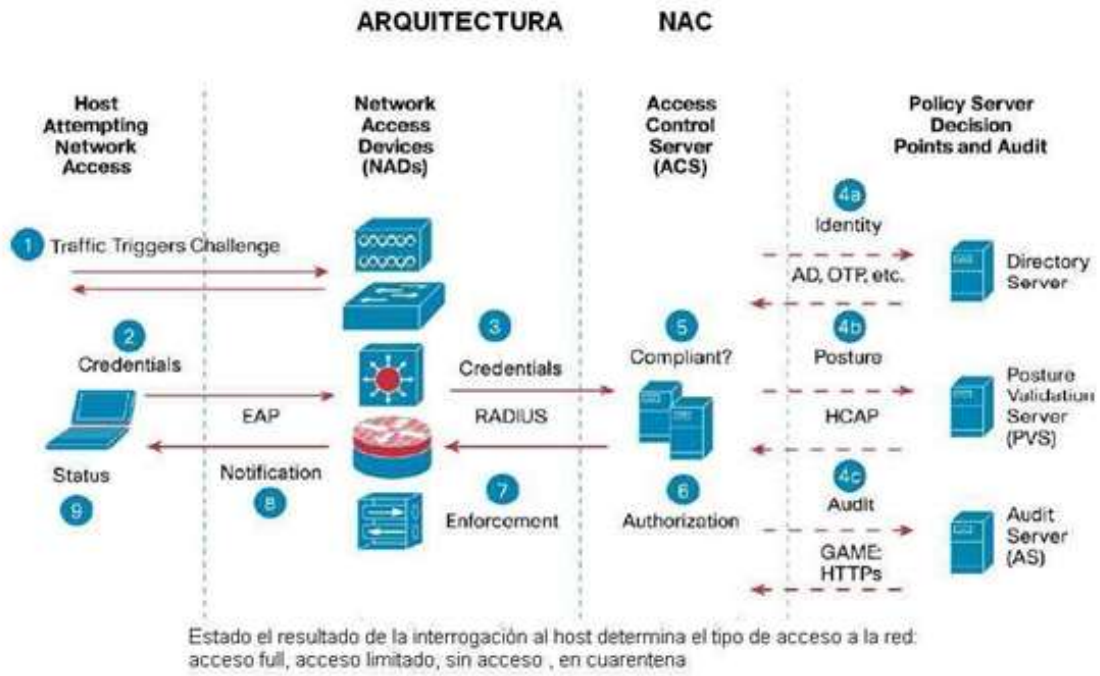
para los *host* que tratan de acceder a la red a través de *routers*, *switches*, puntos de acceso inalámbricos, concentradores VPN, etc.

**3.2.5.5 Componentes.** Los procesos en el escenario de validación de Cisco NAC incluyen los siguientes componentes arquitectónicos:

- Host: Dispositivo de acceso a la red en la que se aplica NAC.
- Postura del *Plugins* (PP). Un dispositivo Cisco o la tercera parte de un DLL que reside en un *host* y proporciona información de las identificaciones o credenciales de un agente y este que reside en el mismo dispositivo.
- Agente de Postura (PA). Agente *host de software* que actúa como un intermediario en el host para la agregación de credenciales potenciales de múltiples situaciones, *plugins* y la comunicación con la red.
- Remediación del cliente: Un componente de una solución de gestión de recuperación que funciona en combinación con un servidor de recuperación para actualización de software cliente específico, tales como parches del sistema operativo.

La Figura **7** muestra la arquitectura básica de NAC y proporciona una visión general del proceso de autorización utilizados para conceder o denegar acceso a la red.

Figura 7. Arquitectura básica de NAC




Fuente: Cisco Systems (2007)

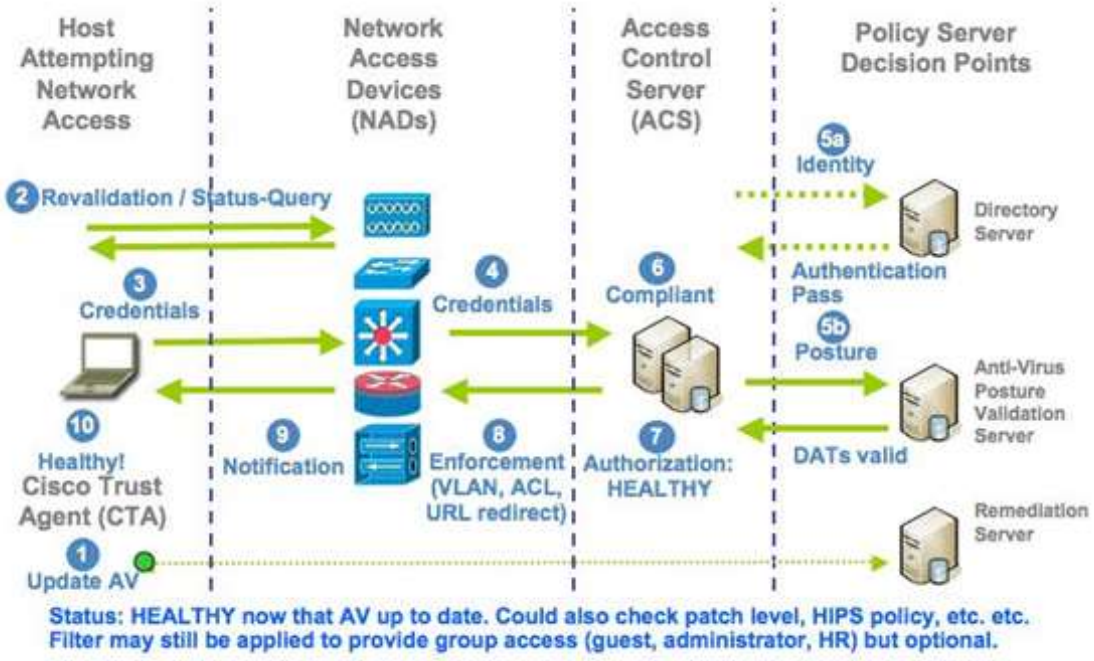
A continuación se describe el funcionamiento de la arquitectura para implementar control de acceso a la red:

- La validación de postura ocurre cuando un dispositivo de acceso a la red detecta que un host se quiere conectar o usar los recursos de la red.
- Una vez detectado el nuevo dispositivo, el NAD (dispositivo de acceso a la red) habilita una conexión entre el AAA (servidor de autorización autenticación y auditoria) y *el Access Control Server (ACS)* o servidor de control de acceso, una vez establecida esta conexión, el Servidor AAA requiere las credenciales de postura al host desde uno o más plugins de posturas.
- El *host* responde a la petición con sus credenciales de postura desde el software compatible con NAC.

- El servidor AAA, valida la información de las posturas localmente, o puede delegar esta decisión a otros servidores de validación de posturas.
- El servidor AAA, agrega los resultados individuales de la postura, o símbolo (tokens) de postura, de todos los servidores para determinar la conformidad total del host, o del símbolo de postura del sistema.
- La autenticación de identidad y el token de postura del sistema son luego chequeadas por una red de autorización, que puede consistir en: servidor Radius, asignación de VLANs o listas de acceso descargables.
- Estas cualidades del Radius se envían al NAD para la aplicación en el host.
- El agente en el host envía el estado de su postura para notificar los plugins respectivos de su postura individual del uso así como la postura entera del sistema.
- Se puede enviar opcionalmente un mensaje al usuario final usando el diálogo de la notificación del agente notificando el estado actual del anfitrión en la red.

Para comprender gráficamente cómo interactúan cada uno de los componentes de la solución de Cisco, se presenta a continuación la Figura **8**.

Figura 8. Funcionamiento de Cisco Network Asset Collector




Fuente: (Cisco Systems, Inc, 2007)

A continuación se detallan los pasos numerados en la imagen anterior:

**Paso 1.** La validación de postura inicia cuando un dispositivo (computador o dispositivo inalámbrico) intenta conectarse a la red.

**Paso 2.** El Dispositivo de acceso a la red (NAD) que puede ser un *router o switch*, realiza una conexión segura con el *Cisco Secure ACS y el Cisco Trust Agent* para solicitar a través de sus protocolos de autenticación como RADIUS o TACACS las credenciales de autenticación

**Paso 3.** El CTA envía estas credenciales al servidor AAA o éste a su vez puede delegar esta función a un servidor de validación de postura

**Paso 4.** El servidor AAA envía las credenciales al *Cisco Secure ACS* quien revisa si cumple o no con los requisitos de acceso entre los que se encuentran: parches de los sistemas operativos, antivirus actualizados, entre otros.

**Paso 5.** El *Cisco Secure ACS* verifica si las credenciales cumplen con los requisitos de validación.

**Paso 6.** El *Cisco Secure ACS* envía notificación al NAD con información sobre si permite o deniega el acceso a la red.

**Paso 7.** El Dispositivo de acceso a la red (NAD) recibe estas notificaciones y las envía al *Cisco Trust Agent (CTA)*

**Paso 8.** El Cisco Trust Agent recibe las notificaciones sobre si se permitió, denegó el servicio a la red o es colocado en cuarentena en una subred diferente.

**Paso 9.** El dispositivo accede a la red o un servidor de cuarentena el cual se encarga de aplicar las actualizaciones requeridas para que el dispositivo pueda iniciar nuevamente el proceso de validación de postura.

**Paso 10.** La solicitud de acceso se niega para la petición del cliente (Feitosa, Oliveira, Lins, & Junior, 2008).

Todos los puntos de decisión son considerados si el servidor AAA o PVS, evalúa uno o más conjuntos de credenciales de host en los motores de políticas basadas en reglas, con resultados en uno o más tokens de aplicación (APT). Un APT representa un control de cumplimiento de las aplicaciones en el host dados a un proveedor. El servidor AAA a continuación, combina todos los APTs con los PVs delegados en su propio motor de políticas dentro de un único token de sistema de la postura (SPT) que representa el cumplimiento general del host. Por lo tanto, si uno de los APTs que componen el SPT en general, no pasa la prueba de conformidad, el SPT general refleja esto. Tanto APTs y SPTs se representan mediante las siguientes fichas predefinidas:

**Saludable.** El *Host* es compatible, no tiene restricciones sobre el acceso a la red.

**Chequeo.** El *Host* está dentro de la política, pero hay una actualización disponible. Este chequeo se utiliza para remediar de forma proactiva el estado de salud.

**Transición.** El *Host* de postura es un proceso para facilitar el acceso provisional en espera de la validación de la postura completa. Este estado es aplicable durante el arranque del host, cuando todas las aplicaciones NAC no se están ejecutando o durante una auditoria cuando la información de la postura aún no se ha obtenido a partir del host.

**Cuarentena.** El *host* no cumple las políticas de control; restringir el acceso a la red, se debe colocar en una red de cuarentena para la remediación. El host no es una amenaza activa pero es vulnerable a un ataque conocido o infección.

**Infectado.** El *Host* es una amenaza activa a otras máquinas, el acceso a la red debe ser severamente restringido o totalmente negado.

**Desconocido.** La postura de un *host* no se puede determinar, se debe poner en un estado de cuarentena el *host*. Se realiza auditoría o remediación hasta que se puede determinar una postura definitiva.

**3.2.5.7 Componentes de CISCO NAC.** A continuación se detallan cada uno de los componentes que hacen parte de la arquitectura de control de acceso a la red propietaria de Cisco:

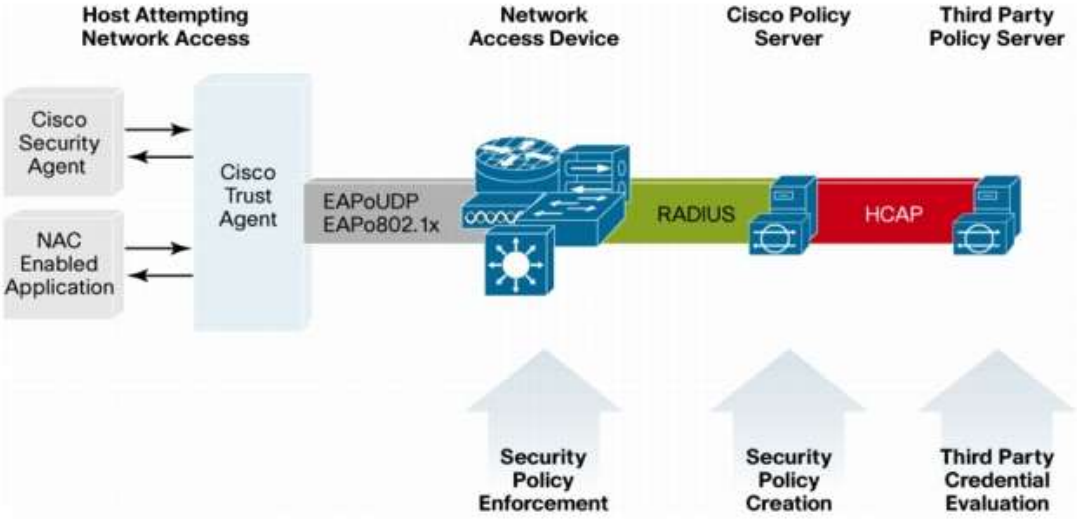
***3.2.5.7.1*** **Cisco Trust Agent (CTA).** El *software Cisco Trust Agent*, es un sistema, instalado en los dispositivos y en los servidores situados en los extremos de la red, obtiene información sobre el nivel de seguridad en cada punto por medio de múltiples aplicaciones, como el *software* antivirus. Una vez obtenida la información, *Trust Agent* la transmite a la red de Cisco, donde se toman y se hacen cumplir las decisiones relativas al control de acceso a la red. Para facilitar el despliegue, este software puede integrarse con *Cisco Security Agent*, una solución de seguridad para los extremos de la red que la protege contra ataques por virus desconocidos (day-zeroattacks) y otras amenazas diseñadas con el propósito de

asegurar una total compatibilidad de los parches con los sistemas operativos de los dispositivos finales (Cisco Systems, Inc, 2005).
Las características del Cisco Trust Agent son las siguientes:

- Permite validar la postura de las aplicaciones en activos administrados
- Funciona en redes cableadas, inalámbricas, de acceso remoto, y los entornos de oficinas remotas
- Está respaldada por una amplia gama de proveedores
- Está disponible en sistemas operativos *Windows y Red Hat Linux*
- Es fácil de instalar, ligero para correr
- Actúa como un componente de middleware que toma la información de la política de acogida y con seguridad se comunica la información a la Autenticación, autorización y contabilidad (AAA) del servidor de políticas.
- *Cisco Trust Agent* se comunica con las aplicaciones habilitados con NAC a través de los canales de comunicación integrados por los participantes del NAC en sus aplicaciones
- Incluye un suplicante 802.1x para las comunicaciones de Capa 2 en entornos cableados.
- Autentica el servidor AAA. *Cisco Trust Agent* valida el solicitante a través de comunicaciones cifradas con el servidor AAA.
- Permite a los clientes para crear secuencias de comandos para la recopilación de información personalizada.

La herramienta de software de Cisco (*Trust Agent*) recopila información de estado de seguridad de las soluciones de software de seguridad en el dispositivo final y la comunica al dispositivo de acceso a la red utilizando EAP o UDP sobre el protocolo 802.1x. *Cisco Trust Agent* reside tanto en la parte superior del modelo TCP/IP como en el 802.1x. La Figura **9** muestra la descripción de arquitectura del Cisco Trust Agent

Figura 9. Cisco Trust Agent Descripción de la arquitectura




Fuente: Cisco Systems (2005)

**3.2.5.7.2 Network Access Device (NAD).** Cada dispositivo de acceso a la red analiza todos los host que intentan conectarse a la red, tales como *router*, *switch*, concentrador de VPN o cortafuegos. Estos dispositivos de seguridad exigen "credenciales" del dispositivo final a través de *Cisco Trust Agent* y transmiten esta información a los servidores de políticas para una decisión de admisión o negación.

**3.2.5.7.3 Cisco Secure Access Control Server.** *Cisco Secure Access Control de servidor* (SCA) (Cisco Systems, Inc, 2006) es un dispositivo que controla que se cumplan las políticas de acceso a la red. Por su integración con otros sistemas de control de acceso, mejoran la productividad de la organización y ayudan a reducir costos. Es compatible simultáneamente con múltiples escenarios, entre los que se encuentran:

- Administración del dispositivo: Autentica, autoriza a los comandos, y proporciona auditoría.

- Acceso remoto: Funciona con redes virtuales privadas (VPN) y otros dispositivos de acceso a la red remoto para hacer cumplir las políticas de acceso.
- *Wireless*: Autentica y autoriza a los usuarios y host que se conectan de manera inalámbrica y hace cumplir las políticas específicas para accesos inalámbricos.
- Control de admisión de red: Se comunica con los servidores de postura y de auditoría para hacer cumplir las políticas de control de admisión.

*Cisco Secure ACS* permite gestionar de forma centralizada el acceso a los recursos de la red para una creciente variedad de tipos de acceso, dispositivos y grupos de usuarios. Estas características son clave frente a las actuales complejidades de control de acceso a la red:

- El apoyo a una amplia gama de protocolos incluyendo protocolo de autenticación extendido (EAP), proporciona la flexibilidad necesaria para satisfacer todas las necesidades de autenticación
- La integración con los productos de Cisco para el control de acceso de administración del dispositivo permite el control centralizado y la auditoría de las acciones administrativas.
- El apoyo a bases de datos externas, los servidores de postura, y servidores de auditoría centraliza el control de la política de acceso y le permite integrar sistemas de control de acceso e identidad.

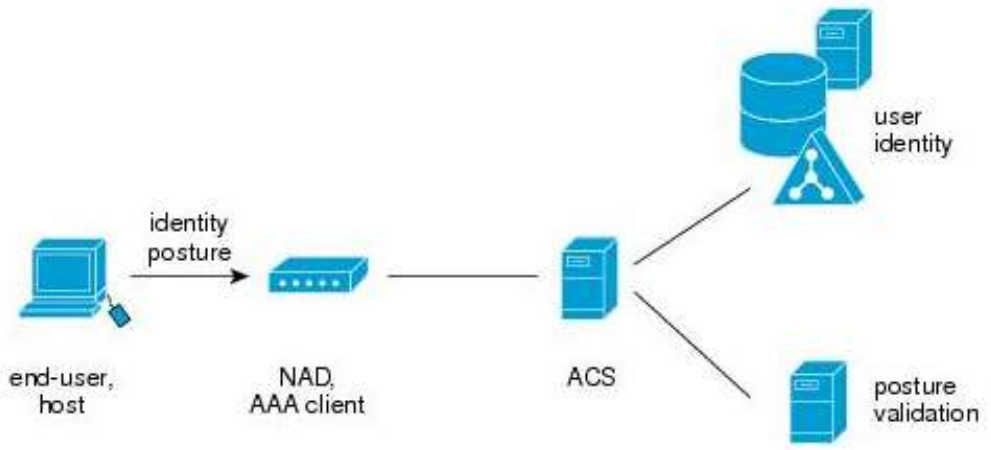
**3.2.5.7.4 Servidor de Validación De Postura.** El servidor de validación de postura puede trabajar con el control de acceso a redes (NAC). NAC utiliza la infraestructura de la red para hacer cumplir la política de seguridad en todos los dispositivos que traten de acceder a los recursos informáticos de la red. El cumplimiento de políticas de seguridad, limita el daño de las amenazas de seguridad emergentes. Mediante el uso de NAC, los clientes pueden permitir el acceso a la

red sólo para dispositivos de punto final y de confianza compatibles (tales como PCs, servidores y PDAs), y pueden restringir el acceso de dispositivos no compatibles (Cisco Systems, Inc, 2013).

El servidor de validación de postura se utiliza para determinar si un host permite el acceso a un dispositivo. Un servidor de validación de postura (PVS) es cualquier servidor que autoriza a los conjuntos de credenciales de la postura en una o más APT. Mientras que el servidor ACS es una instancia de un EVP, el término se utiliza normalmente para describir a un servidor delegado para asistir en la autorización del dominio específico de la postura credencial. Por ejemplo, un Servidor de anti-virus-(AV) puede actuar como un EVP para hacer AV de decisiones específicas de la postura desde el servidor AV sabe el último motor de exploración y las versiones de archivos de firmas.

En la Figura **10** se observa el servidor de validación de postura dentro de la arquitectura de NAC, el cual proporciona reparación a los hosts que no cumplen con los requisitos requeridos para acceder a la red.

Figura 10. Servidor de validación de postura




Fuente: Cisco Systems (2013)

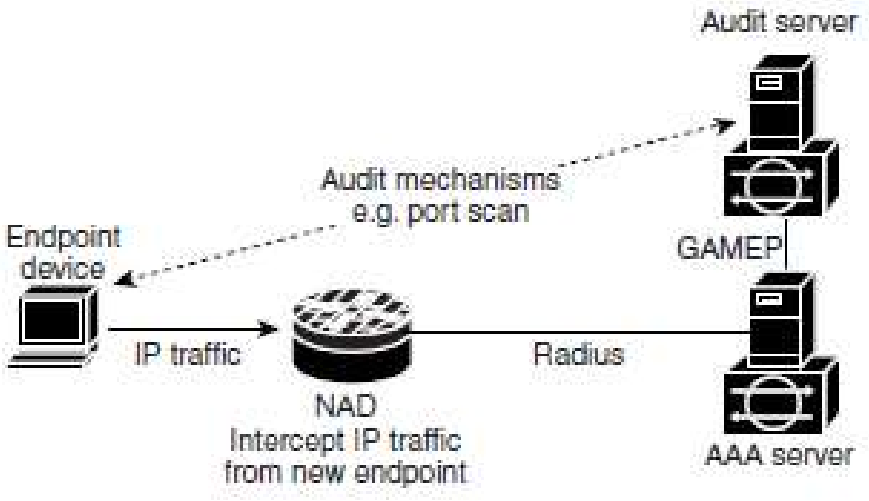
**3.2.5.7.5 Servidor de Auditoria.** El último componente de la solución NAC es el servidor de auditoría (VA), que se aplica para la evaluación de vulnerabilidades y así determinar el nivel de confianza o de riesgo de un host antes de la admisión a la red. El servidor de auditoría usa técnicas tales como el escaneo en red, acceso remoto, o basada en requisitos.

Los agentes se suelen utilizar para recopilar la información que normalmente se proporcionan por el solicitante IEEE 802.1X o CTA. El componente de servidor de auditoría es suministrado por ciertos proveedores en el Programa Cisco NAC para dar a los clientes la posibilidad de elegir un proveedor de VA y la tecnología que mejor se adapte a sus necesidades políticas y los requisitos de implementación.

El servidor de auditoría utiliza el mensaje genérico, el Protocolo de autorización para comunicarse con la información de auditoría de la AEC. ACS es responsable de desencadenar el proceso de auditoría para las máquinas sin agente con el servidor de auditoría. Mientras que el servidor de auditoría está realizando el proceso de auditoría, ACS sondea periódicamente el servidor de auditoría para una decisión de la auditoría. Cuando el servidor de auditoría completa el proceso de auditoría se informa sobre el estado de la postura de la sede de ACS.

La Figura **11** muestra como los servidores de auditoría encajan en la topología típica.

Figura 11. Servidores de auditoría




Fuente: Cisco Systems (2005)

## 1.3 ESTADO DEL ARTE

A continuación se detalla el estado del arte que se realizó a través de una investigación de carácter bibliográfico con el fin de conocer y sistematizar la producción científica que se ha desarrollado en el área de la seguridad informática y el acceso seguro a las redes corporativas por parte de terceros.

Toda la documentación revisada se organizó en cuatro grupos:

- Grupo número uno: Trabajos sobre Seguridad Informática con Control de Acceso a Redes
- Grupo número dos: Trabajos sobre guías metodológicas relacionadas con seguridad informática
- Grupo número tres: Trabajos sobre Guías Metodológicas con Control de Acceso a Redes.

- Grupo número cuatro: Trabajos que incluyen Guías Metodológicas relacionadas con Seguridad Informática, Control de Acceso a Redes e Implementación de políticas de seguridad.

En la Figura **12** se pueden observar los cuatro grupos y la literatura encontrada.

Figura 12. Estado del Arte


Fuente: Autor del proyecto

Como se muestra en la Figura **12**, no se encontraron trabajos que contemplen la implementación de políticas de seguridad en guías metodológicas ni trabajos que brinden orientaciones sobre cómo implementar políticas de control de acceso mediante la elaboración de guías metodológicas.

Cuadro 3. Condiciones de búsqueda para selección de literatura

| Palabras clave | Bases de datos consultadas | Total de referencias recuperadas | Rango de fecha de búsqueda: | Pertinencia con el tema de investigación: |
|---|---|---|---|---|
| Redes de Computadores, Seguridad, Telemática, Redes Informáticas Políticas de Seguridad, Protocolos, Tecnología de la información, Telecomunicaciones, Diagnóstico, Guías Metodológicas, Control de Acceso a Redes, Análisis y evaluación de riesgos, Estándar ISO | Google Scholar Scopus | Scopus: 10 Google Scholar: 25 | Entre los años 2006-2015 | Seguridad Informática, Control de acceso a redes. C-NAC. |

Fuente: Autor del proyecto

**1.3.1 Trabajos sobre seguridad informática con control de acceso a la red**. El siguiente cuadro muestra los criterios de búsqueda que se tuvieron en cuenta para seleccionar la literatura pertinente y relacionada con las áreas de estudio de Seguridad Informática con Control de Acceso a Redes que apoyaron con sus diferentes teorías en la realización del proyecto:

Cuadro 4. Literatura relacionada con seguridad informática y control de acceso a la red

| Autor | Título | ¿Se revisa el concepto de Seguridad Informática? | ¿Se revisa el concepto de Control de Acceso a Redes - NAC? | ¿Presenta políticas de acceso definidas para controlar acceso a la red? |
|---|---|---|---|---|
| Esmoris, Daniel Omar. 2010 | Control de acceso a redes | SI | SI | NO |
| Cisco Systems, Inc | Cisco Network Admission Control (NAC) solution | SI | SI | NO |
| Cisco Systems, Inc | Implementing Network Admission Control Phase One Configuration and Deployment | SI | SI | NO |
| Einstein, A., B. Podolsky, and N. Rosen, 1935 | Towards Trusted Network Access Control | SI | SI | NO |

| Autor | Título | ¿Se revisa el concepto de Seguridad Informática? | ¿Se revisa el concepto de Control de Acceso a Redes - NAC? | ¿Presenta políticas de acceso definidas para controlar acceso a la red? |
|---|---|---|---|---|
| Kim, Hyuncheol. 2007 | Access Control Capable Integrated Network Management System for TCP/IP Networks | SI | SI | NO |
| Metalobos, Juan Manuel | Análisis de los riesgos de seguridad de la infomación | SI | NO | NO |
| Bustamante Sánchez, Ruben | Seguridad en redes | SI | NO | NO |
| Areitio, Javier | Seguridad de la Información: Redes, informática y sistemas de la información | SI | SI | NO |
| Cisco Networking Academy | CCNA Exploration 4.0 Accediendo a la WAN | SI | NO | NO |
| González Gómez, Diego | Sistemas de detección de intrusiones | SI | SI | NO |

Fuente: Autor del proyecto

De acuerdo a la información anterior, se puede evidenciar que existen trabajos que interrelacionan conceptos de seguridad informática y control de acceso relacionados con la protección a la estructura de red de una organización pero no se evidencian teorías sobre los tipos de políticas que se deban implementar para prevenir posibles ataques o posibles amenazas.

**1.3.2 Trabajos sobre guías metodológicas relacionadas con seguridad informática**. El siguiente cuadro muestra los criterios de búsqueda que se tuvieron en cuenta para seleccionar la literatura pertinente y relacionada con las áreas de estudio de guías metodológicas relacionadas con seguridad informática, que apoyaron con sus diferentes teorías en la realización del proyecto:

Cuadro 5. Literatura sobre guías metodológicas relacionadas con seguridad informática.

| Autor | Título | ¿Se revisa el concepto de Seguridad Informática? | ¿Se revisa el concepto de Implementación de Políticas de Seguridad en las organizaciones? | ¿Se revisa el concepto de guías metodológicas? |
|---|---|---|---|---|
| González Gómez, Diego | Sistema de detección de intrusos | SI | NO | SI |
| Franco, David A. | Metodología para la Detección de Vulnerabilidades en Redes de Datos | SI | NO | SI |
| Sánchez Acevedo, Nicolás | Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática. | SI | NO | SI |
| Ayala Puentes, Christian | Guía Metodológica para el mejoramiento, gestión y seguridad en redes informáticas de Centros Educativos en base a soluciones abiertas, el modelo de gestión Internet y el RFC 2196 Site Security Handbook | SI | NO | SI |
| Jiménez Orellana, Julia | Análisis de soluciones de acceso seguro a la red | SI | NO | SI |

Fuente: Autor del proyecto

Con la información suministrada en el cuadro anterior, se puede concluir que una vez realizada la búsqueda de literatura, se encontraron trabajos que mencionan el concepto de seguridad informática y algunas de sus secciones muestran la implementación de guías metodológicas pero a su vez no se encontraron trabajos que mencionaran la definición e implementación de políticas de seguridad.

**1.3.3 Trabajos sobre Guías metodológicas y control de acceso a redes**. El siguiente cuadro muestra los criterios de búsqueda que se tuvieron en cuenta para seleccionar la literatura pertinente y relacionada con las áreas de estudio de guías metodológicas en implementación de control de acceso a redes, que apoyaron con sus diferentes teorías en la realización del proyecto:

Cuadro 6.Literatura relacionada con guías metodológicas y control de acceso a redes

| Autor | Título | ¿Se revisa el concepto de Control de acceso a redes? | ¿Se revisa el concepto de implementación de control de acceso a la red en las Organizaciones? | ¿Se revisa el concepto de implementación de guías para implementación de control de acceso a la red? |
|---|---|---|---|---|
| Cisco Systems, Inc. | Network Admission Control Software Configuration Guide | SI | NO | SI |
| Hasham Ud-Din Qazi | Comparative Study of Network Access Control Technologies | SI | NO | SI |
| Runipulla, Blanca Inés | Análisis de soluciones de acceso seguro a la red e implementación de un proyecto piloto para la Unidad Educativa Técnico Salesiano | SI | NO | SI |
| Esmoris, Daniel Omar | Control de Acceso a Redes | SI | NO | SI |
| Cisco Systems, Inc. | Implementing Network Admission Control Phase One Configuration and Deployment | SI | NO | SI |

Fuente: Autor del proyecto

A partir de la información suministrada en el cuadro anterior, se puede concluir que no se encontró literatura en donde se muestre claramente cómo aplicar el concepto de control de acceso a redes en las organizaciones, se evidencia que hay literatura que mencionan y explican el funcionamiento de esta tecnología y como a través de una serie de pasos e indicaciones se podría implementar.

**3.3.4 Trabajos que incluyen Guías Metodológicas relacionadas con Seguridad Informática, Control de Acceso a Redes e Implementación de políticas de seguridad.** El Cuadro **7** muestra los criterios de búsqueda que se tuvieron en cuenta para seleccionar la literatura pertinente y relacionada con las áreas de estudio de guías metodológicas en implementación de control de acceso a redes y

políticas de seguridad, que apoyaron con sus diferentes teorías en la realización del proyecto:

Cuadro 7. Literatura relacionada con implementación de políticas de seguridad y control de acceso a redes en guías metodológicas

| Autor | Título | ¿Se revisa el concepto de Implementación de políticas de seguridad? | ¿Se revisa el concepto de implementación de control de acceso a la red en las Organizaciones? | ¿Se revisa el concepto de guías metodológicas para implementación de de políticas de seguridad en plataformas para control de acceso? |
|---|---|---|---|---|
| Metalobos, Juan Manuel | Análisis de los riesgos de seguridad de la información | SI | NO | NO |
| Bustamante Sánchez, Ruben | Seguridad en redes | SI | NO | NO |
| Areitio, Javier | Seguridad de la Información: Redes, informática y sistemas de la información | SI | NO | NO |
| Cisco Networking Academy | CCNA Exploration 4.0 Accediendo a la WAN | SI | NO | NO |
| González Gómez, Diego | Sistemas de detección de intrusiones | SI | NO | NO |
| Franco, David A. | Metodología para la Detección de Vulnerabilidades en Redes de Datos | SI | NO | NO |
| Sánchez Acevedo, Nicolás | Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática. | SI | NO | NO |
| Ayala Puentes, Christian | Guía Metodológica para el mejoramiento, gestión y seguridad en redes informáticas de Centros Educativos en base a soluciones abiertas, el modelo de gestión Internet y el RFC 2196 Site Security Handbook | SI | NO | NO |

Fuente: Autor del proyecto

De acuerdo al análisis realizado en las referencias seleccionadas, se puede determinar que son pocos los estudios que se han realizado sobre el tema en mención y que de los resultados obtenidos su tema central no es el diseño de guías metodológicas para implementar control de admisión a la red mediante la definición de políticas de seguridad. Siendo esta la justificación a la propuesta de investigación del proyecto.

## 3.4 MARCO LEGAL

La Ley 1273 del 5 de enero (2009), reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 (Organización Mundial de la Propiedad Intelectual, 1989) se reglamenta la inscripción del soporte lógico (*software*) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de *software*. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. En este mismo sentido y en el entendido de que el soporte lógico o *software* es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano (Congreso de Colombia, 2000).

Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

El Código Penal colombiano, Ley 599 en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías (Congreso de Colombia, 2000), trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

La Ley 1273 (Congreso de Colombia, 2009) complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones. A partir de ésta Ley, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos

personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos", con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

Con los desarrollos jurídicos hasta ahora logrados acerca de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral (Ojeda Pérez , 2010).

# 4. DESCRIPCIÓN DEL PROCESO INVESTIGATIVO

El presente capítulo tiene el propósito de describir el tipo de investigación, etapas del proyecto, población, muestra, técnicas e instrumentos de recolección de información y actividades realizadas para cumplir con los resultados derivados de los objetivos planteados de la investigación realizada.

## 1.1 TIPO DE INVESTIGACIÓN

La presente investigación pretende documentar mediante la elaboración de una guía metodológica para la implementación de políticas de control de acceso, que se puede llevar a cabo un estricto control sobre los dispositivos que intentan conectarse de manera cableada e inalámbrica a las diferentes redes corporativas y que puede garantizar las características fundamentales de los sistemas de información. Para tal efecto se hace uso de una ***metodología con enfoque cualitativo inductivo***. La recolección de los datos está orientada a proveer de un mayor entendimiento de los significados y experiencias de las personas. El investigador es el instrumento de recolección de los datos, se auxilia de diversas técnicas que se desarrollan durante el estudio. Es decir, no se inicia la recolección de los datos con instrumentos preestablecidos, sino que el investigador comienza a aprender por observación y descripciones de los participantes y concibe formas para registrar los datos que se van refinando conforme avanza la investigación. El análisis varía dependiendo del modo en que hayan sido recolectados los datos, se fundamenta en la inducción analítica, realiza un uso moderado de la estadística (conteo, algunas operaciones aritméticas, se basa en casos o personas y sus manifestaciones, es simultánea a la

recolección de los datos, finalmente el análisis consiste en describir información y desarrollar temas. (Hernández Sampieri, 2010).

Para realizar la guía de implementación, el proceso se dividió en etapas sucesivas y sistemáticas; en cada una de ellas se trata de establecer objetivos y metas claras con productos entregables, donde los productos resultado de la primera etapa, servirán para adelantar la segunda y los de las segunda servirán para proseguir con la tercera etapa y así sucesivamente, ya que se plantea que el control que se haga una vez se realice la implementación, debe ser periódico o permanente dependiendo de la organización y los cambios en la tecnología de información usada en el control de acceso a la red.

**1.1.1 Etapa de recolección de información**. Se diseñó y diligenció un formato para el levantamiento del inventario de equipos activos de red y servidores de autenticación de la UNAB. Se desarrolló un formato de entrevista para el levantamiento de requerimientos de políticas de seguridad que se implementarán a futuro en la Infraestructura de red de la UNAB.

**4.1.2 Etapa de análisis de información.** A partir de toda la información recolectada en la sección anterior, se creó una matriz de comparación para cruzar la información de las características de los equipos activos y servidores de autenticación actuales, comparada contra los requerimientos que demanda CNAC para su implementación. Como resultado de la matriz se realizó la guía y sus respectivas recomendaciones para la adquisición de los elementos que se requieran para implementar NAC, formulando la metodología de Implementación.

**1.1.2 Etapa de Verificación.** Se creó una matriz que permitió comparar los elementos que se instalarán según la propuesta metodológica versus los requerimientos levantados en el formato "levantamiento de la información" diligenciado por el Ingeniero José Gregorio Hernández, como director de

Infraestructura Tecnológica, con el propósito de validar el cumplimiento de cada uno de los requerimientos solicitados para implementar.

## 4.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

A continuación se describen las fuentes de información que hicieron parte de la recolección de datos para la continuidad del proyecto:

Fuentes Primarias: Entre las fuentes primarias de información utilizadas en el estudio investigativo descriptivo se encuentran la asesoría del director de infraestructura tecnológica, docentes de la Universidad Autónoma de Bucaramanga y demás personas y entidades que provean información base para este estudio; se utilizó la encuesta al Ingeniero José Gregorio, del área objeto de estudio; todo esto con el fin de conocer las características de los dispositivos Cisco con los cuales se cuenta y de esta manera poder obtener una visión clara de los procedimientos realizados en la misma. En este estudio se emplearon los instrumentos de recolección de información como: la entrevista en la cual se definieron las políticas generales a implementar en la UNAB y el formato de levantamiento de información que contiene las características físicas de los dispositivos con los cuales cuenta la infraestructura de red. Ver Anexo 2 y Anexo **4**

Fuentes Secundarias: Entre las fuentes secundarias de información se tuvo en cuenta la información extraída de libros y diferentes bases de datos online como el caso de Google Scholar, Scopus, entres otras. Los daos que se obtuvieron una vez aplicados los instrumentos de recolección de la información, fueron analizados cuantitativamente a través de cuadros y gráficas, mediante la interpretación de los datos numéricos y el análisis de cada respuesta para la forma cualitativa.

## 4.3. ACTIVIDADES REALIZADAS

A continuación, se describen las actividades que se llevaron a cabo para cumplir con los objetivos planteados.

**4.3.1. Actividades que se realizaron para cumplir con el primer objetivo específico del proyecto**. Para cumplir con el primer objetivo y tener como resultado final del mismo la entrega del documento que contiene la literatura relacionada con seguridad en redes empresariales y control de acceso a la red, se llevaron a cabo las actividades indicadas en el Cuadro **8**:

Cuadro 8. Actividades que se realizaron para cumplir con el primer objetivo específico del proyecto

| Primer Objetivo | Resultado | Actividades |
|---|---|---|
| Elaborar un documento que contenga la revisión de la literatura sobre seguridad en redes empresariales y control de acceso a la red | Un documento con la revisión de la literatura sobre seguridad en las redes empresariales y control de acceso a la red | 1. **Selección de los criterios de búsqueda y su pertinencia en el tema de investigación**. Para esta selección, se tuvieron en cuenta temas como seguridad informática en las organizaciones, guías metodológicas y control de acceso a la red en arquitecturas propietarias como por ejemplo, Cisco.<br><br>2. **Revisión de literatura seleccionada**. Una vez se definió el tipo de literatura a investigar, se realizaron consultas en bases de datos como Scopus y Google Scholar, con el fin de poder obtener información que pudiera brindar las teorías suficientes para la elaboración del documento.<br><br>3. **Elaboración del documento.** Una vez se finalizó el proceso de lectura, se procedió a la realización del documento teniendo como parámetros iniciales, mostrar una estructura detallada de cada tema empezando por la seguridad informática y finalizando con Network Asset Collector como solución propietaria de Cisco. |

Fuente: Autor del proyecto

**4.3.2. Actividades que se realizaron para cumplir con el segundo objetivo específico del proyecto.** Para cumplir con el segundo objetivo y tener como resultado final del mismo, el diagnóstico del estado de los equipos cisco que tiene la UNAB se llevaron a cabo las siguientes actividades:

Cuadro 9. Actividades que se realizaron para cumplir con el segundo objetivo específico del proyecto

| Segundo Objetivo | Resultado | Actividades |
|---|---|---|
| Diagnosticar el estado de los equipos cisco que tiene la UNAB en donde se implementará NAC. | Diagnóstico del estado actual de la infraestructura de red de la UNAB. | 1. **Diseño del formato de levantamiento de información.** Para diseñar este formato se tuvieron en cuenta aspectos tales como, Sede, Ubicación física, Fabricante, Referencia. Equipo, Modelo, Puertos, Serial y Cantidad.<br><br>2. **Levantamiento de la información.** Una vez se realizó el formato el cual figura como Anexo 2, en la sección de ***Anexos***, identificado como **F.L.I.,** se procedió al levantamiento de la información, la cual fue suministrada por el Ingeniero José Gregorio Hernández, jefe de Infraestructura Tecnológica. Con esta información, se realizó el diagnóstico el cual figura en la sección ***Anexos*** del documento.<br><br>3. **Diagnóstico del estado actual de la infraestructura de red de la UNAB.** Con la información recopilada en el formato de levantamiento de información, se realizó un diagnóstico sobre el estado actual de la infraestructura de red de la UNAB, el cual se comparó con los requerimientos de hardware y software establecidos para la implementación de la solución de Control de Acceso Seguro, propietaria de Cisco. |

Fuente: Autor del proyecto

**4.3.3 Actividades que se realizaron para cumplir con el tercer objetivo específico del proyecto.** Para cumplir con el tercer objetivo y tener como resultado final del mismo, diseñar una guía metodológica para la implementación de la solución NAC en los equipos Cisco de la UNAB, se llevaron a cabo las siguientes actividades:

Cuadro 10. Actividades que se realizaron para cumplir con el tercer objetivo específico del proyecto

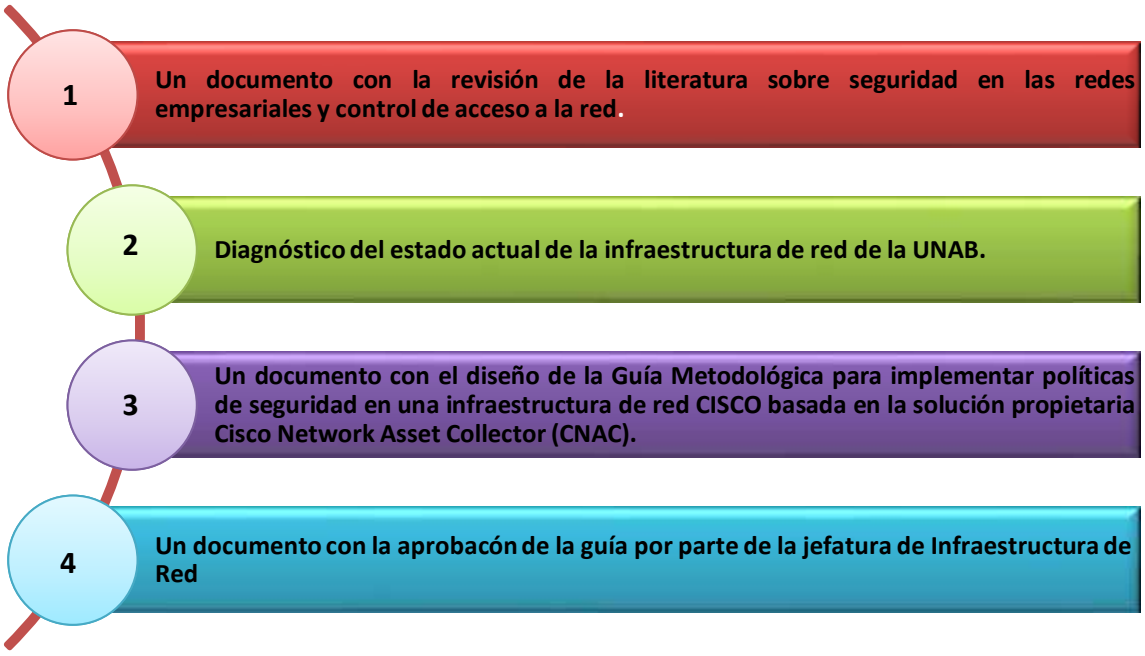
| Tercer Objetivo | Resultado | Actividades |
|---|---|---|
| Diseñar una guía metodológica para la implementación de la solución NAC en los equipos Cisco de la UNAB. | Un documento con el diseño de la Guía Metodológica para implementar políticas de seguridad en una infraestructura de red Cisco basada en la solución propietaria Cisco Network Asset Collector (CNAC). | 1. **Levantamiento de Políticas de Seguridad.** Para llevar a cabo esta actividad, se diseñó el formato de Entrevista, el cual figura como Anexo 3 en la sección de Anexos identificado como: **F.E.D.P.S-UNAB2016**. Estos requerimientos internos fueron suministrados por el Ingeniero José Gregorio Hernández, jefe de Infraestructura Tecnológica de la UNAB.<br><br>2. **Revisión de los requerimientos de hardware y software para la implementación de la solución propietaria de Cisco.** Se revisaron los requerimientos necesarios para implementar CNAC como solución para controlar el acceso a la red interna de la UNAB por parte de terceros.<br><br>3. **Realización comparativo entre estado actual de la infraestructura de red de la UNAB versus los requerimientos de Cisco**. Se revisaron las características de los equipos de la UNAB y se compararon con los solicitados por Cisco para concluir si eran compatibles con los requerimientos para instalar control de acceso a la red. Este comparativo se puede evidenciar en el Anexo 5 identificado como: Comparativo infraestructura UNAB vs Requerimientos CNAC.<br><br>4. **Realización de la guía metodológica.** Una vez finalizado el comparativo, se realizó el documento denominado Guía Metodológica para la implementación de políticas de seguridad en la UNAB usando la plataforma propietaria de Cisco, CNAC el cual contiene todo lo necesario para que en la Universidad Autónoma de Bucaramanga, se implemente la solución NAC.<br><br>5. **Revisión y aprobación de la guía por parte de la jefatura de Infraestructura de Red.** Para la aprobación de la guía metodológica, se envió al correo del Ingeniero José Gregorio Hernández, quien después de una detallada revisión, validó la información almacenada en dicha guía y su importancia en la implementación de la solución NAC. |

Fuente: Autor del proyecto

# 5. RESULTADOS

En la Figura **13** se detallan los resultados obtenidos en la realización del proyecto, cada uno de éstos, está soportado en la sección de Anexos.

Figura 13. Resultados obtenidos




Fuente: Autor del proyecto

## 5.1 DOCUMENTO CON LA REVISIÓN DE LA LITERATURA SOBRE SEGURIDAD EN LAS REDES EMPRESARIALES Y CONTROL DE ACCESO A LA RED.

Este documento soportado en la sección de Anexos, muestra todo el proceso de investigación que se realizó teniendo en cuenta los criterios de búsqueda establecidos inicialmente en el resumen sección palabras claves. Una vez se realizó la selección de literatura pertinente, se continuó con la realización y construcción del documento final.

## 5.2 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA INFRAESTRUCTURA DE RED DE LA UNAB

Este documento soportado en la sección de Anexos, muestra el diagnóstico que se realizó una vez se llevó a cabo el levantamiento de la información. Este diagnóstico presenta las características actuales de los dispositivos de red con los cuales cuenta la Universidad Autónoma de Bucaramanga – UNAB, en su departamento de Infraestructura Tecnológica.

**El**

Cuadro **1** Diagnóstico de levantamiento de información, describe el tipo de necesidad/problema/vulnerabilidad/debilidad que se presenta en la UNAB cuando un usuario intenta conectarse a la red ya sea de manera cableada o inalámbrica, el nombre de cada tipo seleccionado, la descripción y la evidencia encontrada una vez se realizó el levantamiento de la información y por último la propuesta o requerimiento que se cubre con el diseño de la guía metodológica.

Cuadro 11. Diagnóstico Levantamiento de Información

| Tipo | Nombre | Descripción | Evidencia | Propuesta o Requerimiento |
|---|---|---|---|---|
| Vulnerabilidad | Conexión equipos externos red cableada | Posibilidad de conexión de un equipo de cómputo a la red cableada y permitir el acceso a la red | Se encuentra en el levantamiento de información que algunos puntos de red cableada, permiten la asignación de IP por DHCP y esto valida al equipo de cómputo a conectarse a la red y poder tener un posible acceso a los servicios y demás infraestructura. | Se requiere del proceso de autenticación a través de entrega de credenciales tales como usuario y contraseña. Previamente se sugiere una validación de capa 2 en donde se valide la MAC del equipo que se está conectando. |
| Vulnerabilidad | Cumplimiento de estado actualizado de los equipos de cómputo | Los equipos de cómputo que se conectan a la red cableada o inalámbrica pueden estar desactualizados en cuanto a parches de seguridad y service pack de sistemas operativos y aplicativos que puedan comprometer la seguridad de la red o segmento de red donde se conectan. | Se encuentra en el levantamiento de información que los equipos que logran conectarse a la red cableada o inalámbrica pueden estar sin actualizaciones de seguridad en sus sistemas operativos y su acceso no es limitado o denegado. | Se requiere que se revise el estado en el cual se encuentra el dispositivo al momento de solicitar el acceso a la red corporativa. Si el dispositivo no cumple con los requerimientos establecidos, se debe denegar el acceso. |
| Autenticación | Conexión autenticada a la red inalámbrica | Los equipos de cómputo que se conectan a la red inalámbrica lo hacen sin requerimiento de autenticación, lo cual permite que cualquier tipo de usuario se conecte y pueda generar algún tipo de ataque a esta red. | Se encuentra en el levantamiento de información que los equipos de cómputo que se conectan a la red inalámbrica lo hacen sin ser requerido ningún tipo de autenticación en cualquiera de los campus. | Se requiere que los dispositivos que intentan conectarse a la red de manera cableada o inalámbrica pasen por un proceso de autenticación previo a la conexión. |
| Seguridad | Cumplimiento actualización antivirus | Los equipos de cómputo que se conectan a la red cableada o inalámbrica pueden estar desactualizados en la base de datos del antivirus que tengan instalado, poniendo en riesgo la seguridad de la información de los equipos pertenecientes al mismo segmento de red o incluso toda la red de la Universidad. | Se encuentra en el levantamiento de información que los equipos de cómputo que se conectan a la red cableada o inalámbrica pueden estar sin actualización de la base de datos del antivirus y su acceso no es limitado o denegado. | Se requiere que se revise el estado en el cual se encuentra el dispositivo al momento de solicitar el acceso a la red corporativa. Si el dispositivo no cumple con los requerimientos establecidos, se debe denegar el acceso. |
| Vulnerabilidad | Actualización IOS equipos de conectividad | Los equipos de red tales como Switches de acceso presentan versiones no actualizadas de sus IOS (Sistemas Operativos) lo cual representa una vulnerabilidad a posibles bugs de seguridad o funcionamiento. | Se encuentra en el levantamiento de información que las versiones de los IOS de los Switches de Acceso no están actualizados a la última versión soportada por el fabricante. | Se requiere que por parte del personal de infraestructura tecnológica se realicen las respectivas actualizaciones para que de esta manera puedan ser tenidos en cuenta para la implementación de la solución propietaria de Cisco. |

## 5.3 DOCUMENTO CON EL DISEÑO DE LA GUÍA METODOLÓGICA PARA IMPLEMENTAR POLÍTICAS DE SEGURIDAD EN UNA INFRAESTRUCTURA DE RED CISCO BASADA EN LA SOLUCIÓN PROPIETARIA CISCO NETWORK ASSET COLLECTOR (CNAC).

Este documento soportado en la sección de Anexos, muestra la guía metodológica que se diseñó para implementación de políticas de seguridad utilizando la solución propietaria de Cisco, denominada Network Asset Collector e identificada por sus siglas en inglés como CNAC. Esta guía está construida en fases consecutivas, con el fin de llevar a cabo dicha implementación como una solución para proteger el acceso a usuarios no autorizados a todos los servicios de red de la UNAB. En el cuadro se puede evidenciar como la guía cumple con el requerimiento de la organización.

Cuadro 12. Cumplimiento de la guía con base en el requerimiento de la Organización

| Propuesta o Requerimiento | Característica de la guía para atender el requerimiento. |
|---|---|
| Se requiere del proceso de autenticación a través de entrega de credenciales tales como usuario y contraseña. | El cisco secure ACS junto con su servidor de autenticación solicita las credenciales de autenticación del Cisco Trust Agent instalado en el cliente, si esta información no coincide con la almacenada en la base de datos, el acceso será negado. |
| Se requiere que se revise el estado en el cual se encuentra el dispositivo al momento de solicitar el acceso a la red corporativa. Si el dispositivo no cumple con los requerimientos establecidos, se debe denegar el acceso. | El Dispositivo de acceso a la red (NAD) solicita las credenciales de salud al Cisco Trust Agent (CTA). Las credenciales de salud son: antivirus actualizado, parches del sistema operativo instalados y firewall correctamente configurado. Si el dispositivo no cumple con estas características pero cumple con las credenciales de autenticación es enviado a un servidor de remediación quien se encarga de realizar las respectivas actualizaciones en el cliente. |
| Se requiere que los dispositivos que intentan conectarse a la red de manera cableada o inalámbrica pasen por un proceso de autenticación previo a la conexión. | El cisco secure ACS junto con su servidor de autenticación solicita las credenciales de autenticación del Cisco Trust Agent instalado en el cliente, si esta información no coincide con la almacenada en la base de datos, el acceso será negado. |

| Propuesta o Requerimiento | Característica de la guía para atender el requerimiento. |
|---|---|
| Se requiere que se revise el estado en el cual se encuentra el dispositivo al momento de solicitar el acceso a la red corporativa. Si el dispositivo no cumple con los requerimientos establecidos, se debe denegar el acceso. | El Dispositivo de acceso a la red (NAD) solicita las credenciales de salud al Cisco Trust Agent (CTA). Las credenciales de salud son: antivirus actualizado, parches del sistema operativo instalados y firewall correctamente configurado. Si el dispositivo no cumple con estas características pero cumple con las credenciales de autenticación es enviado a un servidor de remediación quien se encarga de realizar las respectivas actualizaciones en el cliente. |
| Se requiere que por parte del personal de infraestructura tecnológica se realicen las respectivas actualizaciones para que de esta manera puedan ser tenidos en cuenta para la implementación de la solución propietaria de Cisco. | Una vez revisadas las características de hardware y software de los dispositivos de red, es posible realizar la implementación de la solución de acceso seguro propietaria de Cisco ya que algunos dispositivos cumplen con las características mínimas solicitadas por el fabricante, pero para un mejor resultado al momento de implementar la solución, se sugieren que se actualicen los sistemas operativos de los Switches. |

Fuente: Autor del proyecto

## 5.4 DOCUMENTO CON LA APROBACIÓN DE LA GUÍA POR PARTE DE LA JEFATURA DE INFRAESTRUCTURA DE RED.

Este documento soportado en la sección de Anexos, muestra la revisión y aprobación de su aplicabilidad por parte del jefe de Infraestructura de Red de la Universidad Autónoma de Bucaramanga – UNAB. Este documento consta de una carta de aceptación.

# 6. CONCLUSIONES Y RECOMENDACIONES

El presente capítulo tiene el propósito de describir las conclusiones y recomendaciones obtenidas con la realización del proceso de investigación de tema de estudio.

## 6.1 CONCLUSIONES

Como resultado de la investigación realizada, se puede concluir que las organizaciones utilizan diversas soluciones para proteger sus infraestructuras de red y a su vez proteger su información, estas soluciones algunas veces son diseñadas directamente por quienes trabajan en las áreas de tecnologías de dichas organizaciones; pero en otras ocasiones son tomadas de soluciones propietarias que ofrecen sus fabricantes, una de estas soluciones, es el Control de Acceso a la Red que ofrece Cisco Systems a través de su plataforma que ayudarán a las organizaciones a protegerse de las amenazas como spyware, virus y gusanos que intenten acceder a la red corporativa a través de una variedad de dispositivos. Es así como analizada la información, ésta solución resuelve de manera inicial la problemática presentada en la Red de la Universidad Autónoma de Bucaramanga - UNAB la cual actualmente no cuenta con un sistema que permita la implementación de políticas de seguridad robustas para tener un control más efectivo y eficiente en las conexiones de redes cableadas e inalámbricas. Adicional a esto, requiere de un sistema de gestión que permita la administración de políticas de forma centralizada de tal forma que se puedan distribuir dentro de la infraestructura Cisco. A la pregunta de investigación planteada inicialmente, podemos concluir que la guía

metodológica de acceso a la red ayudará a reducir el nivel de vulnerabilidad en cuanto a la negación de los servicios de red, canales Internet, perfilamiento en la infraestructura de red de la UNAB ya que controla el acceso de los dispositivos mediante una autenticación y diagnóstico inicial el cual permite detectar si el equipo que requiere acceso a la red cumple o no con las condiciones requeridas en las políticas implementadas. Dentro de la búsqueda bibliográfica que se realizó no se encontraron trabajos que mencionen específicamente guías metodológicas para la implementación de políticas de seguridad utilizando la solución propietaria de Cisco, esto quiere decir, que el diseño de esta guía es de gran aporte a los procesos de investigación futuros que se realicen en el área de la seguridad informática y del control de acceso a las redes. En un futuro próximo sería útil y valiosa su implementación en la UNAB, ya que como se mencionó anteriormente sería una de las soluciones a la problemática actual.

## 6.2 RECOMENDACIONES

En función de los resultados y conclusiones que se obtuvieron con el desarrollo del proyecto y el cumplimiento de los objetivos, se recomiendan las siguientes acciones:

- Teniendo en cuenta que el alcance de este proyecto no era de implementación, se requiere de un trabajo que se dedique a la implementación donde se sugiere que se investigue el proceso de configuración e instalación de cada uno de los componentes que hacen parte de la solución *Network Asset Collector de Cisco*.
- Realizar la actualización con respecto al hardware que actualmente hace parte de la suite de dispositivos de acceso a la red con los cuales cuenta la UNAB. Esta actualización es pieza clave dentro de la implementación de la solución de Cisco.

- Poner en práctica la guía metodológica para implementar las políticas de seguridad en la infraestructura de red de la UNAB.

## REFERENCIAS


Corporación Colombia Digital . (07 de 04 de 2015). *Teletrabajo en Catastro Distrital, un nuevo avance.* Obtenido de Aumentar la productividad, mejorar la movilidad empresarial y virtualizar las compañías son algunos beneficios de adoptar esta modalidad.: http://colombiadigital.net/actualidad/noticias/item/8237-teletrabajo-en-catastro-distrital-un-nuevo-avance.html

Intelligent Community Forum (ICF). (11 de 2015). *The Smart21 Communities - Smart 21 of 2016*. Obtenido de Intelligent Communities of the year : https://www.intelligentcommunity.org/index.php?submenu=Awards&src=gendocs&ref=Smart21&category=Events

International Telecommunication Union - ITU. (s.d. de s.m. de 2013). *Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?* Obtenido de https://itunews.itu.int/Es/3702-Proteccion-de-datos-y-privacidad-en-la-nube-BR-Quien-es-el-propietario-de-la-nube.note.aspx

World Wide Web Consortium (W3C). (3 de 12 de 2015). *W3C Standards*. Obtenido de http://www.w3.org/standards/webofdevices/

Abown, G. (2012). Towards a Better Understanding of Context and Context-Awareness. *Proc. 1st international symposium on Handheld an Ubiquitous Computing. Springer-Verlag, Londres*, 304-307. Obtenido de ftp://ftp.cc.gatech.edu/pub/gvu/tr/1999/99-22.pdf

Access to European Union Law. (23 de 11 de 1995). *Official website of the European Union*. Obtenido de Diario Oficial n° L 281 de 23/11/1995 p. 0031 - 0050: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046

Ackerman, M., Darrell, T., & Weizner, D. (2001 ). *Privacy in Context.* Human-Computer Interaction.

Aguilera López, P. (2010). *Seguridad Informática.* Barcelona: Editex. Obtenido de https://books.google.com.co/books?isbn=8497717619

Aguillón Martínez, E. (2012). *Fundamentos de Criptografía.* México: UNAM, Laboratorio de Redes y Seguridad. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/13-servicios-y-mecanismos-de-seguridad/131-servicios-de-seguridad

Ahn, S., Lim, Y., Mun, Y., & Kim, H. (2005). Access control capable integrated network management system for TCP/IP networks. En *Computational Science and Its Applications--ICCSA 2005* (págs. 676--685). Springer Berlin Heidelberg.

Asamblea Nacional Constituyente (1991). (1991). *Constitución Política de Colombia 1991.* Bogotá: República de Colombia. Obtenido de http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Asamblea Nacional Constituyente 1991. (2006). *Nueva Constitución Política de Colombia 1991.* Bogotá: Unión Ltda. Obtenido de http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Augusto, J. C., Nakashima, H., & Agh, H. (2010). Ambient Intelligence and Smart Environments:A State of the Art. 1-29.

Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthe, D. (2011). Security and Privacy in your Smart City. *Centre Tecnologic de Telecomunicacions de Catalunya (CTTC),Spain - IEEE*, 1-6. Obtenido de http://www.cttc.es/publication/security-and-privacy-in-your-smart-city/

Batty , M., Axhausen, K., Pozdnoukhov, A., Fosca, G., Bazzani, A., Wachowicz, M., . . . Portugali, Y. (2012). Smart Cities of the Future. En C. f. London, *Working Papers Series Paper 188 -Oct 12 Smart Cities of the Future* (págs. 1-40). London: UCL CENTRE FOR ADVANCED SPATIAL ANALYSIS. Obtenido de https://www.bartlett.ucl.ac.uk/casa/pdf/paper188

BBC News. (17 de 01 de 2014). Edward Snowden: Leaks that exposed US spy programme. *BBC NEWS on Internet*. Obtenido de http://www.bbc.com/news/world-us-canada-23123964

BCS. (06 de 2014). *http://www.bcs.org/.* Obtenido de BYOD, CYOD, BYOT, BYOA and more: http://www.bcs.org/content/conWebDoc/52926

Behrooz, A. (01 de 2010). *Privacy of Mobile Users in Contextaware Computing Environments Master of Science Thesis.* Stockholm, Sweden : Royal Institute of Technology Department of Computer and Systems Sciences (KTH Information Communication Tecnology) TRITA-ICT-EX-2011:233. Obtenido de http://www.diva-portal.org/smash/get/diva2:512292/FULLTEXT01.pdf

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

BeVier, L. R. (1995). Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. *William & Mary Law Review*, 455. Obtenido de http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1489&context=wmborj

BHERT. (18 de 01 de 2015). *Internet of Everything - Powering the Smart Campus & the Smart City:Geelong's Transformation to a Smart City.* (B. B. Table, Ed.) Obtenido de In parthershio with University Deakin Worldly Australia, Cisco e IBM: http://www.bhert.com/events/2015-06-08/BHERT-Smart-City-Agenda-June-18.pdf

BID. (2015). *Iniciativa CIUDADES EMERGENTES y SOSTENIBLES*. Obtenido de Banco Interamericano de Desarrollo: http://www.iadb.org/es/temas/ciudades-emergentes-y-sostenibles/ciudades-usando-el-enfoque-de-desarrollo-urbano-sostenible,6693.html

Bort, J. (2012). *Managing An Explosion Of Mobile Devices And Apps In The Enterprise.* Obtenido de http://www.businessinsider.com/how-companies-are-managingthe-explosion-of-mobile-devices

Boulton, A. B. (2011). Cyberinfrastructures and "smart" world cities: Physical, human, and soft infrastructures. *In P. Taylor, B. Derudder, M. Hoyler & F. Witlox (Eds.), International Handbook of Globalization and World Cities. Cheltenham, U.K.: Edward Elgar.*

Braverman, B., Braverman , J., Taylor, J., Todosow, H., & Wimmersperg , U. (2014-2015). The Vision of A Smart City. En C. Communication and Policy Engagement (CPE) Team, *Reconceptualising Smart Cities: A Reference*

*Framework for India Compendium of Resources - Parte 1 Smart City Definitions* (pág. 62). India: STEP Center for Study of Science, Technology & Policy. doi:http://www.osti.gov/scitech/servlets/purl/773961 del documento - 2009

Carreño Gallardo, J. (2004). Seguridad en Redes Telemáticas. España: McGraw-Hill.

Casa editorial El Tiempo. (6 de 09 de 2015). Las fallas de los bancos al reportar a clientes ante DataCrédito. *El Tiempo* , págs. http://www.eltiempo.com/economia/finanzas-personales/reportes-a-datacredito-y-otras-centrales-de-riesgo/14495887.

Cavoukian, A. (sd de 12 de 2013). *Privacybydesing.ca.* Obtenido de Ph.D. Information and Privacy commissioner Ontario, Canada: https://www.ipc.on.ca/site_documents/pbd-byod.pdf

CCM Benchmark Group. (s.f.). *CCM*. Obtenido de LAN (Rea de Area Local): http://es.ccm.net/contents/253-lan-red-de-area-local

Cio. (4 de 04 de 2012). *http://www.cio.com/*. Obtenido de BYOD: If You Think You're Saving Money, Think Again por Tom Kaneshige: http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html

Cio. (13 de 06 de 2014). *www.cio.com.* Obtenido de What Is Going Wrong With BYOD? por Tom Kaneshige: http://www.cio.com/article/2375498/byod/what-is-going-wrong-with-byod-.html

Cisco. (21 de Junio de 2013). *Cisco IOS and NX-OS EOL Redirect page.* Obtenido de http://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html

Cisco. (2014). *Cisco*. Obtenido de http://www.cisco.com/en/US/products/ps6128/index.html

Cisco. (18 de 10 de 2015). *¿Cómo el RADIUS trabaja?* Obtenido de Cisco Systems Inc.: http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

Cisco Academy Networking. (2012). *CCNA Exploration. Aspectos básicos de networking.* Obtenido de Exploration1.

Cisco Networking Academy. (2009). *CCNA Exoloration 4.0 accediendo a la wan.*

Cisco System, Inc. (2014). *802.1X*. Obtenido de Media-Level Network Access Control: http://www.cisco.com/c/en/us/tech/lan-switching/802-1x/index.html

Cisco Systems, Inc. (2005). *Cisco Trust Agent 2.0.* Obtenido de Cisco Trust Agent is a core component of the Network Admissions Control (NAC) solution: http://www.cisco.com/c/en/us/products/collateral/security/trust-agent/product_data_sheet0900aecd80119868.html

Cisco Systems, Inc. (2005). *Implementing Network Admission Control Phase One Configuration and Deployment.* USA. Obtenido de www.cisco.com

Cisco Systems, Inc. (2005). *Network Admission Control.* Obtenido de Software Configuration Guide: www.cisco.com

Cisco Systems, Inc. (2006). *Cisco Secure Access Control Server Solution Engine.* Obtenido de Ready-to-Deploy Access Policy Control: http://www.cisco.com/c/en/us/products/security/secure-access-control-server-solution-engine/index.html

Cisco Systems, Inc. (2007). *Network Admission Control.* USA: Cisco Press.

Cisco Systems, Inc. (7 de Noviembre de 2013). *Chapter: Posture Validation.* Obtenido de User Guide for Cisco Secure Access Control Server 4.2: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/user/guide/ACS4_2UG/PstrVal.html#wp134759

Cisco Systems, Inc. (2016). *Cisco NAC Appliance (Clean Access)*. Obtenido de http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/index.html

Cisco Systems, Inc. (2009). *Usar Guide for Cisco Secure Access.* USA. Obtenido de http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2-1/User_Guide/acs421ug/SCAdv.html

Cities for Cities, W. C. (Dirección). (2014). *WCCD ISO 37120* [Película]. Obtenido de http://www.dataforcities.org/

Citrix . (7 de 07 de 2015). *Un enfoque realista de la experiencia BYOD.* Obtenido de Alem, Ricardo: http://colombiadigital.net/opinion/columnistas/movilidad-y-tendencias/item/8399-un-enfoque-realista-de-la-experiencia-byod.html

Cole, S. A. (2001). *Suspect Identities: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION.* Cambridge, MA: Harvard University.

Comer, D., & Suominen, E. (2002). *TCP/IP.* IT Press.

Complejo Ruta N. (2012). *Ruta N Medellín Centro de Innovación y Negocios*. Obtenido de EL LUGAR DONDE POTENCIA LA INNOVACIÓN: http://rutanmedellin.org/es/sobre-nosotros

Congdon, P. (2000). *IEEE 802.1X Overview - Port Based Network Access Control,.* Albuquerque, NM,: IEEE Plenary. Obtenido de http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

Congreso de Colombia. (24 de Julio de 2000). *Ley 599.* Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Congreso de Colombia. (5 de Enero de 2009). *Ley 1273*. Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Congreso de Colombia. (27 de Junio de 2013). Decreto 1377 de 2013 por la cual se reglamenta parcialmente Ley No. 1581. *Diario Oficial No. 48834*, pág. 28. doi:http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf

Congreso de la República de Colombia. (31 de Diciembre de 2008). Ley Estatutaria 1266. *Diario Oficial 47.219 de diciembre 31 de 2008*, pág. s.p. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Córdoba Téllez, A., & Durán Martínez, G. (2010). *Diseño de un sistema de control de acceso con Radius configurado en un sistema operativo Linux para una LAN inalámbrica.* México. Obtenido de http://tesis.ipn.mx/bitstream/handle/123456789/6823/ESIME-RADIUS.pdf?sequence=1

Cornella, A. (1999). La infoestructura: Un concepto esencial en la sociedad de la información. (i. p. Scopus, Ed.) *El profesional de la Información - Revista Internaciona Cientifica y Profesional*, 26. Recuperado el 2015, de http://www.elprofesionaldelainformacion.com/contenidos/1999/enero/el_concepto_de_infoestructura.html

Costas Santos, J. (2014). *Seguridad Informática.* España: RA-MA Editorial Retrieve from www.ebrary.com. Obtenido de http://site.ebrary.com.aure.unab.edu.co/lib/unabsp/detail.action?docID=11038505

Creative Commons Attribution Share-Alike 3.0 License. (2016). *Control de acceso criptográfico*. Obtenido de https://galiciacuamatzi.wikispaces.com/4.4+Control+de+acceso+criptogr%C3%A1fico.

Cuppens, F., & Cuppens, N. (2007). Modeling Contextual security policies, (2008), pages(285-305). *International Journal of Information Security*, 285-305.

De Angeli, A. (12 de 03 de 2013). Smart students building their campus: A LARGE-SCALE PARTICIPATORY DESIGN. *Smart Campus Lab*, 55. Obtenido de http://disi.unitn.it/~deangeli/homepage/lib/exe/fetch.php?media=teaching:cscw_smart_campus.pdf

Dey, A. e. (1999). CyberDesk: A Framework for Providing Self-Integrating Context-Aware Services. *Knowledge-Based Systems*, 3-13. Obtenido de http://www.cc.gatech.edu/fce/ctk/pubs/KBS11-1.pdf

Dey, A. K. (2001). Understanding and using context. . *Personal and Ubiquitous Computing*, 4-7.

Dhont, J., Pérez Asinari, M. V., & Poullet, Y. (19 de 04 de 2004). Safe Harbour Decision Implementation Study. *European Commission, Internal Market DG*, 23.

Dourish, P. (2004). What We Talk About When Talk About Context. *Personal and Ubiquitous Computing*, 19-30.

Dziedzic, T., & Levien, R. (s.d. de 11 de 2015). *PacketFence Administration Guide.* Obtenido de http:/www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-5.5.2.pdf

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). *Seguridad informática.* España: Macmillan Iberia, S.A.. Retrieved from http://www.ebrary.com. Obtenido de http://site.ebrary.com.aure.unab.edu.co/lib/unabsp/reader.action?docID=10820963&ppg=45

Esquivel, A., Haya, P., Montoro, G., & Alamán, X. (s.f.). UNA PROPUESTA PARA UN MODELO DE PRIVACIDAD EN ENTORNOS ACTIVOS. Obtenido de http://arantxa.ii.uam.es/~montoro/publications/esquivel05propuesta.pdf

ETSI. (2000). *Broadband Radio Access Network (Bran); HIPERLAN Type 2; SYstem Overview.* Sophia Antipolis Cedex - Francia: Etsi TR 101 683 V1.1.1. Obtenido de https://www.etsi.org/deliver/etsi_tr/101600_101699/101683/01.01.01_60/tr_101683v010101p.pdf

Feitosa, E., Oliveira, L., Lins, B., & Junior, A. M. (2008). Security information architecture for automation and control networks. . *8th Brazilian Symposium of Information Security and Computer Systems*, 17-30.

Frias-Martinez, V., Stolfo, S. J., & Keromytis, A. D. (2008). Behavior-Based Network Access Control: A Proof-of-Concept. En *Information Security* (págs. 175-190). Springer-Verlag Berlin.

Futuresight. (2013). *Resultados Clave de Colombia.* LONDON: GSMA Latinoamérica.

Futuresight, & Theodorou, Y. (2013). *Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios móviles - Resultado clave en Colombia.* New Fetter Lane London: GSMA.

Gartner. (3 de 01 de 2014). *Magic Quadrant for Enterprise Mobility Management Suites.* Obtenido de Analyst(s): Terrence Cosgrove, Rob Smith, Chris Silva, Bryan Taylor, John Girard, Monica Basso: http://www.creekpointe.com/pdfs/Magic-Quadrant-for-Enterprise-Mobility-Management-Suites.pdf

Gartner. (17 de 12 de 2015). *http://www.gartner.com/.* Obtenido de Bring Your Own Device (BYOD): http://www.gartner.com/it-glossary/bring-your-own-device-byod

Gartner Inc. (s.d. de s.m. de 2015). *Gartner Enterprise*. Obtenido de http://www.gartner.com/technology/about.jsp

González, J., & Rossi, A. (2001). New Trends for Smart Cities." Competitiveness and Innovation Framework Programme.

Gorenflo , G., & Moran, J. W. (10 de 04 de 2010). *The Elements of the PDCA Cycle.* Obtenido de

http://www.naccho.org/topics/infrastructure/accreditation/upload/abcs-of-pdca.pdf

GSMA. (28 de 01 de 2012). *Móviles y Privacidad.* Obtenido de http://www.gsma.com/latinamerica/mobile-and-privacy

GSMA. (s.d. de 03 de 2013). *Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios Móviles - Resultados clave de Colombia.* Obtenido de http://www.gsma.com/publicpolicy/wp-content/uploads/2013/04/privacy-attitudes-columbia-spanish.pdf

GSMA Association 2012. (s.d. de 06 de 2012). *Móviles y Privacidad Directrices para el diseño de privacidad en el desarrollo de aplicaciones.* doi:www.gsma.com/mobileprivacy

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER. Obtenido de http://www.dlapiperdataprotection.com/#handbook/world-map-section

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER.

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER. Obtenido de http://www.dlapiperdataprotection.com/#handbook/world-map-section

Haya Coll, P. A. (2006). *Tratamiento de información contextual en entornos inteligentes.* UNIVERSIDAD AUT´ ONOMA DE MADRID. Madrid: Tesis Doctora; Universidad Aautónoma de Madrid.

Headquarters, C. (2005). *Implementing Network Admission Control Phase One Configuration and Deployment.*

Helfrich, D., Frazier, J., Ronnau, L., & Forbes, P. (2006). *Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design.* Pearson Education.

Hernández Sampieri, R. (2010). *Metodología de la Investigación* (5 ed.). (I. Editores, Ed.) México D.F.: McGraw-Hill.

Hervás Lucas, R., & Bravo Rodriguez, J. (2009). MODELADO DE CONTEXTO PARA LA VISUALIZACION DE INFORMACION EN AMBIENTES

INTELIGENTES. *Memoria para Doctorados de Informática*. Toledo, La mancha, España: Universidad de Castilla - La Mancha.

Holvast, J. (1993). *"Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?* North-Holland: in the Proceedings of the IFIP-WG9.2 Conference.

Hull, R., Neaves, P., & Bedford-Roberts, J. (1997). Towards Situated Computing. *1st International Symposium on Wearable Computers; . IEEE Network*, 146-153.

IBM. (18 de 10 de 2012). *La adopción de BYOD ¿es una amenaza para las empresas?* Obtenido de Colombia.com / Tecnología / Noticias / Detalle de noticia: http://www.colombia.com/tecnologia/informatica/sdi/48477/la-adopcion-de-byod-es-una-amenaza-para-las-empresas

ico. (2015). *ico. Information Commisioner's Office*. Obtenido de Auditoria Independiente del Reino Unido -defiende los derechos de información de Interés Públido: https://ico.org.uk/

Icontec. (2007). *Norma Técnica Colombiana NTC-ISO/IEC 27002.*

Information Commisioner's Office-ICO. (2014). *Bring your own device (BYOD).* Obtenido de Data Protection Act 1998: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

Information Security Media Group. (2016). *Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices .* Obtenido de Training: http://www.govinfosecurity.com/webinars/mobile-learn-fromintels-ciso-on-securing-employee-owned-devices-w-264

Intelligent Community Forum (IFC). (21 de 10 de 2015). *The Intelligent Community Forum names the Smart21 Communities of 2016.* Obtenido de http://www.intelligentcommunity.org/index.php?src=news&srctype=detail&category=Awards&refno=1830&prid=1830

International Organization for Standardization - ISO. (2011). *ISO/IEC 27005:2011.* Obtenido de Information technology -- Security techniques -- Information security risk management: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742

International Organization for Standardization - ISO. (2013). *ISO/IEC 27000.* Obtenido de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Organization for Standardization. (1989). *ISO 7498-2:1989.* Obtenido de Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture: http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256

International Organization for Standardization. (2013). *ISO/IEC 27001:2013.* Obtenido de Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/catalogue_detail?csnumber=54534

International Organization for Standardization ISO. (23 de 04 de 2005-2013). *International Organization for Standardization ISO*. Obtenido de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Organization for Standardization-ISO. (1989). *ISO 7498-2:1989.* Recuperado el 19 de Abril de 2016, de Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture: http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256

International Telecommunication Union - ITU. (2012). *Privacy in Cloud Computing.* Geneva,: ITU.

International Telecommunication Union - ITU. (2013). *Privacy and Data Protection:Model Policy Guidelines & Legislative Texts.* Geneva: Telecommunication Development Bureau (BDT).

Inverse Inc. (11 de 2015). *Administration Guide for PacketFence version 5.5.0.* Obtenido de GNUFreeDocumentationLicense,Ver: http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-5.5.1.pdf

ISO. (15 de 06 de 2005). *ISO/IEC 17799 - International Organization for Standardization*. Obtenido de Information technology -- Security techniques -- Code of practice for information security management: http://www.iso.org/iso/catalogue_detail?csnumber=39612

ISO. (15 de 05 de 2014). ISO 37120 briefing note: the first ISO International Standard on city indicators. *Normative references*. doi:http://www.iso.org/iso/37120_briefing_note.pdf

ISO -IEC. (2015). *ISO/IEC JTC 1 Information technology.* Switzerland: www.iso.org. doi:http://www.iso.org/sites/mysmartcity/index.html

IT@Intel White Paper. (11 de 2013). *Enabling BYOD with Application Streaming and Client Virtualization.* Obtenido de enabling-byod-with-application-streaming-and-client-virtualization.pdf

ITU-T – Telecommunication Standardization Bureau (TSB). (s.d. de 09 de 2015). *Security in Telecommunications and Information Technology.* (P. d.–C.-1. Switzerland, Ed.) Recuperado el 08 de 12 de 2015, de http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf

ITU-T. (03 de 2012). *Privacy in Cloud Computing.* Obtenido de ITU-T Technology Watch Report: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

Jackson, N., & Walshe, P. (2011). *Móviles y Privacidad Directrices para el diseño de privacidad en el desarrollo de aplicaciones.* New Fetter Lane - London: GSMA.

Johnson, K., & Filkins, B. L. (Marzo de 2012). *SANS Mobility/BYOD Security Survey.* Obtenido de http://www.sans.org/reading_room/analysts_program/mobilitysec-survey.pdf

Kim, H., Ahn, S., Lim, Y., & Mun, Y. (2005). Access control capable integrated network management system for TCP/IP networks. En M. L. Gavrilova, O. Gervasi, V. Kumar, A. Laganá, H. P. Lee, & Y. Mun (Edits.), *Computational Science and Its Applications–ICCSA 2005* (Vol. 3482, págs. 676-685). Berlin, Alemania: Springer-Verlag Berlin Heidelberg. Obtenido de http://link.springer.com/chapter/10.1007%2F11424826_71#page-1

Know, L. (2015). A vision for the development of i-campus. *Smart Learning Environments a SpringerOpen Journal*, 12. Obtenido de http://www.slejournal.com/content/pdf/s40561-015-0009-8.pdf

Kurose, J. F., Ross, K. W., & Hierro, C. M. (2010). *Redes de computadoras: un enfoque descendente.* Addison Wesley.

Laird, J. (07 de 11 de 2014). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. págs. http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore.

Langheinrich, M. (2001). Privacy by design - Principles of Privacy-Aware Ubiquitous Systems. *Ubiquitous Computing - International Conference* (págs. 273-291). Atlanta, Georgia, USA, September 30 - October 2, 2001.: Editorial Springer-Verlag Berlin Heidelberg.

Langheinrich, M. (2005). *Personal Privacy in Ubiquitous Computing – Tools and System Support.* Switzerland: PhD thesis, ETH Zurich, Zurich. Obtenido de PhD thesis, ETH Zurich,Zurich.

Lassila, O. (2005). Using the Semantic Web in Mobile and Ubiquitous Computing. *Proceedings of the 1st IFIP WG12.5 Working Conference on Industrial Applications of Semantic Web), Springer,* , 19--25.

Lazarte, M. (19 de 11 de 2015). *From Australia to Nigeria - The road to building smart cities.* Obtenido de http://www.iso.org/: http://www.iso.org/iso/news.htm?refid=Ref2027

Lee, O., Yonnim, & Kwon. (2010). An index-based privacy preserving service trigger in context-aware computing environments, (2010),pages5192 - 5200,. *Expert Systems with Applications*, 5192-5200.

Lepouras, G. V. (2007). Domain expert user development: The SmartGov approach. *Communications of the ACM, 50 (9)*, 79-83.

López, P. A. (2010). *Seguridad Informática.* Editex.

Lucent, A. (2011.). "Understanding the Market Opportunity in the Cities of Tomorrow.". *Alcatel Lucent,*.

MACDONALD, N. e. (2010). *The Future of Information Security Is Context Aware and Adaptative.* Stamford: Gartner RAS Core Research Note G00200385.

Madden, Brian. (05 de 2012). *http://www.brianmadden.com/.* Obtenido de What is MDM, MAM, and MIM? (And what's the difference?): http://www.brianmadden.com/blogs/brianmadden/archive/2012/05/29/what-is-mdm-mam-and-mim-and-what-s-the-difference.aspx

Maidan, P. (20-22 de 05 de 2015). Smarter Solutions for a Better Tomorrow. (E. I. Group, Ed.) Obtenido de Exhibitions India Group: https://eu-

smartcities.eu/sites/all/files/events/uploads/Smart%20Cities%20India%202015%20Brochure_0.pdf

Maiwald, E. (2012). *Architectural Alternatives for Enforcing Network Access Control Requirements*. (Garner Inc) Recuperado el 09 de Abril de 2016, de Sitio web de Garner Inc: https://www.gartner.com/doc/1969717/architectural-alternatives-enforcing-network-access

Malek, J. A. (2009). Informative global community development index of informative smart city. *In Proceedings of the 8th WSEAS International Conference on Education and Educational Technology (Genova, Italy, Oct 17-19)*.

Manual de Seguridad en Redes. (s.f.). En *Coordinación de emergencias en redes telemáticas* (pág. 13). Obtenido de Manual de Seguridad en Redes página 13 , Coordinación de emergencia en redes telemáticas

Manzano, V. (2005). *Introducción al análisis del discurso .*

Miller, W. I. (1997). *The Anatomy of Disgust.* Cambridge: Harvard University Press.

Moya, J. M., & Martínez, D. R. (2005). *Seguridad en redes y sistemas informáticos.* Thomson Paraninfo.

Nakhjiri , M., & Nakhjiri, N. (2005). *AAA and Network Security for Mobile Access : Radius, Diameter,EAP,PKI and IP Mobility.*

Nam , T., & Pardo , T. (2011). *Conceptualizing Smart City with Dimensions of Technology, People, and Institutions.* Obtenido de The Proceedings of the 12th Annual International Conference on Digital Government Research: http://inta-aivn.org/images/cc/Urbanism/background%20documents/dgo_2011_smartcity.pdf

NAM, T. P. ( 2011.). Conceptualizing Smart City with Dimensions of Technology , People and Institutions. (University of Maryland, Ed.) *12th Annual International Conference on Digital Government Research,*, 282-291.

NetworkWorld. (24 de 06 de 2013). *http://www.networkworld.com/.* Obtenido de 'La contenerización' no es la panacea BYOD: Gartner - Gartner señala que es una importante cuestión de desarrollo de aplicaciones de TI:

http://www.networkworld.com/article/2167570/byod/-containerization--is-no-byod-panacea--gartner.html

Normas-ISO.com. (25 de 02 de 2015). *NORMAS ISO*. Recuperado el 2015, de http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal

Novenca Security Systems. (2015). *Control de Acceso*. Obtenido de http://www.novenca.com/site/index.php?option=com_content&view=article&id=86&Itemid=164

Ojeda Pérez , J. E. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Obtenido de http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

ONU (United Nations Organization). (10 de 12 de 1948). *Universal declaration of human rights.* Obtenido de Adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948: http://www.un.org/en/sections/what-we-do/protect-human-rights/index.html

Organización Mundial de la Propiedad Intelectual. (23 de Junio de 1989). *Decreto 1360.* Obtenido de http://www.wipo.int/wipolex/es/text.jsp?file_id=126038

*PacketFence.* (11 de 2015). Obtenido de http://www.packetfence.org/about/advanced_features.html

Pandey, Y. (2015). Journey to Smart Campus How the Internet of Everything is Changing Everything. *CSI Symposium held on BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.,* (pág. 34). Bundesverband, Alemania: CISCO.COM. Obtenido de http://www.csi-2015.org/Downloads/CISCO%20Presentation%20at%20CSI%20Symposium%20held%20on%2006.08.2015.pdf

Parekh, S. (03 de 09 de 2014). *IEEE 802.11 Wireless LANs Unit 11.* Obtenido de EECS Instructional and Electronics Support - University of California, Berkeley: http://inst.eecs.berkeley.edu/~ee122/sp07/80211.pdf

Pascoe, J. (1998.). Adding Generic Contextual Capabilities to Wearable Computers. 2nd International Symposium on Wearable Computers,. *2nd International Symposium on Wearable Computers*, 92-99,.

Patiño Sedan, M. (2013). *CITY OF THE YEAR*. Obtenido de Investments and Corporate Banking, Citigroup: https://online.wsj.com/ad/cityoftheyear

Paul, I. (2013). 3 essential techniques to protect your online privacy. *PCWorld Digital*.

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Fundamentos y aplicaciones de seguridad en redes WLAN: de la teoría a la práctica.* Marcombo.

Periódico El Tiempo. (15 de 10 de 2015). Ley de Hábeas Data. *Archivo el Tiempo*, pág. s.p. Obtenido de http://www.eltiempo.com/noticias/ley-de-habeas-data

Pistore, M. (2015). Creating services WITH and FOR people. *Smart Community Lab*, 31. Obtenido de Project Manager – Smart Campus: http://www.science20-conference.eu/wp-content/uploads/2013/08/14_Marco_Pistore_-_Smart_Campus__Services_with_and_for_People.pdf

PMI. (21 de 07 de 2014). *PMI Colombia Capitulo Bogotá.* Obtenido de Empresas de Clase Mundial: http://www.pmicolombia.org/2014/07/empresas-de-clase-mundial/

Preuveneers, D., & Joosen, W. (2015). Change Impact Analysis for Context-Aware Applications in Intelligent Environments. . *Workshop Proceedings of the 11th International Conference on Intelligent Environments. Open Access, IOS Press,* , 70-81.

Radic, L. (1 de 4 de 2015). *Estándares de privacidad para el entorno cloud.* Obtenido de http://www.ccsur.com/estandares-de-privacidad-para-el-entorno-cloud/

RAE. (2014). *DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición.*

Real Academia Española. (2014). *DICCIONARIO DE LA LENGUA ESPAÑOLA*. Obtenido de http://lema.rae.es/drae/

Rege, O. (17 de Agosto de 2011). *Bring Your Own Device: Dealing With Trust and Liability Issues.* Obtenido de http://www.forbes.com/sites/ciocentral/2011/08/17/bring-your-own-device-dealing-with-trust-and-liability-issues/#7cf605625182

Robinson, B. (26 de 07 de 2007). *What you Need to Know About NAC.* Obtenido de IT SECURITY: http://www.itsecurity.com/features/what-you-need-to-know-about-nac-072607/

Rodriguez H., A. A., Espindola, D., J. E., & Rodriguez H., F. (09 de 2015). Implementación de dispositivos móviles personales (BYOD) en la universidad pública. *Memorias II Congreso Internacional de Educación a Distancia; ResearchGate*, 412-420. Obtenido de https://www.researchgate.net/publication/282850481_Implementacin_de_dispositivos_mviles_personales_BYOD_en_la_universidad_pblica

Rosenberg, R. (2004). *The Social Impact of Computers.* San Diego, United States of America: Academic Press.

Round Table Business/Higher Education. (2015). *Internet of Everything -Powering the Smart Campus & the Smart City:Geelong's Transformation to a Smart City.* Deakin Worldly; Cisco; IBM. DC. Victoria Parade: Round Table Business/Higher Education. Obtenido de http://www.bhert.com/events/2015-06-08/BHERT-Smart-City-Agenda-June-18.pdf

Ruiz, C. (31 de 05 de 2013). *Movilidad empresarial y convergencia de dispositivos.* Obtenido de oficina de prensa de Lenovo Colombia: http://www.mintic.gov.co/portal/vivedigital/612/w3-article-4442.html

Sairamesh, J. L. (2004). Information cities. . *Communications of the ACM, 47 (2)*, 28-31.

Salber D, e. a. (1998). Georgia Tech GVU Technical Report GIT-GVU-98-0. 1,. *Georgia Tech GVU Technical Report GIT-GVU-98-0*, 1-15.

Sánchez Acevedo, N., & Segura Castañeda, J. S. (s.f.). *Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática.*

SANS. (2000). *The most trusted source for information security training, certification, and research.* Obtenido de https://www.sans.org/

Scarón de Quintero, M. T., & Genisans, N. (1985). *El diagnóstico social.*

Schaffers, H., Komninos, N., Tsarchopoulos, P., Pallot, M., Trousse, B., Posio, E., . . . Almirall,, E. (18 de 04 de 2012). Landscape and Roadmap of Future Internet and Smart Cities. *HAL archives - ouvertes - Fireball Proyect*, 209. Obtenido de https://hal.inria.fr/hal-00769715/document

Schilit, B., & Theimer , M. (1994). Disseminating Active Map Information to Mobile Hosts. . *IEEE Network, 8(5),* , 22-32.

Schmidt, A. (26 de 07 de 2015). *INTERACTION DESIGN FOUNDATION*. (I. D. Foundation, Editor) Obtenido de https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/context-aware-computing-context-awareness-context-aware-user-interfaces-and-implicit-interaction#chapter_start

*Siliconweek*. (s.f.). Recuperado el Junio de 25 de 2015, de http://www.siliconweek.es/e-enterprise/como-elegir-la-mejor-solucion-de-control-de-acceso-a-la-red-nac-751

Solove, D. J. (2006). A TAXONOMY OF PRIVACY Vol. 154 No.3. *University of Pennsylvania Law Review*, 477-560. Obtenido de https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf

Spandas, L. (2012). *Citrix favours selective BYOD program.* Obtenido de http://www.zdnet.com/article/citrix-favours-selective-byod-program/: http://www.zdnet.com/article/citrix-favours-selective-byod-program/

Stojanovic, D. (2009). *Contex - Aware Mobile and Ubiquitous Computing fir Enhanced Usability: Adaotatuve Technologies and Applications.* New York: Information Science Reference Hershey -IGI GLOBAL - Brithis Library. Obtenido de https://books.google.com.co/books?hl=es&lr=&id=sY6IXsn5xjMC&oi=fnd&pg=PP1&dq=Context+-+Aware+Mobile+and+Ubiquitous+Computing+for+Enhanced+Usability:+Adaptation+Technologies+and+Applications&ots=qB2rAYMeQq&sig=gRdV74xI-EybY0tcX9VnT5-UdG0&redir_esc=y#v=onep

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics 19*, 173-192.

Tacacs. (04 de 2011). *The Advantages of TACACS+ for Administrator Authentication .* Obtenido de www.tacacs.net. : http://www.tacacs.net/docs/TACACS_Advantages.pdf

Tanenbaum, A. S. (2003). *Redes de computadoras* (4 ed.). México: Prentice-Hall.

TechRepublic. (9 de 02 de 2015). *http://www.techrepublic.com/.* Obtenido de 5 Reasons why BYOD survived 2014 and will prosper in 2015, BYOD faced some criticisms in 2014 but appears set to evolve further this year. por Will Kelly: http://www.techrepublic.com/article/5-reasons-why-byod-survived-2014-and-will-prosper-in-2015/

THE COMMISSION EUROPEAN. (27 de 11 de 2013). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN. *on the Functioning of the Safe Harbour from the Perspective of EU Citizens and*. Brussels,, s.p., Bélgica: EUROPEAN EUROPEAN.

The Federal Council - Portal of the Swiss government. (s.d. de s.m. de 2014). *Schweizerische Eidgenossenschaft - Confederation suisse*. Obtenido de The federal Council: http://www.edoeb.admin.ch/org/00129/00132/index.html?lang=en

The Huffington Post. (27 de 12 de 2013). NSA Phone Surveillance Is Legal, New York Judge Rules . *por: Neumeister, Larry (Internet)*. Obtenido de http://www.huffingtonpost.com/2013/12/27/nsa-phone-surveillance_n_4508483.html

Tur, J. N. (2009). *Pensamiento y planificación estratégica. Definición e implementación de estrategias de desarrollo. Gestión y promoción del desarrollo local.*

United Nations. (07 de 2014). *Population world*. Obtenido de www.worldometers.info: http://www.worldometers.info/world-population/india-population/

Universia Colombia. (21 de 05 de 2013). *Para el año 2016 se afianzará el BYOD en las empresas.* Obtenido de Universia.net.co : http://noticias.universia.net.co/en-portada/noticia/2013/05/21/1024756/ano-2016-afianzara-byod-empresas.html

Value, N. (2 de 04 de 2001). ACADEMIA DE REDES LLEGA A COLOMBIA. *El tiempo*. Obtenido de http://www.eltiempo.com/archivo/documento/MAM-567980

Vogt, W. P., & Johnson, R. B. (2011). *Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences: A Nontechnical Guide for the Social Sciences.* Sage.

Volokh, E. (1999). Freedom of Speech and Information Privacy: The Troubling Impli-cations of a Right To Stop People from Speaking About You. *University of California, Los Angeles (UCLA)*, 1049-1051.

W3C NOTE. (21 de 07 de 1998). *P3P Guiding Principles*. Obtenido de NOTE-P3P10-principles-19980721: http://www.w3.org/TR/NOTE-P3P10-principles

W3C Recomentation. (16 de 04 de 2002). *The Platform for Privacy Preferences 1.0* . Obtenido de (P3P1.0) Specification: http://www.w3.org/TR/P3P/

W3C Working Group Note. (13 de 11 de 2006). *The Platform for Privacy Preferences 1.1* . Obtenido de (P3P1.1) Specification: http://www.w3.org/TR/P3P11/

Wan, K. (2009). A Brief History of Context. *International Journal of Computer Science Issues Vol 6, No.2*, 33-42.

Want, R., Schilit, B., & Et al. (Diciembre, 1995.). An Overview of the PARCTab Ubiquitous Computing Experiment. *IEEE Personal Communications,*, 28-43. Obtenido de https://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Papers/Want95_PARCTab.pdf

Ward, R., Hopper, A., Falcao, V., & Gibbons, J. (1992). The active Badge Location System. *ACM Transactions on Information Systems*, 91-102,.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *4 HARV. L. R EV*, 193.

WatchGuard Technologies Inc. (s.d. de s.m. de 2008). *Las 10 principales amenazas a la seguridad de los datos de las PyMEs*. Obtenido de Parte. No. WGCE66599_112408: http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf

Weiser, M. (1993). Some computer science problems in ubiquitous computing. *Communications of the ACM*, 137–143.

Westin, A. F. (3 de 1 de 1968). *Privacy And Freedom.* Obtenido de http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Willis, D. A. (2012). Bring Your Own Device: New Opportunities,. *Gartner, Inc. G00238131*, 1-9.

Wills, D. A. (2013). Bring Yout Own Device: The Facts and the Future. doi:G00250384

World Law Group. (2013). *Global Guide to Data Breach Notifications.* Washington, D.C.: The World Law Group, Ltd.,.

Yovanof, G. S. (2009). An architectural framework and nabling wireless technologies for digital cities & intelligent urban environments. *Wireless Personal Communications, 49(3)*, 445-463.

# ANEXOS

Anexo 1. Revisión y aprobación de la aplicabilidad de la guía metodológica por parte del jefe de Infraestructura de Red de la Universidad Autónoma de Bucaramanga – UNAB. El documento anexo hace parte de la revisión y aprobación dada por el Jefe de infraestructura de red de la UNAB con el fin de validar su aplicabilidad e importancia dentro de la institución.



Noviembre 02 de 2015

**TÍTULO DE LA PROPUESTA: GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE NAC EN LA UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB**

La siguiente propuesta surge como iniciativa del proyecto de grado del programa de Maestría en Telemática de la Universidad Autónoma de Bucaramanga – UNAB, para el departamento de Infraestructura Tecnológica de la UNAB por parte de la estudiante Ing. Alexa María Ramírez Ardila.

**OBJETIVO**

El objetivo de esta propuesta es entregar a Infraestructura Tecnológica de la UNAB una guía metodológica para que pueda realizar la implementación de la arquitectura NAC (Network Admission Control) de Cisco, aprovechando que la infraestructura de red de la Universidad cuenta con este tipo de equipos activos de red y una arquitectura de cómputo robusta para administrar.

**ALCANCE DE LA PROPUESTA**

La presente propuesta se define con el siguiente alcance:

**Fase 1**: Arquitectura de NAC

Esta fase pretende mostrar de forma comprensible la conformación de la arquitectura NAC que ofrece el proveedor Cisco para su implementación, describiendo con detalle

cada elemento que la conforma, su funcionalidad y el flujo de trabajo que se ejecuta al momento de operarlo.

**Fase 2**: Diagnóstico de la Infraestructura de Red de la UNAB

Esta fase corresponde al inventario de equipos activos que hacen parte de la infraestructura de red de la UNAB con el propósito de levantar una linea base y poder establecer un diagnóstico de cumplimiento conforme lo estipula la arquitectura NAC de Cisco.

**Fase 3**: Definición de requerimientos de Hardware y Software

Esta fase corresponde a determinar con base en el inventario optenido en la fase 2 de la infraestructura de red de la UNAB, los equipos y componentes de la arquitectura NAC necesarios para su implementación.

**Fase 4**: Diseño de la arquitectura NAC para la UNAB

Esta fase se encargará de abordar el diseño de la arquitectura NAC de CISCO con base al inventario de equipos activos con los cuales cuenta la infraestructura de red de la UNAB y los requerimientos de Hardware y Software que se puedan determinar para su implementación.

**Fase 5: Casos de prueba**

En esta fase se realizará la comprobación de la propuesta de la guía metodológica para la implementación de NAC mediante la recolección de los casos de prueba de las políticas que la Unab defina para el control de acceso a la red de la Universidad por parte de los usuarios que acceden a la red cableada o inalámbrica.

Esta propuesta es presentada y aprobada por el Ing. José Gregorio Hernández Sánchez, Jefe de Infraestructura Tecnológica de la UNAB a los 2 días del mes de Noviembre de 2015.

En constancia los abajo firmantes.

Ing. **José Gregorio Hernández S.**
Jefe Infraestructura Tecnológica
UNAB

Ing. **Alexa M. Ramírez Ardila**
Estudiante – Maestría Telemática
UNAB

Anexo 2. Levantamiento de Información – F.L.I

La Universidad Autónoma de Bucaramanga, cuenta con una diversidad de dispositivos que permiten sus conexiones a internet y a su vez permiten que los diferentes usuarios se conecten a su red interna. Los dispositivos que hacen parte de la Infraestructura de Red son los siguientes: 105 Access Point distribuidos en los campus Jardín, Terrazas, Tejar, Bosque y Hospital del Norte, 36 Switches distribuidos en los campus Jardín y Tejar, 1 Switch capa 3 ubicado en el Campus Jardín y 3 Controladores ubicados en el Campus Jardín

**FORMATO DE LEVANTAMIENTO DE INFORMACIÓN - INFRAESTRUCTURA DE RED**

| | |
|---|---|
| ENTIDAD: | UNIVERSIDAD AUTONOMA DE BUCARAMANGA |
| DEPARTAMENTO: | RED INSTITUCIONAL |
| NOMBRES Y APELLIDOS: | JOSE GREGORIO HERNANDEZ - JEFE INFRAESTRUCTURA DE RED |
| FECHA: | Mayo 02 de 2016 |

| ITEM | SEDE | EDIFICIO/BLOQUE | DPTO | PISO | FABRICANTE | REF. EQUIPO | MODELO | PUERTOS | SERIAL | CANTIDAD |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | JARDIN | BLOQUE N | CPA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 2 | JARDIN | BLOQUE N | AUDITORIO MENOR | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | #¡REF! | | | 1 |
| 3 | JARDIN | BLOQUE N | BLOQUE N | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 4 | JARDIN | BLOQUE N | BLOQUE N | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 5 | JARDIN | BLOQUE N | BLOQUE N | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 6 | JARDIN | BLOQUE D | BLOQUE N | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 3 |
| 7 | JARDIN | BLOQUE D | BLOQUE N | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 3 |
| 8 | JARDIN | BLOQUE D | BLOQUE N | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 3 |
| 9 | JARDIN | UNAB TECNOLÓGICA | UNAB TECNOLÓGICA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 10 | JARDIN | UNAB TECNOLÓGICA | UNAB TECNOLÓGICA | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 11 | JARDIN | BLOQUE A | BLOQUE A | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 2 |
| 12 | JARDIN | BLOQUE A | BLOQUE A | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 13 | JARDIN | BLOQUE ADMINISTRATIVO | DPTO SISTEMAS | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 14 | JARDIN | BLOQUE ADMINISTRATIVO | PASILLO AUDITORIO | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 15 | JARDIN | BLOQUE ADMINISTRATIVO | AUDITORIO MAYOR | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 16 | JARDIN | BLOQUE ADMINISTRATIVO | FAC. FINANCIERA | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 17 | JARDIN | BLOQUE ADMINISTRATIVO | FAC. MERCADEO | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1142N-A-K9 | | | 2 |
| 18 | JARDIN | BLOQUE ADMINISTRATIVO | FAC. ADMINISTRACIÓN | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 5 |
| 19 | JARDIN | BLOQUE ADMINISTRATIVO | SALA DE PROFESORES | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 20 | JARDIN | BLOQUE ADMINISTRATIVO | FAC. DERECHO | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 21 | JARDIN | BLOQUE ADMINISTRATIVO | FAC. EDUCACIÓN | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 22 | JARDIN | BLOQUE ADMINISTRATIVO | GESTIÓN HUMANA | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 23 | JARDIN | BLOQUE ADMINISTRATIVO | INVESTIGACIONES | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 24 | JARDIN | BLOQUE ADMINISTRATIVO | FRENTE SALA DE JUNTAS | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 25 | JARDIN | BLOQUE ADMINISTRATIVO | FRENTE OFICINA VICERRECTORÍA | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 26 | JARDIN | BLOQUE ADMINISTRATIVO | OFICINA RECTOR | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 27 | JARDIN | BLOQUE L | AUDITORIO INGENIERIAS | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 28 | JARDIN | BLOQUE L | MULTIMEDIOS | MEZANINE | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 29 | JARDIN | BLOQUE L | FAC. SISTEMAS | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 30 | JARDIN | BLOQUE L | SALA DE PARES | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 31 | JARDIN | BLOQUE L | PLANTA PILOTO | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 32 | JARDIN | BLOQUE L | LABORATORIO DE FÍSICA | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 33 | JARDIN | BLOQUE L | AULA DE INFORMÁTICA SIMULACIÓN | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 34 | JARDIN | BLOQUE L | LABORATORIO DE AUTOMATIZACIÓN | PISO 6 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 35 | JARDIN | BLOQUE L | AULA DE INFORMÁTICA UNIVERSIA | PISO 7 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 36 | JARDIN | HOSTAL | AUDITORIO VENEZUELA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 37 | JARDIN | HOSTAL | FRENTE A LAS ESCALERAS | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 38 | JARDIN | HOSTAL | BAR DEL RESTAURANTE | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 39 | JARDIN | HOSTAL | OFICINAL DEL HOSTAL | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 40 | JARDIN | ZONAS ABIERTAS | MASTIL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 41 | JARDIN | ZONAS ABIERTAS | MASTIL NORTE | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 42 | JARDIN | ZONAS ABIERTAS | MASTIL SUR | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 43 | JARDIN | ZONAS ABIERTAS | MASTIL NORTE | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 44 | JARDIN | ZONAS ABIERTAS | MASTIL SUR | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 45 | JARDIN | BLOQUE G | | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 46 | JARDIN | BLOQUE I | | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 47 | JARDIN | BLOQUE E | | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 48 | JARDIN | BLOQUE F | | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 49 | JARDIN | PISO 1 (COCINA BANU) | COCINA BANU | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 50 | JARDIN | PISO 1 ( RED INSTITUCIONAL) | RED INSTITUCIONAL | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 51 | JARDIN | PISO 2 ( HEMEROTECA) | HEMEROTECA | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 52 | JARDIN | PISO 5 ( BIBLIOTECA) | BIBLIOTECA | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 53 | JARDIN | PISO 5 ( BIBLIOTECA) | BIBLIOTECA | PISO 6 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 54 | TERRAZAS | CSU | CABINA DE TRANSMISSION | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 55 | TERRAZAS | CSU | CAFETERIA | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 56 | TERRAZAS | CSU | CAMPANARIO | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 57 | TERRAZAS | CSU | AULA DE INFORMATICA | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 58 | TERRAZAS | CSU | GIMNASIO | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 59 | TERRAZAS | CSU | INFORMATICA DUAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 60 | TERRAZAS | CSU | INFORMATICA DUAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 61 | TEJAR | CALIDAS | PASILLO PRIMARIA | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 62 | TEJAR | CALIDAS | PASILLO PREESCOLAR | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 63 | TEJAR | CALIDAS | SALA PROFESORES BACHILLERATO | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 64 | JARDIN | CASAS | CASA 13 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 65 | JARDIN | CASAS | CASA17 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 66 | JARDIN | CASAS | CASA19 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 67 | JARDIN | CASAS | CASA26 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 68 | JARDIN | CASAS | CASA 30 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 69 | BOSQUE | POSCAL | SALA DE ESTAR MEDICO | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 70 | BOSQUE | POSCAL | AULA DE CLASES N° 2 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 71 | BOSQUE | POSCAL | PASILLO DE ACCESO | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 72 | BOSQUE | POSCAL | SALA DE JUNTAS DE MEDICOS | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 73 | BOSQUE | POSCAL | AULA DE CLASES N° 1 | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 74 | BOSQUE | POSCAL | OFICINA PRINCIPAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 75 | BOSQUE | BLOQUE A | MORELIA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 76 | BOSQUE | BLOQUE A | AULAS INFORMATICA | PISO | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 77 | BOSQUE | BLOQUE A | FAC. DE PSICOLOGIA | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 78 | BOSQUE | BLOQUE A | HALL DE ACCESO PRINCIPAL | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 79 | BOSQUE | BLOQUE A | PASILLO | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 80 | BOSQUE | BLOQUE A | PASILLO | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 81 | BOSQUE | BLOQUE A | PASILLO | PISO 6 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 82 | BOSQUE | BLOQUE A | PASILLO FRENTE AL ASCENSOR | PISO 6 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 83 | BOSQUE | BLOQUE B | RACK GENETICA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 83 | BOSQUE | BLOQUE B | BARRA DEL PASILLO DEL AUD. MAYOR | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 84 | BOSQUE | BLOQUE B | TERRAZA | PISO 1 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 85 | BOSQUE | BLOQUE B | BIBLIOTECA | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602E-A-K9 | | | 1 |
| 86 | BOSQUE | BLOQUE B | CUARTO DE REDES HACIA AUD. MAYOR | PISO 2 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1242G-A-K9 | | | 1 |
| 87 | BOSQUE | BLOQUE B | | | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 88 | BOSQUE | BLOQUE B | AUDITORIO MENOR | PISO 3 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 89 | BOSQUE | BLOQUE B | PASILLO | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 90 | BOSQUE | BLOQUE B | PASILLO | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 91 | BOSQUE | BLOQUE B | PASILLO | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 92 | BOSQUE | BLOQUE B | BUITRON | PISO 4 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 93 | BOSQUE | BLOQUE B | PASILLO | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1141N-A-K9 | | | 1 |
| 94 | BOSQUE | BLOQUE B | PASILLO | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 95 | BOSQUE | BLOQUE B | PASILLO | PISO 5 | CISCO | ACCESS POINT CISCO AIRONET | AIR-CAP2602I-A-K9 | | | 1 |
| 96 | CENTRO | CONSULTORIO JURIDICO | | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 97 | CENTRO | CONSULTORIO JURIDICO | | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 98 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 99 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1262N-A-K9 | | | 1 |
| 100 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | CISCO | ACCESS POINT CISCO AIRONET | AIR-LAP1131G-A-K9 | | | 1 |
| 101 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 102 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 103 | RESERVA | BIBLIOTECA | RED INSTITUCIONAL | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 104 | HOSPITAL DEL NORTE | HOSPITAL DEL NORTE | | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 105 | HOSPITAL DEL NORTE | HOSPITAL DEL NORTE | | | 3COM | ACCESS POINT 3COM | WIRELESS LAN AP 8250 | | | 1 |
| 106 | BOSQUE | BLOQUE A | Aula de Informática | 1 | 3COM | CATALYST | 3300 | 25 | 6MM64F92FD8 | 1 |
| 107 | BOSQUE | BLOQUE A | Baño de hombres | 1 | CISCO | CATALYST | WS-C2960S-24TD-L | 28 | FOC1636X291 | 1 |
| 108 | BOSQUE | BLOQUE A | Baño de hombres | 1 | CISCO | CATALYST | WS-C2960S-24TD-L | 28 | FOC1635Z0H6 | 1 |
| 109 | BOSQUE | BLOQUE A | Baño de hombres | 1 | CISCO | CATALYST | WS-C2960S-24TD-L | 28 | FOC1531Z150 | 1 |
| 110 | BOSQUE | BLOQUE A | Baño de hombres | 2 | 3COM | CATALYST | 4200 | 28 | LZ1V888887460 | 1 |
| 111 | BOSQUE | BLOQUE A | Baño de hombres | 2 | CISCO | CATALYST | WS-C2960-24TC-L | 26 | FCQ1621249J | 1 |
| 112 | BOSQUE | BLOQUE A | Cuarto técnico - junto a tinto | 3 | CISCO | CATALYST | WS-C2960-48TC-L | 50 | FCQ1535Y2A8 | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 113 | BOSQUE | BLOQUE A | Baño de hombres | 4 | 3COM | CATALYST | 4400 | 24 | 7MV1283WPQ8 | 1 |
| 114 | BOSQUE | BLOQUE A | Baño de hombres | 5 | 3COM | CATALYST | 3300 | 25 | 42M64394R08 | 1 |
| 115 | BOSQUE | BLOQUE A | Cuarto técnico ora. Flor | 6 | 3COM | CATALYST | 3300 | 25 | 7MMVHC91G7B | 1 |
| 116 | BOSQUE | BLOQUE B | Proyecto Chicamocha | 1 | 3COM | CATALYST | 4210 | 28 | | 1 |
| 117 | BOSQUE | BLOQUE B | Parqueadero (Gerencia) | 2 | CISCO | CATALYST | WS-C2960-24TC-L | 28 | FOC1535Y5D6 | 1 |
| 118 | BOSQUE | BLOQUE B | Frente a Biblioteca | 3 | CISCO | CATALYST | WS-C2960-48TC-L | 50 | FCQ1535Y1X3 | 1 |
| 119 | BOSQUE | BLOQUE B | Frente a Biblioteca | 3 | 3COM | CATALYST | 4200 | 28 | LZ1V9CAJ83332 | 1 |
| 120 | BOSQUE | BLOQUE B | Aula de Informática | 5 | CISCO | CATALYST | WS-C2960-48TC-L | 50 | FCQ1535Z0E4 | 1 |
| 121 | BOSQUE | FISICAL | Oficinas Docentes | 4 | CISCO | CATALYST | WS-C2960-48TC-L | 50 | FCQ1535Y1B0 | 1 |
| 122 | CALDAS | ADMINISTRATIVO | Cuarto técnico | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1712W14V | 1 |
| 123 | JARDIN | ADMINISTRATIVO | Auditorio Mayor | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 50 | FOC1702Y4PE | 1 |
| 124 | JARDIN | ADMINISTRATIVO | Departamento de Sistemas | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W3D5 | 1 |
| 125 | JARDIN | ADMINISTRATIVO | Cuarto técnico - Rack 1 | 2 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W3E2 | 1 |
| 126 | JARDIN | ADMINISTRATIVO | Cuarto técnico - Rack 1 | 2 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W32W | 1 |
| 127 | JARDIN | ADMINISTRATIVO | Cuarto técnico - Rack 2 | 2 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1544X2AY | 1 |
| 128 | JARDIN | ADMINISTRATIVO | Rack grande Entrenos | 3 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1711W1PE | 1 |
| 129 | JARDIN | ADMINISTRATIVO | Rack grande Entrenos | 3 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W1DL | 1 |
| 130 | JARDIN | ADMINISTRATIVO | Oficina de Sindicatura | 4 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W0DU | 1 |
| 131 | JARDIN | ADMINISTRATIVO | Oficina de Sindicatura | 4 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W1N2 | 1 |
| 132 | JARDIN | BLOQUE A | Frente a oficina Planta Física | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W1MM | 1 |
| 133 | JARDIN | BLOQUE A | Frente a oficina Planta Física | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1536W1K2 | 1 |
| 134 | JARDIN | BLOQUE A | Frente a oficina Planta Física | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1534W5A4 | 1 |
| 135 | JARDIN | BLOQUE D | Cuarto técnico junto a baños | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1534X3DR | 1 |
| 136 | JARDIN | BLOQUE L | Rack oficinas docentes | 1 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1701W1AM | 1 |
| 137 | JARDIN | BLOQUE L | Aula de Simulación | 5 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1534X3HB | 1 |
| 138 | JARDIN | BLOQUE L | Aula de Simulación | 5 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535W2X1 | 1 |
| 139 | JARDIN | BLOQUE L | Aula de Vivencia | 7 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1534W3EA | 1 |
| 140 | JARDIN | BLOQUE L | Aula de Vivencia | 7 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1535X3KF | 1 |
| 141 | JARDIN | BLOQUE N | Aula N4-1 | 4 | CISCO | CATALYST | WS-C2960S-48TD-L | 52 | FOC1702W4FL | 1 |
| 142 | BIBLIOTECA | BIBLIOTECA | RED INSTITUCIONAL | 1 | CISCO | SW CAPA 3 6500 | WSC6509-E-VSS | | | |
| 143 | BIBLIOTECA | BIBLIOTECA | RED INSTITUCIONAL | 1 | CISCO | WIRELESS LAN CONTROLLER 4400 | AIR-WLC4402-50-K9 V04 | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 143 | BIBLIOTECA | BIBLIOTECA | RED INSTITUCIONAL | 1 | CISCO | WIRELESS LAN CONTROLLER 4400 | AIR-WLC4402-50-K9 V04 | | | |
| 144 | BIBLIOTECA | BIBLIOTECA | RED INSTITUCIONAL | 1 | CISCO | WIRELESS LAN CONTROLLER 4400 | AIR-WLC4402-25-K9 V03 | | | |
| 145 | BIBLIOTECA | BIBLIOTECA | RED INSTITUCIONAL | 1 | CISCO | WIRELESS LAN CONTROLLER 5500 | AIR-CT5508-K9 V02 | | | |

NOTA:

- El usuario autoriza el levantamiento de información en el presente formato. SI X NO
- El usuario declara que suministra toda la información requerida sobre los dispositivos de red a su cargo y que no cuenta con otros dispositivos en lugar diferente.
- El usuario reconoce y acepta el uso que se dará a la información suministrada en el formato. SI X NO

JOSE GREGORIO HERNANDEZ
FIRMA DEL USUARIO

ALEXA RAMIREZ ARDILA
FIRMA DEL INVENTARIADOR

Anexo 3. Carta de aceptación del formato F.L.I.

Bucaramanga, Enero 20 de 2016

**CERTIFICADO DE APROBACIÓN**

Por medio del presente documento la Universidad Autónoma de Bucaramanga – UNAB, por medio de la Jefatura de Infraestructura Tecnológica certifica y aprueba el uso del Formato de levantamiento de Información que será diligenciado para el proyecto de grado que está realizando la Ing. Alexa M. Ramírez Ardila estudiante del programa Maestría en Telemática de la UNAB.

Se firma a los 20 días del mes de Enero de 2016 en Bucaramanga, en constancia a quien pueda interesar.

Cordialmente,

**José Gregorio Fernández S.**
Jefe | Infraestructura Tecnológica | UNAB
Tel. 6573489 | Cel. 3043882255

Anexo 4. Entrevista para definición de políticas de seguridad

| | | |
|---|---|---|
| Entidad: Universidad Autónoma de Bucaramanga | | |
| Dependencia: Infraestructura Tecnológica | | |
| Asunto: Definición de Políticas de Seguridad | | |
| Datos del Entrevistado | Nombre: José Gregorio Hernández S. | Cargo: Jefe Infraestructura & Operaciones |
| Datos del Entrevistador | Nombre: Alexa Ramírez Ardila | Cargo: Estudiante en proyecto de grado Maestría en Telemática |
| Fecha: 26 / 02 /2016 | | |

A continuación se describen las políticas de seguridad sugeridas por el área de Infraestructura Tecnológica de la UNAB, para la implementación de la solución propietaria de Cisco - Network Asset Collector – NAC.

| ***Número*** | ***Descripción de la política*** | ***Justificación de la política descrita*** | ***Acción*** |
|---|---|---|---|
| 1 | Inhabilitación de puertos libres en Switch | Se requiere que los puertos libres por cada Switch estén bloqueados con el propósito de evitar conexión de equipos ajenos a la red de la UNAB | Se bloquearan los puertos libres de los Switches impidiendo que el servidor DHCP haga entrega de una IP al dispositivo que se llegue a conectar a la red y no esté autorizado. |
| 2 | Autenticación de Usuarios | Se requiere autenticación de todos los usuarios que se conectan a la red de la Universidad para poder tener acceso a los diferentes servicios. | Como proceso de pre-admisión se debe validar el usuario contra un servidor de autenticación (LDAP, RADIUS, Active Directory) |
| 3 | Revisar cumplimiento de actualizaciones a nivel de sistemas operativo | Se requiere verificar las actualizaciones de seguridad y service pack del sistema operativo de los equipos que se conecten a la red. | Verificar el cumplimiento de actualizaciones, en el evento de no cumplimiento el dispositivo debe quedar en modo cuarentena o buscar el servidor WSUS y ejecutar la actualización. |

| *Número* | *Descripción de la política* | *Justificación de la política descrita* | *Acción* |
|---|---|---|---|
| 4 | Revisar cumplimiento de actualizaciones a nivel de antivirus | Se requiere verificar que los computadores tengan antivirus y éste se encuentre actualizado en su base de datos. | Verificar el cumplimiento de actualizaciones de la base de datos de antivirus, en el evento de no cumplir el dispositivo debe entrar en modo cuarentena o buscar el servidor de actualizaciones de antivirus. |
| 5 | Acción en Modo epidemia de virus | Se requiere revisar la actualización del motor de búsqueda del antivirus y activar el escaneo automático de los computadores para evitar contagios masivos. | Verificar la actualización del motor de búsqueda del antivirus, ejecutar el escaneo del dispositivo en forma automática y presentar mensaje de informe al usuario. |
| 6 | Acción en Modo contagio | Se requiere aislar los computadores contagiados por virus de la red institucional | Verificar la actualización del motor de busque del antivirus, ejecutar escaneo automático del dispositivo, en el evento de contagio y no tener vacuna disponible el dispositivo debe entrar en cuarentena y presentar informe al usuario. |

Las políticas aquí definidas son formuladas a criterio del área de Infraestructura Tecnológica, las cuales deberán pasar por el proceso de aprobación ante la oficina de Seguridad de la Información de la UNAB.

**JOSE GREGORIO HERNANDEZ S**

Anexo 5. Comparativo infraestructura UNAB vs Requerimientos CNAC

A continuación se muestra un cuadro comparativo entre los requerimientos solicitados para implementar la solución de control de acceso propietaria de Cisco y lo que se encontró en el formato de levantamiento de información aplicado a la Universidad Autónoma de Bucaramanga-UNAB.

**Network Access Device - NAD**

| ***Requerimientos de Router CNAC*** | ***Existencia actual en la organización*** | ***Propuesta para implementación*** |
|---|---|---|
| Cisco 800 series 831, 836, 837, 871, 876, 877 y 878<br>Cisco 2600XM (la serie 2600 no es compatible con NAC)<br>Cisco 3640 y 3660-ENT<br>Cisco 1700 series 1701, 1711, 1721, 1751 y 1760. Los modelos 1710, 1720 y 1750 no son compatibles con NAC)<br>Cisco 1800<br>Cisco 2800<br>Cisco 3700 y 3800<br>Cisco series 7200, 7301 y 7500 | No se cuenta en la actualidad con dispositivos de borde como routers. | Se debe realizar la compra de estos dispositivos para poder realizar la implementación de la solución de control de acceso CNAC. |

| *Requerimientos de Switch* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| • Cisco Catalyst 2940, 2950, 2955, 2960 y 2970. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 3550, 3560 y 3750. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 4500 y 4900. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 6500. Switches que corran Sistema Operativo CatOS versión 8.5.1 o superior.<br>**Requerimientos para conexiones inalámbricas**<br>• Cisco Catalyst 6500 series para LAN inalámbrica corriendo sistema operativo versión 1.4.1 o superior | 11 Cisco Catalyst 2960 de 24 puertos<br>32 Cisco Catalyst 2960 de 48 puertos<br>8 Cisco Catalyst 2960S de 24 puertos<br>8 Cisco Catalyst 2960S de 24 puertos<br>20 Cisco Catalyst 2960S de 48 puertos<br>Cisco IOS Software, (C2960 Software), Version 15.0 SE6<br><br>Switch Capa 3 Cisco 6500 | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

| *Requerimientos Concentrador VPN* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Concentradores Cisco VPN 3000 para plataformas virtuales privadas que corran la versión 4.7 solamente con IPSec | Switch Capa 3 Cisco 6500 concentrador core principal<br><br>Firewall Fortinet 1500D | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

**Cisco Secure Access Control Server - ACS**

| **Requerimientos de Hardware** | ***Existencia actual en la organización*** | ***Propuesta para implementación*** |
|---|---|---|
| • Microprocesador Intel Core 2 Duo 2.4 GHz<br>• 2 MB de caché de nivel 2.<br>• Ranuras SDRAM con 4 GB.<br>• Como mínimo una unidad de disco duro de 250 GB SATA instalado. | Servidores Cisco USC240<br>768 GB en RAM<br>4 Interfaces LAN<br>Capacidad de expansión de almacenamiento<br>Procesador Intel Xeon processor E5-2600 | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de servidores solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de servidores que se requieren. |

| **Requerimientos de Sistema Operativo** | ***Existencia actual en la organización*** | ***Propuesta para implementación*** |
|---|---|---|
| • Windows 2003 Server - Service Pack 3<br>• Windows 2008 Server – Service pack 2 o<br>• Windows 2012 Server<br>• Internet Explorer versión 10 o superior<br>• Google Chrome versión 50.0.2661.102 | S.O VSphere 5.5 de Vmware y sobre ellos se virtualizan los servidores (Linux, Windows y Solaris) que se requieran. | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Sistema Operativo solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el tipo de Sistema Operativo se requieren. |

**Cisco Trust Agent – CTA**

| ***Requerimientos*** | ***Existencia actual en la organización*** | ***Propuesta para implementación*** |
|---|---|---|
| Microprocesador Intel Core 2 Duo 2.4 GHz<br>Conexión a Internet<br>Instaladores de Microsoft (MSI). Versión 2.0 o más recientes<br>20 MB como mínimo. Espacio libre en disco duro<br>256 MB de memoria RAM como mínimo<br>UDP – Puerto 21862<br>Windows 2003 professional o superiores<br>Windows 7 o superiores. Sistema operativo Windows para la versión 2.1 de CTA y 802.1x | Actualmente la Universidad cuenta con computadores de escritorio desde Core i3 en adelante con capacidad de memoria de 2 GB y 500 GB de espacio de almacenamiento y sistemas operativos Windows 7, 8.1 y 10 | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Equipos de cómputo clientes solicitados para implementar CNAC en redes cableadas e inalámbricas. |

Anexo 6. Casos de prueba para verificar las políticas a implementar en la Infraestructura de red de la Universidad Autónoma de Bucaramanga - UNAB

A continuación se describen los casos de prueba para verificar las políticas a implementar:

**Caso de prueba uno. Política Inhabilitación de puertos libres en Switch**

| | |
|---|---|
| **Nombre:** | Inhabilitación de puertos libres en Switch |
| **Autor:** | Dispositivo de acceso a la red - NAD |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Realización previa de un inventario de los puntos de red existentes en la organización y que pueda permitir el acceso a la red de manera cableada. Todo punto libre debe ser inhabilitado para que el cliente a través de computador de escritorio o portátil no se pueda conectar. Para aplicar esta seguridad, el puerto del switch debe estar en modo access, con el puerto así configurado, por defecto, la primera MAC que aprenda será la única que se podrá usar, hasta que se desconecte, entonces la que aprenda después se convertirá en segura. Se puede cambiar para que aprenda más de una como segura. Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. | |
| **Actores:** Cliente (equipo de escritorio, portátil) que se conecte a la red cableada, switch de distribución. | |
| **Precondiciones:** Que el cliente que se vaya a conectar tenga un previo registro de la dirección MAC en las tablas del switch | |
| **Flujo Normal:** Una vez registrada la dirección MAC del equipo cliente, al momento de conectarse el switch valide la dirección y verifique que coincide con la almacenada en la tabla. | |
| **Flujo Alternativo:** Cuando no se cumple o no está registrado no habrá conexión a través de la red cableada. | |
| **Pos condiciones:** Una vez se realiza la conexión y se hace validación por MAC, el agente envía las credenciales de salud al NAD quien posteriormente envía el ACS para finalmente autorizar o denegar el acceso a la red cableada. | |

## Caso de prueba dos. Política Autenticación de usuarios

| | |
|---|---|
| **Nombre:** | Autenticación de usuarios |
| **Autor:** | Servidor de Autenticación – Cisco Secure Access Control - ACS |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. Estas condiciones más conocidas como credenciales de autenticación son por ejemplo que contenga un antivirus actualizado, que el firewall esté correctamente configurado y que cuente con los parches de actualización del sistema operativo. Una vez se han revisado estas condiciones se debe verificar a través de un servidor de autenticación, que el equipo cliente cumpla con los datos de autenticación tales como nombre de usuario y contraseña. | |
| **Actores:** Cliente, Cisco Trust Agente, Cisco Secure ACS bajo servidores de autenticación (RADIUS, TACACS, LDAP o directorio activo). | |
| **Precondiciones:** Inicialmente se debe verificar que el Cisco Trust Agent se encuentre instalado en el cliente, que se hayan configurado el Dispositivo de Acceso a la Red (NAD) y el Cisco Secure ACS dentro de la estructura de red de la Organización. Debe haber conexión entre el CTA y el NAD para que se pueda producir el primer paso de la solución el cual es validar el estado del cliente mediante credenciales solicitadas el CTA. Debe haber conexión entre el CTA y el ACS para intercambio de datos de autenticación como son el usuario y la contraseña. Verifica el ACS con lo que tiene el LDAP o el directorio activo de la UNAB | |
| **Flujo Normal:** Una vez se realiza la conexión y se verifica la información recibida del agente tanto para el NAD como para el ACS, se autoriza parcial o completamente el acceso a la red. El tipo de acceso depende del perfil del usuario que solicita el acceso a la red interna. Si el cliente no recibe ningún tipo de autorización de ingreso, se deniega completamente el acceso. | |
| **Flujo Alternativo:** Cuando el cliente cumple con una parte de las credenciales solicitadas, es enviado a un estado llamado Cuarentena, en el cual pasa por diferentes servidores de remediación para que pueda reiniciar nuevamente su proceso de solicitud de acceso a la red. | |
| **Pos condiciones:** El servidor de reparación debe verificar que se instalen adecuadamente las credenciales implementadas en el Cisco Secure ACS y a su vez verificar que el proveedor de antivirus haya enviado el certificado de actualización. Una vez se cumple este proceso, se inicia nuevamente el proceso de petición del cliente. | |

**Caso de prueba tres. Política Revisar cumplimiento de actualizaciones a nivel de sistema operativo**

| | |
|---|---|
| **Nombre:** | Revisar cumplimiento de actualizaciones a nivel de sistema operativo |
| **Autor:** | Dispositivo de acceso a la red - NAD |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. Debe contar con los parches de actualización del sistema operativo. | |
| **Actores:** Cliente, Cisco Trust Agent, Cisco Secure ACS bajo servidores de autenticación RADIUS o TACACS, servidores de remediación, servidor de actualizaciones de Windows, (WSUS) | |
| **Precondiciones:** Inicialmente se debe verificar que el Cisco Trust Agent se encuentre instalado en el cliente, que se hayan configurado el Dispositivo de Acceso a la Red (NAD) y el Cisco Secure ACS dentro de la estructura de red de la Organización. Debe haber conexión entre el CTA y el NAD y entre el CTA y el ACS. El equipo cliente debe tener los parches y actualizaciones de seguridad del sistema operativo actualizados para poder entregarlos al agente. | |
| **Flujo Normal:** Una vez se realiza la conexión y se verifica la información recibida del agente tanto para el NAD como para el ACS, se autoriza parcial o completamente el acceso a la red. El acceso dependerá del cumplimiento o no de las actualizaciones que tenga el sistema operativo, si esta actualizado se permite el acceso si no se enviara al servidor de remediación. | |
| **Flujo Alternativo:** Cuando el cliente no cumpla con las condiciones de actualización del sistema operativo se enviará a cuarentena y posteriormente a un servidor de reparación conocido como Windows Server Update Services (WSUS) el cual provee actualizaciones de seguridad para los sistemas operativos Microsoft. | |
| **Pos condiciones:** El servidor de reparación debe verificar que se instalen adecuadamente las credenciales implementadas en el Cisco Secure ACS y a su vez verificar las actualizaciones del sistema operativo. Una vez se cumple este proceso, se inicia nuevamente el proceso de petición del cliente. | |

**Caso de prueba cuatro. Política Revisar cumplimiento de actualizaciones a nivel de antivirus.**

| | |
|---|---|
| **Nombre:** | Revisar cumplimiento de actualizaciones a nivel de antivirus |
| **Autor:** | Dispositivo de acceso a la red - NAD |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. Debe contar con los certificados de actualización del antivirus instalado. | |
| **Actores:** Cliente, Cisco Trust Agent, Cisco Secure ACS bajo servidores de autenticación RADIUS o TACACS, servidores de remediación, servidor de actualizaciones del antivirus | |
| **Precondiciones:** Inicialmente se debe verificar que el Cisco Trust Agent se encuentre instalado en el cliente, que se hayan configurado el Dispositivo de Acceso a la Red (NAD) y el Cisco Secure ACS dentro de la estructura de red de la Organización. Debe haber conexión entre el CTA y el NAD y entre el CTA y el ACS. El equipo cliente debe tener las actualizaciones del antivirus para poder entregarlas al agente. | |
| **Flujo Normal:** Una vez se realiza la conexión y se verifica la información recibida del agente tanto para el NAD como para el ACS, se autoriza parcial o completamente el acceso a la red. El acceso dependerá del cumplimiento o no de las actualizaciones que tenga el antivirus, si esta actualizado se permite el acceso, si no se enviara al servidor de remediación. | |
| **Flujo Alternativo:** Cuando el cliente no cumpla con las condiciones de actualización del antivirus se enviará a cuarentena y posteriormente a un servidor de reparación el cual se pondrá en contacto con el proveedor de servicios de antivirus para su remediación | |
| **Pos condiciones:** El servidor de reparación debe verificar que se instalen adecuadamente las credenciales implementadas en el Cisco Secure ACS y a su vez verificar las actualizaciones enviadas por el proveedor de antivirus. Una vez se cumple este proceso, se inicia nuevamente el proceso de petición del cliente. | |

## Caso de prueba cinco. Política Acción en Modo epidemia de virus

| | |
|---|---|
| **Nombre:** | Revisar cumplimiento de actualizaciones a nivel de sistemas operativo |
| **Autor:** | Dispositivo de acceso a la red - NAD |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Se debe inhabilitar el acceso por completo de la máquina a la red previa verificación de la actualización del antivirus, denegar el acceso a equipos nuevos que se conecten a la red hasta que pase la alerta de epidemia. Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. En este caso se verifica que la credencial de autenticación contenga un antivirus actualizado y que se envíen las notificaciones por parte del proveedor de antivirus contratado. | |
| **Actores:** Cliente, Cisco Trust Agent, Cisco Secure ACS bajo servidores de autenticación (RADIUS o TACACS, servidores de remediación, cliente del antivirus instalado y consola gestión de antivirus. | |
| **Precondiciones:** La máquina debe estar con el cliente antivirus activo y actualizado en su base de datos, Debe haber conexión entre el CTA y el NAD para que se pueda producir el primer paso de la solución el cual es validar el estado del cliente mediante credenciales solicitadas el CTA. | |
| **Flujo Normal:** En el caso de epidemia, se deniega el acceso hasta que la consola no reporte que la epidemia se ha reparado. | |
| **Flujo Alternativo:** Cuando el cliente cumple con una parte de las credenciales solicitadas, es enviado a un estado llamado Cuarentena, en el cual pasa por diferentes servidores de remediación para que pueda reiniciar nuevamente su proceso de solicitud de acceso a la red. El equipo entra a cuarentena hasta tanto no pase la alarma de epidemia. | |
| **Pos condiciones:** Una vez pasa la alerta de cuarenta se repita la actualización del antivirus en el cliente. | |

Anexo 7. Guía Metodológica para implementar políticas de seguridad en una infraestructura de red Cisco basada en la solución propietaria Cisco Network Asset Collector (CNAC).

Esta guía está conformada por las siguientes fases:

Fase 1. Comprender la arquitectura NAC. En esta fase se describe a manera general como está conformada la arquitectura NAC.

Fase 2. Levantamiento de la información de la infraestructura de red. En esta fase se muestra el formato que se utilizó para realizar este levantamiento. Con los datos obtenidos, se procedió a realizar el diagnóstico.

Fase 3. Requerimientos de hardware y software necesarios para implementar Cisco Network Asset Collector (CNAC). En esta fase se especifican cuáles son los requerimientos de hardware y software que se deben cumplir para poder implementar la solución de cisco.

Fase 4. Diseño de la arquitectura cisco network asset collector (CNAC) a implementar. Esta fase comprende la topología de red diseñada para implementar NAC.

Fase 5. Descripción de los componentes de la arquitectura Cisco Network Asset Collector. En esta fase se describieron cada uno de los componentes que hacen parte de la arquitectura CNAC.

Fase 6. Comparativo infraestructura de la organización vs requerimientos CNAC. Esta fase comprende el comparativo que se realizó una vez hecho el levantamiento de la información. En esta fase se puede evidenciar que los dispositivos cisco con

los cuales cuenta la UNAB cumplen con las características requeridas para implementar NAC.

Fase 7. Definición de políticas para implementar NAC en el cisco secure ACS. En esta fase mediante un instrumento denominado Entrevista se definieron las políticas a implementar en la UNAB.

Fase 8. Casos de prueba para verificar la política a implementar. Finalmente, en esta fase se realizaron los casos de prueba de cada una de las políticas a implementar mediante una serie de pasos predefinidos.

# GUIA METODOLOGICA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL DE ACCESO SOBRE ARQUITECTURA CISCO

**ALEXA MARIA RAMIREZ ARDILA**

**2016**

**CONTENIDO**

**pág.**

**LISTA DE FIGURAS**

**pág.**

**LISTA DE CUADROS**

## INTRODUCCIÓN

La seguridad es un aspecto primordial en la implementación y administración de red y se ha hecho evidente que con la evolución de las empresas y el acceso mediante dispositivos móviles y no-móviles de los diferentes tipos de usuarios, cambiaron también los requerimientos de seguridad de la misma. La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes, los cuales podrían traer consecuencias graves si se pone en peligro su integridad, como las interrupciones de la red que impiden la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios; el robo de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia; hacer pública la información personal o privada de los usuarios sin su consentimiento; mala orientación y pérdida de recursos personales y comerciales, la pérdida de datos importantes cuyo reemplazo requiere un gran trabajo y finalmente, la denegación del servicio (DoS) que son la forma más promocionada de ataques y también están entre los más difíciles de eliminar. Debido a su fácil implementación y al daño potencialmente significativo, los ataques de DoS merecen especial atención de los administradores de seguridad, los cuales pueden ser mitigados utilizando listas de control de acceso en la definición de políticas de seguridad.

Existen dos tipos de problemas de seguridad que deben tener en cuenta los administradores de una red: la seguridad de su infraestructura de red y la seguridad de la información.

La seguridad de una infraestructura de red, incluye el aseguramiento físico de los dispositivos que proporcionan conectividad de red tales como, Switches y Routers y a su vez la implementación de políticas de seguridad para prevenir el acceso no autorizado al software de administración que reside en ellos. La seguridad de la información se refiere a, proteger la información que contienen los paquetes que se transmiten por la red y la

información almacenada en los dispositivos conectados a la red, aplicando barreras y procedimientos que resguarden los datos y solo se permita acceder a ellos a las personas que cumplan con los requisitos establecidos en dichas políticas.

Al analizar esta vulnerabilidad, es necesario implementar medidas y técnicas de seguridad en redes para proteger la información y recursos, éstas deben ser proporcionales a lo que se intenta proteger como son: servidores Web, servidores de correo, protocolos de transferencia de archivos (FTP), bases de datos o cualquier tipo de red, en donde también, se pretende crear manuales los cuales están encaminados al uso adecuado de estas nuevas tecnologías, con recomendaciones para obtener las mejores ventajas y no realizar un mal uso de las nuevas tecnologías que se dispone.

Estas nuevas tecnologías permiten asegurar de manera lógica la información de una organización, la cual se almacena en dispositivos de la red y es movida a través de su infraestructura. Una de estas tecnologías es el control de acceso a la red; según Frias-Martínez, Stolfo y Keromytis[1], tiene como objetivo, asegurar que todos los dispositivos que se conectan a las redes corporativas cumplan con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, entre otros problemas, mediante la implementación de una fase previa a la conexión a la red, en donde el estado del dispositivo final se comprueba por medio de la configuración de un conjunto de políticas establecidas antes de ser concedido el acceso a la red y una fase posterior a la conexión que examina si el dispositivo cumple con las políticas que corresponden a su papel dentro de la red.

Finalmente, la necesidad de implementar tecnologías de control de acceso para poder autenticar dispositivos y usuarios que requieren conectarse a redes corporativas, ha

[1] Frias-Martinez, V., Stolfo, S. J., & Keromytis, A. D. (2008). Behavior-Based Network Access Control: A Proof-of-Concept. En Information Security (págs. 175-190). Springer-Verlag Berlin.

impulsado a diferentes organizaciones privadas y públicas como Cisco, Microsoft, Juniper, entre otras, a ofrecer soluciones para estas necesidades. Una de estas soluciones se propone a continuación en el diseño de una guía metodológica desarrollada con base en una necesidad presentada por la organización de estudio. Las fases para su construcción se detallan a continuación:

Fase 1. Comprender la arquitectura NAC. En esta fase se describe a manera general como está conformada la arquitectura NAC.

Fase 2. Levantamiento de la información de la infraestructura de red. En esta fase se muestra el formato que se utilizó para realizar este levantamiento. Con los datos obtenidos, se procedió a realizar el diagnóstico.

Fase 3. Requerimientos de hardware y software necesarios para implementar Cisco Network Asset Collector (CNAC). En esta fase se especifican cuáles son los requerimientos de hardware y software que se deben cumplir para poder implementar la solución de cisco.

Fase 4. Diseño de la arquitectura cisco network asset collector (CNAC) a implementar. Esta fase comprende la topología de red diseñada para implementar NAC.

Fase 5. Descripción de los componentes de la arquitectura Cisco Network Asset Collector. En esta fase se describieron cada uno de los componentes que hacen parte de la arquitectura CNAC.

Fase 6. Comparativo infraestructura de la organización vs requerimientos CNAC. Esta fase comprende el comparativo que se realizó una vez hecho el levantamiento de la información. En esta fase se puede evidenciar que los dispositivos cisco con los cuales cuenta la UNAB cumplen con las características requeridas para implementar NAC.

Fase 7. Definición de políticas para implementar NAC en el cisco secure ACS. En esta fase mediante un instrumento denominado Entrevista se definieron las políticas a implementar en la UNAB.

Fase 8. Casos de prueba para verificar la política a implementar. Finalmente, en esta fase se realizaron los casos de prueba de cada una de las políticas a implementar mediante una serie de pasos predefinidos.Esta guía puede variar dependiendo del diagnóstico realizado en las Organizaciones.

## GUIA METODOLOGICA PARA LA IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL DE ACCESO SOBRE ARQUITECTURAS CISCO

### FASE 1. COMPRENDER LA ARQUITECTURA DE NAC

### 1.1 CÓMO TRABAJA NETWORK ADMISSION CONTROL DE CISCO

La implementación de NAC combina un número de protocolos y productos existentes de referencia Cisco con algunos nuevos productos y características entre las que se encuentran:

- *Cisco Trust Agen*t - (CTA) *y plugins*
- *Cisco IOS Network Access Device (NAD)*
- *Extensible Authentication Protocol (EAP)*
- *Cisco Secure Access Control Server (ACS)/Remote Authentication Dial-In User Service (RADIUS)*
- *Posture validation/remediation server*

El cuadro 1 muestra la funcionalidad de los tres componentes principales que hacen parte de la solución de control de acceso de Cisco.

Cuadro 13. Funcionalidades de los componentes de CNAC

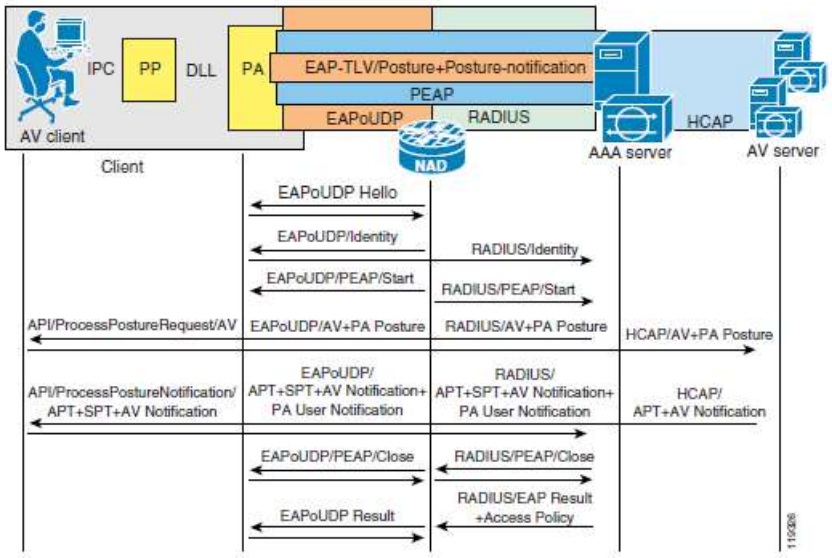
| ***Componente*** | ***Funcionalidad*** |
|---|---|
| *Cisco Trust Agent - CTA* | Se comunica con otro software en el computador del cliente a través de la interfaz de programación de aplicaciones (*API*) y responde las preguntas del servidor de postura (*NAD*). Implementa la comunicación EAP sobre UDP la cual es necesaria para implementar NAC. El software residente incluye un *plugin de* |

| Componente | Funcionalidad |
|---|---|
| | *postura* (*PP*) que se conecta con el CTA. El PP es un agente que informa sobre el estado y las políticas de este dispositivo. |
| *Cisco IOS Network Access Device - NAD* | Es un software instalado en un dispositivo de capa 3 de cisco que revisa los dispositivos que se van a conectar a la red mediante autenticación a través de UDP. |
| *Cisco Secure Access Control Server - ACS* | Cuando Cisco Secure ACS recibe las credenciales provenientes del CTA, revisa en una base de datos de usuario externa para NAC configurado en el ACS con la mejor coincidencia en igualdad de credenciales como las que se recibieron del CTA. |

Fuente: Autor

En la Figura 14 se pueden identificar los diferentes protocolos que hacen parte de la arquitectura NAC.

Figura 14. Flujo de protocolos Arquitectura NAC




Fuente: Helfrich, D., Frazier, J., Ronnau, L., & Forbes, P. (2006). Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design. Pearson Education.

La base de datos de usuarios externos de NAC tiene una o más políticas configuradas. Cuando el ACS encuentra una coincidencia, revisa sus credenciales y atributos contra las políticas locales o externas almacenadas en la base de datos. Estas políticas especifican los valores de los atributos recibidos en las credenciales los cuales deben cumplir con las políticas configuradas para la admisión a la red.

Cada política devuelve un tóken de aplicación de postura (APT) en una sola credencial de vuelta al cliente, junto con algunas acciones soportadas, que son únicos para cada agente de postura. Las más restrictivas del token de aplicación de postura son las que se utilizan en los tóken de postura del sistema (STP). El STP determina el grupo en el que Cisco Secure ACS coloca al cliente y la postura general de ese cliente. Las actuales reglas de aplicación son configuradas en el grupo de políticas del Cisco Secure ACS. Las reglas de aplicación toman la forma de ACLs descargables, URL redireccionadas y temporizadores ajustados. Estas aplicaciones son enviadas al NAD por el ACS cuando finaliza satisfactoriamente la validación de la sesión.

El NAD periódicamente consulta al host para determinar si la postura del cliente ha cambiado o si es el mismo host que ha pasado por el proceso de validación. El NAD también puede hacer cumplir una redirección URL para hacer que un cliente vaya automáticamente a un servidor attribute-value (AV) para obtener actualizaciones cuando el cliente intenta el acceso a la web. Esta redirección URL es configurable desde el ACS para cada estado de postura[2].

[2] Headquarters, C. (2005). Implementing Network Admission Control Phase One Configuration and Deployment.

## 1.2 RESTRICCIONES DE ACCESO PARA LAS POSTURAS DE LOS CLIENTES

Las categorías en las cuales los clientes pueden quedar clasificados de acuerdo a la revisión efectuada por el NAD son las siguientes:

- Categoría y asignación de emergencia
- Saludable
- Chequeo
- Cuarentena
- Infectado
- Desconocido

**NOTA:** Para conocer sobre cada una de estas categorías, puede consultar el documento de proyecto de grado de la Maestría en Telemática de la Facultad de Ingeniería de la Universidad Autónoma de Bucaramanga – UNAB, titulado, PROPUESTA DE UNA GUIA METODOLOGICA PARA LA IMPLEMENTACION DE POLITICAS DE CONTROL DE ACCESO UTILIZANDO LA PLATAFORMA DE CISCO – CNAC (Cisco Network Admission Control) EN LA UNIVERSIDAD AUTONOMA DE BUCARAMANGA. Autor: ALEXA MARÍA RAMÍREZ ARDILA, apartado CONTROL DE ACCESO A LA RED – CNAC.

## FASE 2. LEVANTAMIENTO DE INFORMACIÓN DE LA INFRAESTRUCTURA DE RED

Para poder realizar la implementación de Políticas de Control de Acceso a la red, se requiere de un levantamiento de información técnica referente a los dispositivos de acceso a la red con los cuales cuenta la Organización; esta información será la base del proceso de implementación ya que a partir de ésta, se podrán conocer las condicionales iniciales con las que se cuenta y los requerimientos adquisitivos que se deben tener para su implementación final. La Figura 15 es el formato diseñado para levantamiento de información relacionada con los dispositivos de acceso a la red existentes.

Figura 15. Formato de levantamiento de información

F.L.I

**FORMATO DE LEVANTAMIENTO DE INFORMACIÓN - INFRAESTRUCTURA DE RED**

ENTIDAD: _____

DEPARTAMENTO: _____

NOMBRES Y APELLIDOS: _____ CARGO: _____

FECHA: _____

| ITEM | SEDE | EDIFICIO/BLOQUE | DPTO | PISO | FABRICANTE | REF. EQUIPO | MODELO | PUERTOS | SERIAL | CANTIDAD | VERSIÓN S.O. (IOS) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

**NOTA:**

- El usuario autoriza el levantamiento de información en el presente formato SI ☐ NO ☐
- El usuario declara que suministra toda la información requerida sobre los dispositivos de red a su cargo y que no cuenta con otros dispositivos en lugar diferente. SI ☐ NO ☐
- El usuario reconoce y acepta el uso que se dará a la información suministrada en el formato. SI ☐ NO ☐

_____ _____

**FIRMA DEL USUARIO** **FIRMA DEL INVENTARIADOR**

## FASE 3. REQUERIMIENTOS DE HARDWARE Y SOFTWARE NECESARIOS PARA IMPLEMENTAR CISCO NETWORK ASSET COLLECTOR (CNAC)

NAC consta de varios componentes de Cisco y de otros fabricantes; requiere de un sistema operativo compatible con el Router que realiza el proceso de admisión entre el cliente y la red interna. De la misma manera, NAC requiere de un Cisco Secure ACS versión 3.3 o posterior como una parte integral del proceso de control de admisión. El Cisco Trust Agent es un componente instalado y proporcionado por Cisco que reside en el cliente y proporciona una interfaz compatible con el software de otros fabricantes[3].

Esta sección proporciona información sobre los componentes del sistema necesarios e incluye los requerimientos de Hardware y Software requeridos para implementar esta solución dentro de la Organización.

### 3.1 REQUERIMIENTOS DE HARDWARE PARA EL CISCO SECURE ACS

En el Cuadro 14 se pueden identificar cuáles son los requerimientos necesarios para la implementación del Cisco Secure Access Control Server - ACS

Cuadro 14. Requerimientos de hardware para el Cisco Secure ACS

| Componente | Requerimientos | Recomendaciones y/o sugerencias |
|---|---|---|
| Servidor Cisco Secure (Access Control Server) | Procesador Pentium III (550 MHz o más) | Si se va a utilizar una base de datos de usuarios en el mismo servidor, se recomienda dejar más espacio en disco. |
| | 6 GB de memoria | |
| | 250 MB libres en disco duro | |
| | Resolución de pantalla de 800 x 600 pixeles | |

Fuente: Autor de la guía

[3] Ibíd.

## 3.2 REQUERIMIENTOS DE HARDWARE PARA EL CISCO TRUST AGENT (CTA)

En el Cuadro 15 se especifican los requerimientos de Hardware que se deben tener en cuenta en el cliente al momento de configurar el Agente

Cuadro 15. Requerimientos de Hardware para el Cisco Trust Agent (CTA)

| Componente | Requerimientos | Recomendaciones y/o sugerencias |
|---|---|---|
| Cisco Security Agent (CSA) – Instalado y configurado en el cliente | Microprocesador Intel Core 2 Duo 2.4 GHz<br>2 MB de caché de nivel 2.<br>Ranuras SDRAM con 4 GB. | Es recomendable que el cliente cuente con CSA instalado, ya que el Cisco Security Agent ofrece protección preventiva contra amenazas desconocidas, así como contra nuevas explotaciones y variantes que intenten aprovecharse de vulnerabilidades publicadas y no publicadas. |
| | 128 MB de memoria como mínimo | |
| | • Como mínimo una unidad de disco duro de 250 GB SATA instalado. 15 MB libres en disco duro. | |

Fuente: Autor de la guía

### 3.3 REQUERIMIENTOS DE HARDWARE PARA NETWORK ACCESS DEVICE (NAD)

En el Cuadro 16 se realiza una descripción de los requisitos que debe cumplir el equipo que actuará como dispositivo de acceso a la red.

Cuadro 16. Requerimientos de Hardware para Network Access Device

| Componente | Modelo del Router | Imagen del IOS | DRAM Requerida | Flash Requerida | Recomendaciones y/o sugerencias |
|---|---|---|---|---|---|
| Cisco IOS Dispositivo de acceso a la red - Network Access Device (NAD) | Cisco 83x Series | c831-k9o3sy6-mz<br>c831-k9o3y6-mz | 48 MB<br>48 MB | 12 MB<br>8 MB | Cada cliente validado con éxito consume una cantidad fija de aproximadamente 6 Kb. Además, cada ACL descargable aplica como una entrada dinámica y utiliza unos 8 KB adicional de memoria. |
| | Cisco 1700 Series | c1700-adventerprisek9-mz<br>c1700-advipservicesk9-mz<br>c1700-advsecurityk9-mz | 128 MB<br>96 MB<br>64 MB | 32 MB<br>32 MB<br>16 MB | |
| | Cisco 1841 Integrated Services | c1841-advsecurityk9-mz.123-8.T5.bin | 128 MB | 32 MB | |
| | Cisco 2600XM IP Communications Voice/Fax NM | c2600-adventerprisek9-mz<br>c2600-advipservicesk9-mz<br>c2600-advsecurityk9-mz | 128 MB<br>128 MB<br>96 MB | 32 MB<br>32MB<br>32 MB | |
| | Cisco 2691 Multiservice Platform | c2691-adventerprisek9-mz<br>c2691-advipservicesk9-mz<br>c2691-advsecurityk9-mz | 128 MB<br>128 MB<br>128 MB | 64 MB<br>64 MB<br>32 MB | |
| | Cisco 2801 Integrated Services | c2801-advsecurityk9-mz.123-8.T5.bin<br>c2801-advipservicesk9-mz.123-8.T5.bin<br>c2801-adventerprisek9-mz.123-8.T5.bin | 128 MB | 64 MB | |

| Componente | Modelo del Router | Imagen del IOS | DRAM Requerida | Flash Requerida | Recomendaciones y/o sugerencias |
|---|---|---|---|---|---|
| | Cisco 2811, 2821, 2851 Integrated Services | c2800nm-advsecurityk9-mz.123-8.T5.bin<br>c2800nm-advipservicesk9-mz.123-8.T5.bin<br>c2800nm-adventerprisek9-mz.123-8.T5.bin | 256 MB | 64 MB | |
| | Cisco 3640 Multiservice Platform | c3640-jk9o3s-mz | 128 MB | 32 MB | |
| | Cisco 3660-ENT Series | c3660-jk9s-mz | 128MB | 64 MB | |
| | Cisco 3725/3745 Multiservice Access | c37x5-adventerprisek9-mz<br>c37x5-advipservicesk9-mz<br>c37x5-advsecurityk9-mz | 128 MB<br>128 MB<br>128 MB | 64 MB<br>64 MB<br>32 MB | |
| | Cisco 3825 Integrated Services | c3825-advsecurityk9-mz.123-11.T2.bin | 256 MB | 64 MB | |
| | Cisco 3845 Integrated Services | c3845-advsecurityk9-mz.123-11.T2.bin | 256 MB | 64 MB | |
| | Cisco 7200 Series | c7200-jk9o3s-mz | 128MB | 48 B | |

Fuente: Autor de la guía

### 3.4 REQUERIMIENTOS DE SOFTWARE PARA EL CISCO SECURE ACCESS CONTROL SERVER

Los Cuadro 17Cuadro 18 muestran los requerimientos en cuanto a software para implementar Cisco Secure ACS y Cisco Trust Agent

Cuadro 17. Requerimientos de software para el Cisco Secure Access Control Server

| Componente | Requerimientos de software |
|---|---|
| *Servidor Cisco Secure Access Control Server (ACS)* | Windows 2003 Server - Service Pack 3<br>Windows 2008 Server – Service pack 2 o<br>Windows 2012 Server<br>Internet Explorer versión 10 o superior<br>Google Chrome versión 50.0.2661.102 o superior |

Fuente: Autor de la guía

### 3.5 REQUERIMIENTOS DE SOFTWARE PARA EL CISCO TRUST AGENT

Cuadro 18. Requerimientos de software para el Cisco Trust Agent

| Componente | Requerimientos de software |
|---|---|
| *Cisco Trust Agent (CTA) en cada cliente* | Microsoft Windows XP<br>Microsoft Windows 7<br>Microsoft Windows 8, 8.1<br>Microsoft Windows 10 |
| *Imagen del Cisco IOS* | Imágenes avanzadas iniciando con la versión 12.3(8)T.<br>Versión del IOS 12.3(8)T5 |

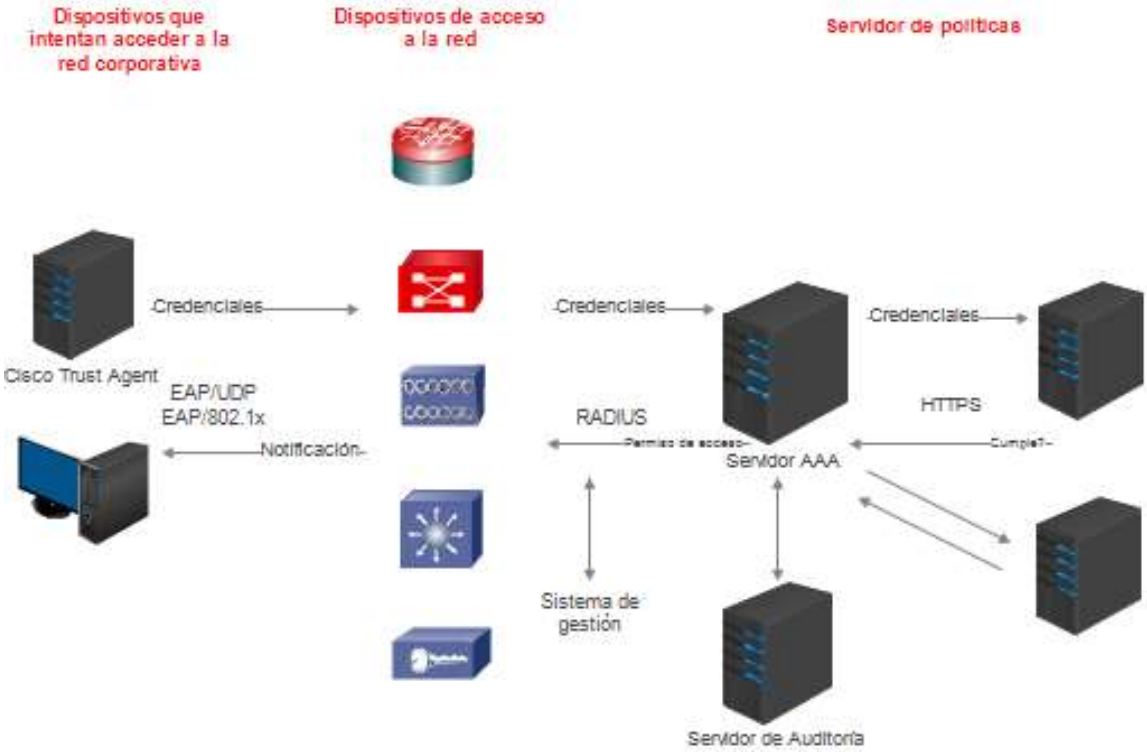
Fuente: Autor de la guía

**Certificación de actualización de antivirus proporcionado por un proveedor de antivirus compatible con NAC**

## FASE 4. DISEÑO DE LA ARQUITECTURA CISCO NETWORK ASSET COLLECTOR (CNAC) A IMPLEMENTAR

El proceso de implementación de la solución Network Access Control (NAC) de Cisco requiere de unos componentes específicos de Hardware y Software los cuales y teniendo en cuenta su aplicabilidad y características se detallan en la Figura 16.

Figura 16. Arquitectura de implementación NAC




Fuente: Autor de la guía

Cada estación de trabajo, al intentar obtener acceso a la red debe enviar una solicitud hacia el equipo por el que logrará la entrada a la red, este puede ser un Switch, un Router, un Access Point o un Concentrador de VPNs, utilizando un protocolo estándar IEEE 802.1x. El dispositivo por el que la estación pide el acceso a la red solicita unas credenciales a la estación, que incluyen todas las políticas necesarias para que la máquina sea considerada

confiable (parches necesarios, últimas actualizaciones de antivirus, etc.), credenciales que son enviadas por el Cisco Trust Agent a un servidor utilizando otro protocolo estándar llamado RADIUS.

Si las credenciales son correctas, y la máquina es considerada confiable, hasta entonces el dispositivo de acceso - NAD (Switch, Router, AP, etc.) le permite el acceso a la red, de lo contrario, se puede decidir denegarle el acceso o reconfigurar la red para enviar dicha estación a una red independiente llamada de cuarentena, para que sea actualizada. Una vez la estación de trabajo ha pasado por cuarenta, debe iniciar nuevamente el proceso de autenticación mediante el envío de credenciales. El control de acceso de esta estación de trabajo será permanente por el Cisco Secure ACS.

## FASE 5. DESCRIPCIÓN DE LOS COMPONENTES DE LA ARQUITECTURA CISCO NETWORK ASSET COLLECTOR (CNAC) Y SU FORMA DE IMPLEMENTACIÓN

La instalación de los componentes de NAC se puede realizar en cualquier orden, ya que la instalación entre ellos no requiere de ningún orden, sin embargo, la configuración del NAD puede bloquearse si el Agente CTA y el Cisco Secure ACS no se han instalado y configurado completamente. A continuación se describen los componentes de NAC, y su forma de implementación:

### 5.1 CISCO SECURE ACCESS CONTROL SERVER[4]

Cisco Secure ACS proporciona servicios de Autenticación, Autorización y Contabilidad a los dispositivos de red que funcionan como clientes AAA, tales como servidores de acceso, Firewall o Router. Centraliza el control de acceso y contabilidad, además de enrutar y administrar el switch de acceso. Con el Cisco Secure ACS, los administradores de red pueden administrar fácilmente las cuentas y hacer cambios en los servicios que ofrece a grupos enteros de usuarios.

Cisco Secure ACS es compatible con clientes Cisco AAA tales como, Cisco 2509, 2511, 3620, 3640, AS5200 y AS5300, AS5800, Firewall PIX Cisco, dispositivos inalámbricos de acceso a la red, Concentradores VPN 3000 y Concentradores VPN 5000. También es compatible con otros dispositivos controladores de acceso tales como el sistema de control de acceso desde terminales (TACASC+) el cual es un protocolo de autenticación remota, propietario de cisco, que se usa para comunicarse con un servidor de autenticación comúnmente usado en redes Unix. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de

[4] Cisco Systems, User Guide for Cisco Secure ACS for Windows Server. Consultado el 10 de Mayo de 2016. [En línea]:http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/user/guide/ACS4_2UG.pdf

autenticación para determinar si el usuario tiene acceso a la red, o el servicio de acceso remoto como el protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP (RADIUS) y utiliza el puerto 1812 UDP para establecer sus conexiones. Cisco Secure ACS trata a todos los dispositivos como clientes AAA.

Las capacidades de rendimiento de Cisco Secure ACS dependen del servidor con sistema operativo Windows en donde esté instalado, la topología y administración de la red, la selección de las bases de datos de usuarios y otros factores. Por ejemplo, Cisco Secure ACS pueden realizar varias autenticaciones por segundo si se usa en un base de datos de usuarios internos y en un computador que tenga procesador más rápido y una interfaz de red disponible para conexiones con servidores que manejen bases de datos de usuarios externos que contengan las mínimas características.

### 5.1.1 Especificaciones de rendimiento del sistema

**Número máximo de usuarios que soporta Cisco Secure ACS.** El límite práctico para la autenticación de usuarios en bases de datos externas e internas en un solo servidor Cisco Secure ACS es de 300.000 a 500.000 usuarios. Este número se incrementa significativamente si la carga de autenticación se extiende a través de varias solicitudes de ACS's.

**Transacciones por segundo.** Las autenticaciones y autorizaciones que realiza el ACS por segundo dependen de diferentes factores, la mayoría de los cuales son externos. Por ejemplo, la red de alta tensión en la comunicación con bases de datos de usuarios externos reduce las transacciones que se puedan realizar.

**Número máximo de clientes AAA.** Cisco Secure ACS puede soportar servicios AAA para aproximadamente 5000 configuraciones de clientes AAA. Esta limitación es principalmente

de la interfaz HTML del ACS. El rendimiento de la interfaz se degrada cuando se tienen más de las configuraciones permitidas.

**5.1.2 Cisco Secure ACS en Windows.** Cisco Secure ACS controla la autenticación, autorización y contabilidad de los usuarios que acceden a la red bajo ambiente Windows. Los servicios ACS de Windows que corren en una máquina con el servidor ACS son los siguientes:

- CSAdmin— Proporciona la interface HTML para la administración del Cisco Secure ACS
- CSAuth—Proporciona autenticación de servicios.
- CSDBSync—Proporciona sincronización de la base de datos de usuarios con una aplicación externa identificada como RDBMS.
- CSLog—Proporciona servicios de usuario tanto para contabilidad como para la actividad del sistema.
- CSMon—Proporciona monitoreo, grabación y notificación al Cisco Secure.
- CSTacacs—Proporciona comunicación entre clientes con servidores AAA como TACACS y el servicio CSAuth.

**5.1.3 Funciones y conceptos del servidor AAA.** Cisco Secure ACS es un servidor AAA que provee servicios de red a dispositivos que pueden actuar como clientes AAA. Como servidor AAA, Cisco Secure ACS incorpora diferentes tecnologías para prestar servicios AAA a clientes AAA.

**5.1.3.1 Cisco Secure ACS y el cliente AAA.** Un cliente AAA es un software que funciona en un dispositivo de red que permite activar los servicios de autenticación, autorización y contabilidad de usuarios que inician sesión con un servidor AAA. Los clientes AAA deben estar configurados para direccionar todos los servicios al Cisco Secure ACS, tales como la autenticación y autorización de los usuarios. Utilizando los protocolos TACACS o RADIUS,

los clientes AAA envían las autenticaciones solicitadas por el ACS. El Cisco Secure ACS verifica los datos de usuario y contraseñas configurados en la base de datos. Cisco Secure devuelve una respuesta al cliente AAA informando si autoriza o deniega el acceso de los usuarios basado en la respuesta recibida del cliente AAA. Cuando las autenticaciones de los usuarios son satisfactorias, el Cisco Secure ACS envía unos atributos de autorización al cliente AAA. El cliente AAA comienza entonces el envío de información contable para el Cisco Secure ACS.

**5.1.3.2 Protocolo AAA — TACACS+ y RADIUS.** Cisco Secure ACS puede usar los protocolos AAA, TACACS+ y RADIUS. En el Cuadro 19 se comparan los dos protocolos.

Cuadro 19. Comparativo de los protocolos TACACS+ y RADIUS

| Punto de comparación | TACACS+ | RADIUS |
|---|---|---|
| Protocolo de transmisión | TCP, orientado a la conexión, protocolo seguro de la capa de transporte, transmisión full-duplex | UDP, no orientado a la conexión, protocolo de la capa de transporte, intercambio de datagramas sin acuse de recibo |
| Puertos usados | 49 | Autenticación y autorización: Puertos 1645 y 1812. Contabilidad: puertos 1646 y 1813 |
| Encriptación | Encripta todos los paquetes | Encripta solo contraseñas de máximo 16 bytes |
| Arquitectura AAA | Realiza control por separado de cada servicio: Autenticación, autorización y contabilidad | Combina la autenticación y autorización en un solo servicio. |
| Gestión de dispositivos | Administración del dispositivo | Control de acceso a los usuarios. |

Fuente: Autor de la guía

**TACACS+.** El protocolo TACACS+ hace parte del Cisco Secure ACS bajo el documento 1.77. Este documento está disponible en la página http://www.cisco.com.

**RADIUS.** El protocolo RADIUS hace parte del Cisco Secure ACS y se encuentra definido en el documento con fecha abril de 1997 y en las siguientes solicitudes de comentarios (RFCs):

RFC 2138, Autenticación de acceso telefónico de manera remota, RFC 2139, Contabilidad de RADIUS, RFC 2865, RFC 2866, RFC 2867, RFC 2868, RFC 2869. Para el soporte entre los antiguos y los nuevos RFCs, Cisco Secure ACS acepta autenticación bajo los puertos 1645 y 1812. Para contabilidad, acepta los paquetes de los puertos 1646 y 1813. Adicional a los atributos de RADIUS, Cisco Secure ACS incluye el soporte para la creación de atributos específicos por vendor (VSA). Los siguientes RADIUS VSA son los predefinidos por el ACS.

- Cisco IOS/PIX
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend
- Juniper
- Microsoft
- Nortel

**5.1.3.3 Autenticación.** Determina la identificación del usuario y verifica su información mediante la autenticación. La autenticación tradicional utiliza un nombre de usuario y una contraseña fija. Las autenticaciones más modernas utilizan autenticación por contraseña de un solo uso (OPTs). Cisco Secure ACS es compatibles con estos métodos de autenticación.

**5.1.3.4 Autorización.** Este servicio determina lo que el usuario está autorizado para hacer. Cisco Secure ACS puede enviar el perfil del usuario con las políticas a un cliente AAA y éste a su vez determina los servicios a los que puede acceder. Las funciones de restricciones de acceso de Cisco le permiten al ACS permitir o denegar inicios de sesión con base en unahora establecida de la semana.

Se puede restringir a los usuarios el servicio o combinación de servicios como el PPP, AppleTalk Remote Access (ARA), Serial Line Internet Protocol (SLIP), o EXEC. Después de seleccionar un servicio, puede restringir protocolo de Capa 2 y Capa 3 como IP e IPX, y se puede aplicar listas de acceso individuales. Las listas de acceso individuales o por grupo restringen a los usuarios para que accedan a servicios tales como el Protocolo de Transferencia de Archivos (FTP) o Protocolo simple de administración de la red (SNMP).

**5.1.3.5 Contabilidad.** El cisco secure ACS escribe registros de contabilidad a un archivo log o en una base de datos ODBC dependiente de su configuración. Estos archivos log se pueden importar fácilmente a una base de datos común y aplicaciones de hojas de cálculo para facturación, auditoría de seguridad y generación de reportes. Los tipos de logs de contabilidad que se puede generar son los siguientes:

- Contabilidad TACACS+
- Contabilidad RADIUS
- Contabilidad administrativa

**5.1.3.6 Administración.** Para configurar, mantener y proteger las funcionalidades AAA, cisco secure ACS proporciona un esquema de administración flexible basado en interfaces HTML. La administración contiene las siguientes características:

- **Asignación de puertos HTTP para sesiones administrativas:** la característica de asignación de puertos HTTP permite configurar el rango de puertos TCP usados por Cisco Secure ACS para sesiones HTTP administrativas. Estrechando este rango con la característica de asignación de puertos HTTP se reduce el riesgo de acceso no autorizados a la red por un puerto abierto para sesiones administrativas. No se recomienda que se administre el cisco secure ACS a través de un firewall. De requerirse se debe configurar el firewall para permitir tráfico HTTP sobre el rango de puertos administrativos que usa cisco

secure ACS para lo cual debe habilitarse el puerto 2002 dado que este es el puerto que se requiere para iniciar una sesión administrativa desde un navegador web.

- **Grupos de dispositivos de red (NDG)**: Dentro de un Cisco Secure ACS pueden crearse dos niveles de dispositivos de red: Dispositivos discretos como un router individual, un servidor de acceso un servidor AAA o un firewall PIX y los NDGs, los cuales permiten administrar una colección de clientes y servidores AAA como un grupo lógico. A estos grupos se les puede asignar un nombre para referirse a todos los dispositivos de grupo. Un dispositivo de red puede pertenecer a un solo NDG al mismo tiempo. Usando NDGs, las organizaciones con un gran número de clientes AAA distribuidos en áreas geográficas amplias pueden organizar este ambiente dentro de Cisco Secures ACS para reflejar una configuración física.

**Otras funciones relacionadas con la administración:**

- Capacidad para definir diferentes privilegios por administrador
- Capacidad para registrar actividades del administrador
- Capacidad para visualizar una lista de usuarios conectados
- Servicio CSMonitor que proporciona monitoreo, notificación, logging, y respuesta de fallo automatizado limitado
- Capacidad para configuración automática de usuarios, grupos, dispositivos de red y Radius VSAs personalizado
- Programación de backup del sistema cisco secure ACS
- Entre otras

**5.1.3.7 Validación de postura.** Cisco secure ACS soporta Network Asset Collector proporcionando servicios de validación de postura a clientes AAA y a los equipos desde donde acceden los clientes conforme a la arquitectura de NAC.

NAC proporciona medios robustos para defender la red, los datos con los que se puede configurar cisco secure ACS para evaluar las solicitudes de validación de postura pueden incluir niveles de parches o actualizaciones de sistemas operativos, versiones actualizadas de antivirus, entre otros.

En lugar de establecer la identidad, la validación de postura determina el estado del cliente NAC utilizando los datos enviados al Cisco Secure ACS por el cliente NAC. Cisco secure ACS usa el resultado de la evaluación de postura para determinar si se concede total o parcialmente el acceso.

**5.1.4 Requisitos de implementación.** El equipo que ejecuta el servidor Cisco Secure ACS debe cumplir con los requisitos mínimos de hardware y software que se describen a continuación en el Cuadro 20 para poder llevar a cabo la implementación del control de acceso a la red.

Cuadro 20. Requisitos de hardware y software para implementación de Cisco Secure ACS

| **Requerimientos de Hardware** | **Requerimientos de Sistema Operativo** | **Requerimientos de software de terceros (Empresas diferentes a Cisco)** |
|---|---|---|
| • Microprocesador Intel Core 2 Duo 2.4 GHz<br>• 2 MB de caché de nivel 2.<br>• Ranuras SDRAM con 4 GB.<br>• Como mínimo una unidad de disco duro de 250 GB SATA instalado. | • Windows 2003 Server - Service Pack 3<br>• Windows 2008 Server – Service pack 2 o<br>• Windows 2012 Server<br>• Internet Explorer versión 10 o superior | • La red debe cumplir con los siguientes requisitos antes de empezar a implementar Cisco Secure ACS.<br>• Se debe ejecutar la versión 15.2 o superior del IOS de Cisco para que pueda soportar los protocolos TACACS y RADIUS.<br>• Los clientes AAA deben ejecutar la versión 15.2 del IOS de Cisco.<br>• Los clientes que no cuentan con sistema operativo de Cisco deben configurarse con TACACS + y / o RADIUS |

| Requerimientos de Hardware | Requerimientos de Sistema Operativo | Requerimientos de software de terceros (Empresas diferentes a Cisco) |
|---|---|---|
| | • Google Chrome versión 50.0.2661.102 | • VPN o clientes inalámbricos deben ser capaces de conectarse con los servicios AAA.<br>• El equipo que ejecuta el servidor Cisco Secure ACS debe poder hacer ping a todos los clientes AAA.<br>• Los dispositivos de puerta de enlace entre Cisco Secure ACS y otros dispositivos de red deben permitir la comunicación a través de los puertos necesarios para admitir las funcionalidades de los protocolos AAA.<br>• Navegador web compatible con Cisco Secure ACS. |

Fuente: Autor de la guía

Cisco Secure ACS utiliza otros puertos UDP y TCP para comunicarse con las bases de datos de usuarios externos. Estos puertos se especifican en el Cuadro 21:

Cuadro 21. Puertos que Cisco Secure ACS escucha

| Protocolo | UDP/TCP | Puertos |
|---|---|---|
| RADIUS. Autenticación y Autorización | UDP | 1645, 1812 |
| RADIUS. Contabilidad | UDP | 1646, 1813 |
| TACACS+ | TCP | 49 |
| Base de datos ACS | TCP | 2000 |
| Sincronización entre los Sistemas de Administración de Base de Datos | TCP | 2000 |
| Usuario de contraseña cambiable con navegador web | TCP | 2000 |
| Acceso a través de Nombre de Usuario | TCP | 2001 |
| Administración de puerto HTTP para nuevas sesiones | TCP | 2002 |
| Rangos de puertos para administración de HTTP | TCP | Configurables por defecto 1024 a 65535 |

Fuente: Autor de la guía

## 5.2 CISCO TRUST AGENT – CTA

Cisco Trust Agent (CTA) es un componente de Cisco Network Admission Control (NAC). NAC permite a los dispositivos de acceso de red permitir o denegar clientes que solicitan acceso a la red de acuerdo a la validación de postura previa en el host[5].

Los cuatro componentes principales del proceso de validación postura del Cisco Trust Agent son los siguientes:

1. **Cliente de red que ejecuta Cisco Trust Agent.** El CTA recopila la información de seguridad denominada como validación de postura de acuerdo a las solicitudes configuradas en la solución NAC e informa al servidor de control de acceso seguro (ACS). Estas son algunas de las validaciones compatibles con NAC:

- Antivirus actualizados
- Firewall configurados
- Versión actualizada de Cisco Security Agent (CSA)

2. **Network Access Device (NAD)**. El Dispositivo de acceso a la red (NAD) permite o deniega el acceso a la red. Frecuentemente el NAD es un Router o Switch Cisco.

3. **Servidor de autenticación.** (Cisco Secure Access Control Server). El servidor de autenticación es el responsable de obtener y evaluar las credenciales de seguridad

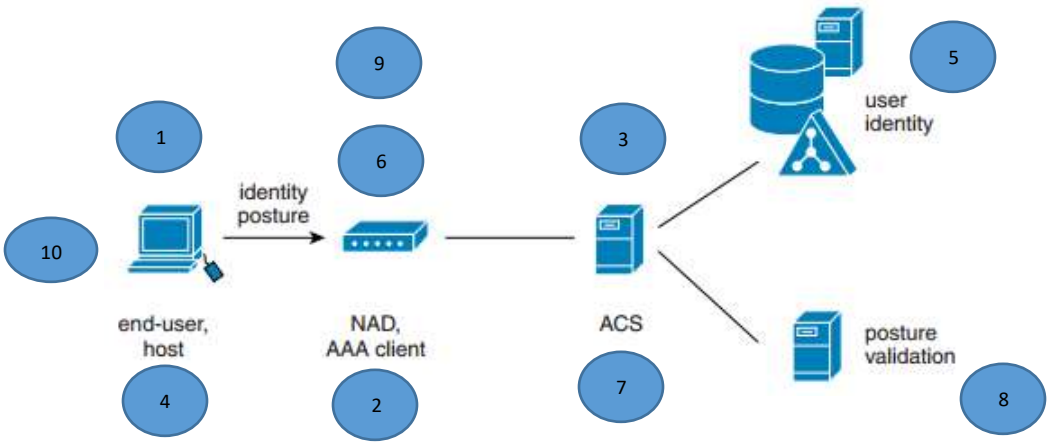
[5] Cisco Systems, Administrator Guide for Cisco Trust Agent. Consultado el 10 de Mayo de 2016. [En línea]: http://www.cisco.com/c/en/us/td/docs/security/cta/admin_guide/cta21ag_unbundled.pdf

entregadas por el cliente cuando intenta conectarse a la red, determinando la postura y validando las políticas definidas por el NAD.

**4. Servidor de validación de postura (opcional).** Son los servidores de validación de postura que soporta Cisco Secure ACS en la postura general del sistema. Estos son frecuentemente aplicaciones de terceros que validan las credenciales especificadas por NAC. Por ejemplo, una compañía de software antivirus puede preferir mantener su propio servidor de validación de postura en lugar de conservar y actualizar la información de validación de postura en el servidor ACS de Cisco.

**5.2.1 Descripción general del proceso de validación de postura.** A continuación se proporciona una visión general de cómo los componentes de validación de postura trabajan juntos durante un proceso inicial de validación postura.

Figura 17. Descripción general del proceso de validación de postura




Fuente: Feitosa, E., Oliveira, L., Lins, B., Junior, A., Melo, R., Sadok, D., & Carmo, U. (2008). Security information architecture for automation and control networks. In 8th Brazilian Symposium of Information Security and Computer Systems, Rio Grande do Sul, SBC, Brasil (pp. 17-30).

1. El computador envía una solicitud DHCP para obtener una dirección IP o una petición ARP (Address Resolution Protocol) para convertir una dirección IP en una dirección física.

2. El dispositivo de acceso de red (NAD), un router o switch Cisco, solicita las políticas de acceso a la red desde el servidor de control de acceso seguro de Cisco (ACS).

3. El ACS solicita las credenciales de postura del equipo cliente en donde fue instalado previamente el Cisco Trust Agent (CTA).

4. CTA recibe la solicitud de credenciales de postura quien a su vez recoge las credenciales de postura de las aplicaciones instaladas en el cliente y compatibles con NAC.

5. El CTA reúne todas las credenciales de postura del cliente y devuelve la información al NAD. Si las credenciales de postura son enviadas utilizando EAP sobre el protocolo UDP, la información de postura es enviada directamente desde el CTA hasta el ACS. Si las credenciales de postura se envían usando el protocolo IEEE 802.1x, el CTA instalado y denominado como CTA 802.1x solicitante envía la información al ACS.

6. El Cisco Secure ACS evalúa las credenciales de seguridad para cada aplicación que reside en el equipo. ACS puede realizar la evaluación de credenciales usando reglas en la base de datos local o puede transmitir credenciales de la aplicación a un servidor de validación de postura. El resultado de la evaluación es un token de validación de postura para cada solicitud evaluada y una notificación opcional de usuario.

7. El Cisco Secure ACS agrega las credenciales de validación de postura y define un token general de postura para el cliente. Las posturas en las cuales se clasifica al cliente son las siguientes**:** Saludable, Chequeo, Cuarentena, Transición, Infectado, Desconocido.

8. El Cisco Secure ACS asigna el token general de postura de acuerdo a una política de acceso.

9. El Cisco Secure ACS envía el resultado de la validación de postura de nuevo al NAD, junto con el token de acceso a la red para ese cliente, y cualquier notificación al usuario.

10. El NAD implementa la política de seguridad para el cliente y envía la información de postura al CTA instalado en el equipo. Dependiendo de cómo se ha configurado el CTA, los resultados de la validación de postura se registran y las notificaciones de usuario se visualizan en la pantalla en un cuadro de diálogo.

### 5.2.2 Requerimientos del sistema para la instalación del Cisco Trust Agent

En el Cuadro 22 se describen los requerimientos de hardware y software para configurar Cisco Trust Agent

Cuadro 22. Requerimientos de Hardware y Software para configurar Cisco Trust Agent

| ***Componente del sistema*** | ***Requerimientos*** |
|---|---|
| Sistema | Microprocesador Intel Core 2 Duo 2.4 GHz<br>Conexión a Internet |
| Instaladores de Microsoft (MSI) | Versión 2.0 o más recientes |
| Espacio libre en disco duro | 20 MB como mínimo |
| Memoria | 256 MB de memoria RAM como mínimo |
| Puertos que escuchan | UDP – Puerto 21862 |
| Sistema operativo Windows para la versión 2.1 de CTA y 802.1x | Windows 2003 professional o superiores<br>Windows 7 o superiores |

Fuente: Autor de la guía

## 5.3 DISPOSITIVO DE ACCESO A LA RED – NAD

El NAD actúa como un punto de aplicación NAC. Estos pueden incluir routers cisco (800 – 7200), puertas de enlace VPN (VPN 3000 series), switches Catalys capa 2 y capa 3, switches y puntos de acceso inalámbrico. Este dispositivo solicita las credenciales de autenticación y envía la información recibida al Cisco Secure ACS quien toma la decisión de control de acceso a la red. De acuerdo a las políticas definidas para acceso del cliente, las decisiones pueden ser: permitir el acceso, negar el acceso o enviar a una zona de cuarentena la cual se encuentra en una subred específica[6].

**5.3.1 Requerimientos de Hardware para Network Admission Control – NAD.** NAC introduce nuevos requisitos de memoria y CPU para las plataformas de acceso de red. Por

[6] Helfrich, D., Frazier, J., Ronnau, L., & Forbes, P. (2006). *Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design*. Pearson Education.

esta razón, algunas plataformas de hardware antiguas no soportan NAC. Los requerimientos de hardware se muestran en el Cuadro 23:

Cuadro 23. Requerimientos de Hardware para Network Admission Control – NAD

| ***Requerimientos de Router*** | ***Requerimientos de Switch*** | ***Requerimientos Concentrador VPN*** |
|---|---|---|
| Cisco 800 series 831, 836, 837, 871, 876, 877 y 878<br>Cisco 2600XM (la serie 2600 no es compatible con NAC)<br>Cisco 3640 y 3660-ENT<br>Cisco 1700 series 1701, 1711, 1721, 1751 y 1760. Los modelos 1710, 1720 y 1750 no son compatibles con NAC)<br>Cisco 1800<br>Cisco 2800<br>Cisco 3700 y 3800<br>Cisco series 7200, 7301 y 7500 | Cisco Catalyst 2940, 2950, 2955, 2960 y 2970. Switches que corran Sistema Operativo release 12.2 o superior.<br>Cisco Catalyst 3550, 3560 y 3750. Switches que corran Sistema Operativo release 12.2 o superior.<br>Cisco Catalyst 4500 y 4900. Switches que corran Sistema Operativo release 12.2 o superior.<br>Cisco Catalyst 6500. Switches que corran Sistema Operativo CatOS versión 8.5.1 o superior. | Concentradores Cisco VPN 3000 para plataformas virtuales privadas que corran la versión 4.7 solamente con IPSec |

Fuente: Autor de la guía

**Requerimientos para conexiones inalámbricas**

- Cisco Aironet 1100, 1130AG, 1200, 1230AG, 1240AG y series 1300 corriendo sistema operativo versión 12.3 o superior
- Cisco Catalyst 6500 series para LAN inalámbrica corriendo sistema operativo versión 1.4.1 o superior
- Dispositivos cliente con soporte para 802.11

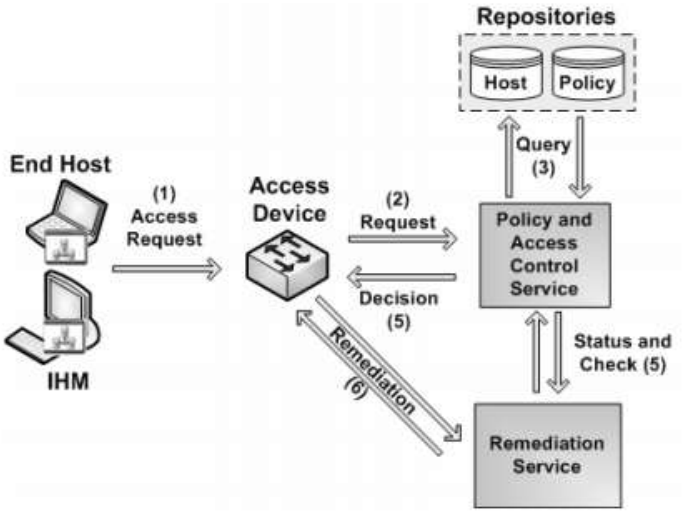
## 5.4 PROCESO DE INTERACCION ENTRE COMPONENTES DE ARQUITECTURA CNAC

El proceso de interacción de los componentes de la arquitectura de NAC debe considerar inicialmente las siguientes características:

Se debe contar con los servicios de un protocolo de autenticación bajo un servidor RADIUS para conectar los dispositivos cliente con los dispositivos de acceso, un protocolo 802.1x para implementar el control de acceso basado en puertos, un protocolo de autenticación extensible (EAP) para proporcionar esquemas de autenticación a través de métodos EAP y en caso de utilizar IPv4, un protocolo IPSec para proporcionar la seguridad en la comunicación.

La interacción de los componentes de NAC se produce de la siguiente manera:

Figura 18. Proceso de control de acceso mediante el Host




Fuente: Feitosa, E., Oliveira, L., Lins, B., Junior, A., Melo, R., Sadok, D., & Carmo, U. (2008). Security information architecture for automation and control networks. In *8th Brazilian Symposium of Information Security and Computer Systems, Rio Grande do Sul, SBC, Brasil* (pp. 17-30).

Para que un host pueda obtener acceso a la red Figura 18. Proceso de control de acceso mediante el HostFigura 18 debe identificarse ante el servidor de control de acceso seguro

(Cisco Secure ACS), a través del dispositivo de acceso a la red (Network Access Device – NAD) donde se conecta (1). Este paso inicial implica el intercambio de mensajes entre los dispositivos Agentes (Cisco Trust Agent – CTA) y el NAD. Por lo tanto, el dispositivo de acceso crea la conexión con el agente en donde realiza la solicitud que contiene los requerimientos de las credenciales de autenticación, estas credenciales son enviadas (2) al servidor de políticas (ACS) para evaluar si el cliente tiene o no acceso a la red y los recursos que puede utilizar. El Servidor de control de acceso seguro analiza toda la información contenida en la solicitud (3) a través de consultas a las bases de datos (clientes y políticas) para validar la autorización de conexión del cliente (4). Una vez verificado, El ACS devuelve al NAD la decisión que se tomó con respecto a la petición de cliente (5). Cuando se permite el acceso, se presentan dos acciones posibles: la primera que permite completamente la entrada del host a la red interna o, la segunda que permite la entrada pero envía el dispositivo a una VLAN aparte en donde se le brindarán los servicios de remediación ya que el dispositivo se encontrará en estado de Cuarentena (6).

Figura 19. Proceso de control de acceso mediante el Usuario

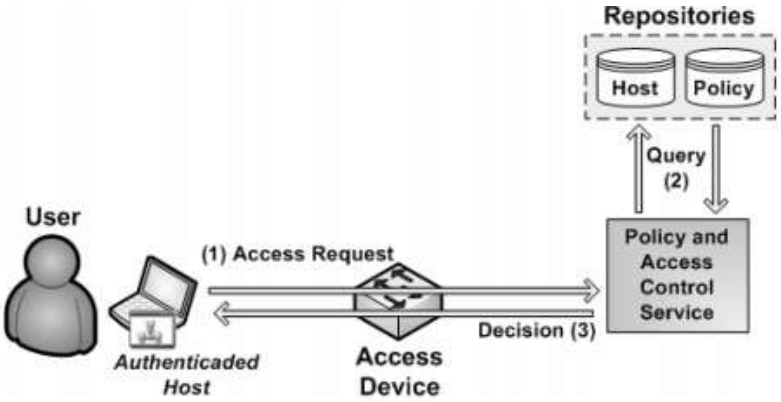



**Figure 3. User Access Control process.**

Fuente: Feitosa, E., Oliveira, L., Lins, B., Junior, A., Melo, R., Sadok, D., & Carmo, U. (2008). Security information architecture for automation and control networks. In *8th Brazilian Symposium of Information Security and Computer Systems, Rio Grande do Sul, SBC, Brasil* (pp. 17-30).

El proceso de autenticación de usuario Figura 19 es más simple pero requiere que el cliente anteriormente haya realizado el proceso de autenticación a través del intercambio de credenciales (antivirus actualizados, parches de los sistemas operativos actualizados, firewall no defectuosos y configuración de firmas digitales). De este modo, a través del agente (CTA), el usuario envía sus identidades (nombre de usuario, contraseña y credenciales) (1) directamente al Servidor ACS. El ACS analiza toda la información contenida en la solicitud (2) a través de consultas en las bases de datos (usuarios y políticas). Después de analizar estas consultas, el ACS devuelve al usuario (Agente) una resolución que contiene la acción que debe ejecutarse (3). [7]

[7] Feitosa, E., Oliveira, L., Lins, B., Junior, A., Melo, R., Sadok, D., & Carmo, U. (2008). Security information architecture for automation and control networks. In *8th Brazilian Symposium of Information Security and Computer Systems, Rio Grande do Sul, SBC, Brasil* (pp. 17-30).

## FASE 6. COMPARATIVO INFRAESTRUCTURA DE LA ORGANIZACIÓN VS REQUERIMIENTOS CNAC

A continuación se muestra un cuadro comparativo entre los requerimientos solicitados para implementar la solución de control de acceso propietaria de Cisco y lo que se encontró en el formato de levantamiento de información aplicado a la organización. La información se organizó de la siguiente manera:

En la primera columna se describen los requerimientos generales de Hardware y Software que se deben tener en cuenta para la implementación de la solución en cualquier organización; en la segunda columna se muestra el resultado que se obtuvo una vez realizado el levantantamiento de la información existente con respecto a equipos activos en la organización; finalmente, en la tercera columna, se realiza el comparativo entre lo que se requiere y lo que se encontró y se describe si éstos dispositivos cumplen o no para dicha implementación y lo que se debe hacer en caso de no contar con estos dispositivos.

### Network Access Device - NAD

| *Requerimientos de Router CNAC* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Cisco 800 series 831, 836, 837, 871, 876, 877 y 878<br>Cisco 2600XM (la serie 2600 no es compatible con NAC)<br>Cisco 3640 y 3660-ENT<br>Cisco 1700 series 1701, 1711, 1721, 1751 y 1760. Los modelos 1710, 1720 y 1750 no son compatibles con NAC)<br>Cisco 1800<br>Cisco 2800<br>Cisco 3700 y 3800<br>Cisco series 7200, 7301 y 7500 | No se cuenta en la actualidad con dispositivos intermediarios como routers. | Se debe realizar la compra de estos dispositivos para poder realizar la implementación de la solución de control de acceso CNAC. Solicitar cotizaciones a Cisco como proveedor de equipos activos de red. |

| *Requerimientos de Switch* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| • Cisco Catalyst 2940, 2950, 2955, 2960 y 2970. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 3550, 3560 y 3750. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 4500 y 4900. Switches que corran Sistema Operativo release 12.2 o superior.<br>• Cisco Catalyst 6500. Switches que corran Sistema Operativo CatOS versión 8.5.1 o superior.<br><br>**Requerimientos para conexiones inalámbricas**<br>• Cisco Catalyst 6500 series para LAN inalámbrica corriendo sistema operativo versión 1.4.1 o superior | 11 Cisco Catalyst 2960 de 24 puertos<br>32 Cisco Catalyst 2960 de 48 puertos<br>8 Cisco Catalyst 2960S de 24 puertos<br>8 Cisco Catalyst 2960S de 24 puertos<br>20 Cisco Catalyst 2960S de 48 puertos<br>Cisco IOS Software, (C2960 Software), Version 15.0 SE6<br>Switch Capa 3 Cisco 6500 | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

| *Requerimientos Concentrador VPN* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Concentradores Cisco VPN 3000 para plataformas virtuales privadas que corran la versión 4.7 solamente con IPSec | Switch Capa 3 Cisco 6500 concentrador core principal | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

**Cisco Secure Access Control Server - ACS**

| Requerimientos de Hardware | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Microprocesador Intel Core 2 Duo 2.4 GHz<br>2 MB de caché de nivel 2.<br>Ranuras SDRAM con 4 GB.<br>Como mínimo una unidad de disco duro de 250 GB SATA instalado. | 768 GB en RAM<br>4 Interfaces LAN<br>Capacidad de expansión de almacenamiento<br>Procesador Intel Xeon processor E5-2600 | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

| Requerimientos de Sistema Operativo | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Windows 2003 Server - Service Pack 3<br>Windows 2008 Server – Service pack 2 o Windows 2012 Server<br>Internet Explorer versión 10 o superior<br>Google Chrome versión 50.0.2661.102 | S.O VSphere 5.5 de Vmware y sobre ellos se virtualizan los servidores (Linux, Windows y Solaris) que se requieran. | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

**Cisco Trust Agent – CTA**

| *Requerimientos* | *Existencia actual en la organización* | *Propuesta para implementación* |
|---|---|---|
| Microprocesador Intel Core 2 Duo 2.4 GHz<br>Conexión a Internet<br>Instaladores de Microsoft (MSI). Versión 2.0 o más recientes<br>20 MB como mínimo. Espacio libre en disco duro<br>256 MB de memoria RAM como mínimo<br>UDP – Puerto 21862<br>Windows 2003 professional o superiores<br>Windows 7 o superiores. Sistema operativo Windows para la versión 2.1 de CTA y 802.1x | 768 GB en RAM<br>4 Interfaces LAN<br>Capacidad de expansión de almacenamiento.<br>Procesador Intel Xeon processor E5-2600<br>S.O VSphere 5.5 de Vmware y sobre ellos se virtualizan los servidores (Linux, Windows y Solaris) que se requieran. | Los dispositivos con los cuales cuenta la organización son compatibles con los requerimientos de Switch solicitados para implementar CNAC en redes cableadas e inalámbricas. De acuerdo a la topología de red a implementar se definirá el número de Switches que se requieren. |

## FASE 7. DEFINICIÓN DE POLÍTICAS PARA IMPLEMENTAR NAC EN EL SERVIDOR CISCO SECURE ACS

A continuación se describen las políticas de seguridad sugeridas por el área de Infraestructura Tecnológica de una organización, para la implementación de la solución propietaria de Cisco - Network Asset Collector – NAC. Estas políticas se deben tener en cuenta al momento de implementación y configuración en cada uno de los dispositivos que hacen parte de la solución de control de acceso.

| *Número* | *Descripción de la política* | *Justificación de la política descrita* | *Acción* |
|---|---|---|---|
| 1 | Inhabilitación de puertos libres en Switch | Se requiere que los puertos libres por cada Switch estén bloqueados con el propósito de evitar conexión de equipos ajenos a la red de la organización | Se bloquearan los puertos libres de los Switches impidiendo que el servidor DHCP haga entrega de una IP al dispositivo que se llegue a conectar a la red y no esté autorizado. |
| 2 | Autenticación de Usuarios | Se requiere autenticación de todos los usuarios que se conectan a la red de la organización para poder tener acceso a los diferentes servicios. | Como proceso de pre-admisión se debe validar el usuario contra un servidor de autenticación (LDAP, RADIUS, Active Directory) |
| 3 | Revisar cumplimiento de actualizaciones a nivel de sistemas operativo | Se requiere verificar las actualizaciones de seguridad y service pack del sistema operativo de los equipos que se conecten a la red. | Verificar el cumplimiento de actualizaciones, en el evento de no cumplimiento el dispositivo debe quedar en modo cuarentena o buscar el servidor WSUS y ejecutar la actualización. |
| 4 | Revisar cumplimiento de actualizaciones a nivel de antivirus | Se requiere verificar que los computadores tengan antivirus y éste se encuentre actualizado en su base de datos. | Verificar el cumplimiento de actualizaciones de la base de datos de antivirus, en el evento de no cumplir el dispositivo debe entrar en modo cuarentena o buscar el servidor de actualizaciones de antivirus. |

| *Número* | *Descripción de la política* | *Justificación de la política descrita* | *Acción* |
|---|---|---|---|
| 5 | Acción en Modo epidemia de virus | Se requiere revisar la actualización del motor de búsqueda del antivirus y activar el escaneo automático de los computadores para evitar contagios masivos. | Verificar la actualización del motor de búsqueda del antivirus, ejecutar el escaneo del dispositivo en forma automática y presentar mensaje de informe al usuario. |
| 6 | Acción en Modo contagio | Se requiere aislar los computadores contagiados por virus de la red institucional | Verificar la actualización del motor de búsqueda del antivirus, ejecutar escaneo automático del dispositivo, en el evento de contagio y no tener vacuna disponible el dispositivo debe entrar en cuarentena y presentar informe al usuario. |

Las políticas aquí definidas son formuladas a criterio del área de Infraestructura Tecnológica, las cuales deberán pasar por el proceso de aprobación ante la oficina de Seguridad de la Información de la organización.

## FASE 8. CASOS DE PRUEBA PARA VERIFICAR LAS POLÍTICAS A IMPLEMENTAR

Según Swebok “Las pruebas de un proyecto consisten en la verificación dinámica del comportamiento de un programa en un conjunto finito de casos de prueba, adecuadamente seleccionado de los posibles escenarios del sistema, para asegurarse que arroja el resultado definido en la especificación, los casos de prueba surgen desde la fase de análisis de requisitos”. Con base en lo anterior, la función del formato descrito a continuación es verificar si la solución propuesta en la guía cumple con las necesidades a solucionar a través de las políticas que se requieren implementar.

Los campos se describen de la siguiente manera:

**Nombre:** Nombre de la política a implementar. En el caso de la organización de estudio, se plantearon 6 políticas.

**Autor:** Dispositivo que permite que la política se cumpla

**Descripción:** Cuál es la situación actual que se presenta y que características se deben tener en cuenta al momento de la implementación de la solución propietaria.

**Actores:** Todos los componentes o dispositivos que hacen posible cumplir con dicha política

**Precondiciones:** Son las características iniciales que se deben considerar o tener en cuenta antes de implementar la política

**Flujo Normal:** Proceso de cumplimiento de la política una vez sean revisadas las precondiciones

**Flujo alternativo:** Solución a implementar en caso de no producirse un flujo normal para dar cumplimiento a la política.

**Poscondiciones:** Procesos a implementar una vez sea verificado el flujo alternativo para finalmente poder implementar la solución propietaria.

A continuación se describe un caso de prueba para verificar una de las políticas a implementar denominada Autenticación de Usuarios:

| | |
|---|---|
| **Nombre:** | Autenticación de usuarios |
| **Autor:** | Servidor de Autenticación – Cisco Secure Access Control - ACS |
| **Fecha:** | Junio 05 de 2016 |
| **Descripción:** Se debe verificar cuáles condiciones presenta el equipo cliente al momento de solicitar la conexión a la red interna. Estas condiciones más conocidas como credenciales de autenticación son por ejemplo que contenga un antivirus actualizado, que el firewall esté correctamente configurado y que cuente con los parches de actualización del sistema operativo. Una vez se han revisado estas condiciones se debe verificar a través de un servidor de autenticación, que el equipo cliente cumpla con los datos de autenticación tales como nombre de usuario y contraseña. | |
| **Actores:** Cliente, Cisco Trust Agent , Cisco Secure ACS bajo servidores de autenticación (RADIUS o TACACS, servidores de remediación y proveedores de antivirus | |
| **Precondiciones:** Inicialmente se debe verificar que el Cisco Trust Agent se encuentre instalado en el cliente, que se hayan configurado el Dispositivo de Acceso a la Red (NAD) y el Cisco Secure ACS dentro de la estructura de red de la Organización. Debe haber conexión entre el CTA y el NAD para que se pueda producir el primer paso de la solución el cual es validar el estado del cliente mediante credenciales solicitadas el CTA. Debe haber conexión entre el CTA y el ACS para intercambio de datos de autenticación como son el usuario y la contraseña. | |
| **Flujo Normal:** Una vez se realiza la conexión y se verifica la información recibida del agente tanto para el NAD como para el ACS, se autoriza parcial o completamente el acceso a la red. El tipo de acceso depende del perfil del usuario que solicita el acceso a la red interna. Si el cliente no recibe ningún tipo de autorización de ingreso, se deniega completamente el acceso. | |
| **Flujo Alternativo:** Cuando el cliente cumple con una parte de las credenciales solicitadas, es enviado a un estado llamado Cuarentena, en el cual pasa por diferentes servidores de remediación para que pueda reiniciar nuevamente su proceso de solicitud de acceso a la red. | |
| **Poscondiciones:** El servidor de reparación debe verificar que se instalen adecuadamente las credenciales implementadas en el Cisco Secure ACS y a su vez verificar que el proveedor de antivirus haya enviado el certificado de actualización. Una vez se cumple este proceso, se inicia nuevament el proceso de petición del cliente. | |

## REFERENCIAS


Cisco Systems, Administrator Guide for Cisco Trust Agent. Consultado el 10 de Mayo de 2016. [En línea]: http://www.cisco.com/c/en/us/td/docs/security/cta/admin_guide/cta21ag_unbundled.pdf

Cisco Systems, User Guide for Cisco Secure ACS for Windows Server. Consultado el 10 de Mayo de 2016. [En línea]:http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/user/guide/ACS4_2UG.pdf

Feitosa, E., Oliveira, L., Lins, B., Junior, A., Melo, R., Sadok, D., & Carmo, U. (2008). Security information architecture for automation and control networks. In 8th Brazilian Symposium of Information Security and Computer Systems, Rio Grande do Sul, SBC, Brasil (pp. 17-30)

Frias-Martinez, V., Stolfo, S. J., & Keromytis, A. D. (2008). Behavior-Based Network Access Control: A Proof-of-Concept. En Information Security (págs. 175-190). Springer-Verlag Berlin.

Helfrich, D., Frazier, J., Ronnau, L., & Forbes, P. (2006). Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design. Pearson Education

Headquarters, C. (2005). Implementing Network Admission Control Phase One Configuration and Deployment



Helfrich, D., Frazier, J., Ronnau, L., & Forbes, P. (2006). Cisco Network Admission Control, Volume I: NAC Framework Architecture and Design. Pearson Education