REVISTA COLOMBIANA DE COMPUTACIÓN
Volumen 18, número 1
Págs. 46 - 60

Guía metodológica para la implementación de políticas de control de acceso utilizando la plataforma de Cisco Network Admission Control (CNAC) en la Universidad Autónoma de Bucaramanga - UNAB

Methodological guide to develop Access control politics by using Cisco´s Network Admission Control platform at Universidad Autónoma de Bucaramanga

Alexa M. Ramírez A.
Universidad Autónoma de Bucaramanga
Correo: aramirez@unab.edu.co

José G. Hernández
Universidad Autónoma de Bucaramanga
Correo: jhernand@unab.edu.co

Fecha de recibido: 17/02/2017 y Fecha de aprobación: 05/04/2017

Resumen

La presente investigación tiene como fin mostrar la importancia que tiene hoy en día la implementación de soluciones de control de acceso en las organizaciones las cuales son usadas con el fin de controlar de manera eficiente el acceso de cada uno de los dispositivos que intentan conectarse a las redes corporativas y de esta manera proteger sus datos y reputación. En este documento se mencionan conceptos de seguridad, control de acceso y control de acceso a redes, haciendo énfasis en la solución propietaria de Cisco la cual lleva por nombre Cisco Network Assett Collector y sobre la cual se diseñó una propuesta de implementación de una guía metodológica para la implementación de políticas de control de acceso en la Universidad Autónoma de Bucaramanga – UNAB. Esta guía está dividida en ocho fases, las cuales permiten conocer y comprender la solución de Cisco, los requerimientos técnicos en cuanto a software y hardware relacionados y finalmente las políticas generales que se deben considerar al momento de implementar CNAC.

Palabras Clave:

Seguridad, Telemática
Políticas de Seguridad
Telecomunicaciones
Diagnóstico
Guías Metodológicas
Control de Acceso a Redes

‡Se concede autorización para copiar gratuitamente parte o todo el material publicado en la *Revista Colombiana de Computación* siempre y cuando las copias no sean usadas para fines comerciales, y que se especifique que la copia se realiza con el conocimiento de la Revista Colombiana de Computación.

Abstract

The investigation below was made to show the importance of developing access control politics in organizations which are used to control the access of every single device that try to get a connection to company's networks and by this way get the solution to protect their data, information and even their reputation. You will find security´s concepts on this document, access control and network´s control focusing on the own solution of cisco network assett collector as an emphasis to develop and design a proposal about a methodological guide to develop access control politics at Universidad Autonoma de Bucaramanga. This guide is divided into eight phases which let you know and understand the solutions for cisco. The technical requirements about software and hardware related and finally the general politics we must consider when setting CNAC.

Keywords:

Security, telematics
Security politics
Telecommunications
Diagnostic
Methodological guides
Network´s access control.

1. Introducción

Esta propuesta de investigación tiene como fin mostrar la importancia que tiene la implementación de políticas de seguridad implementando soluciones de control de acceso ya sea de fabricantes propietarios o soluciones basadas en software libre. Hoy en día las organizaciones requieren cada vez más, que sus datos estén protegidos de ataques que se generen ya sea de manera cableada o inalámbrica. 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, estas 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. 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 Frías-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. 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 Organización? De lo anterior, la hipótesis planteada es, 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 organización 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. Marco teórico-conceptual

2.1 Seguridad, tipos, servicios y análisis de riesgos en la red

2.1.1 Seguridad en la red

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 [1]. 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 [2]. Según la Organización Internacional para la Estandarización (ISO) [3] y con respecto a la Seguridad de Información, en todas sus formas (automatizada o no 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 trazados dentro de la misma

2.1.2 Tipos de seguridad

La seguridad en la red se plantea desde dos enfoques distintos aunque complementarios:

Seguridad Física	Seguridad Lógica
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	Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y que solo se permita acceder a ellos a las personas autorizadas mediante el enmascaramiento 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

Tabla 1. Enfoque de la seguridad en la red.

Con respecto a este tipo de seguridad son varias las técnicas aplicadas entre las que se encuentran; el control de acceso, la autenticación, la encriptación, el *firewall* y el antivirus, entre otros.

2.1.3 Servicios de seguridad

Los principales servicios básicos de seguridad y en los cuales mencionan en sus apartados Nakhjiri y Nakhjiri [4]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. De acuerdo a Carreño Gallardo [5], el servicio de autenticación de datos, son medidas dirigidas a garantizar que la persona o la máquina 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. Carreño Gallardo en su libro Seguridad en redes telemática [5], 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, que 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. A diferencia del servicio de confidencialidad, el servicio de integridad de los datos 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 [5]. 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 solo 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.

El servicio de control de acceso 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 [6], este servicio se implementa bajo la autenticación en la que el usuario demuestra quién dice ser para poder acceder a los privilegios y restricciones correspondientes. En el control de acceso se presentan 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 debe identificarse para acceder de acuerdo a los servicios que requiera, (2) El acceso a terminales desde los 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.

2.1.4 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 [7] 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.

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 [8]. Este fenómeno inició en 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 [9]. Fue solo 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 [10]. Existen muchos aspectos a considerar si la implementación del 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 [11]; 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 competitivas 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 [12].

David A. Willis argumenta en su artículo Bring Your Own Device: The Facts and the Future [13] 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.

2.3 Control de acceso

El control de acceso es el proceso de conceder permisos a usuarios o grupos y poder conocer quiénes están autorizados para acceder a los sistemas de información y recursos. Su concepto se resume en tres pasos que son: identificación, autenticación y autorización. Para el caso de existir comunicación móvil, redes inalámbricas, computadores portátiles, etc. también es necesario implementar políticas que contemplen cada uno de estos aspectos [14]. Se debe establecer, documentar y revisar una política de control de acceso con base en las necesidades de seguridad y de negocio de la organización.

Frías-Martínez, Stolfo y Keromytis [15], 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, teletrabajadores, usuarios invitados, etc. El uso de estos escenarios afectan 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 básicamente 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 y 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. Dentro de las clasificaciones de control de acceso se encuentran las siguientes:

Control de acceso por identificación	Control de acceso por autenticación	Control de acceso criptográfico
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.	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 [16].	Existen mecanismos de control de acceso criptográfico donde se combinan algunas técnicas de la criptografía para desarrollar protocolos, modelos y mecanismos de autenticación para el control de acceso.

Tabla 2. Clasificaciones del control de acceso a la red.

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. 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. Las funcionalidades que una solución NAC debe tener son detección del nodo, autenticación, evaluación de seguridad del dispositivo final, autorización, cumplimento de la política, cuarentena, remediación y control postadmisión

2.4.1 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 [17]. La Figura. 1 muestra los elementos que hacen parte de la solución de control de acceso

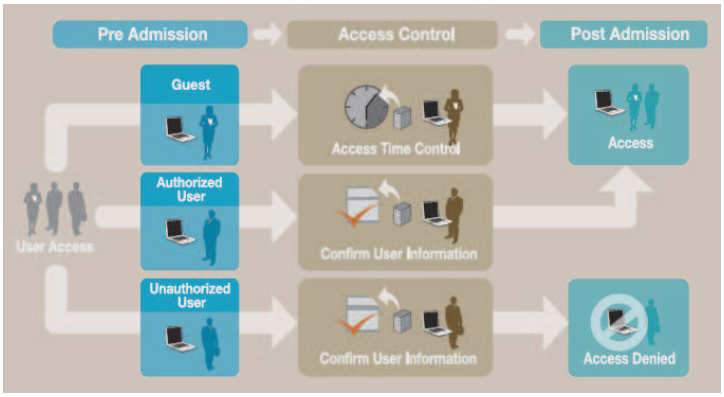

Figura 1. Elementos de NAC.
Fuente: Cisco, «Cisco IOS and NX-OS EOL Redirect page,» 21 Junio 2013. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html.

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.

5.1 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 los dispositivos, compu-

tadores 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 [18]. 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 [19].

La Figura. 2 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. La diferencia entre ambas es que sobre UDP se hace solo validación y en 802.1x se hace validación y autenticación.

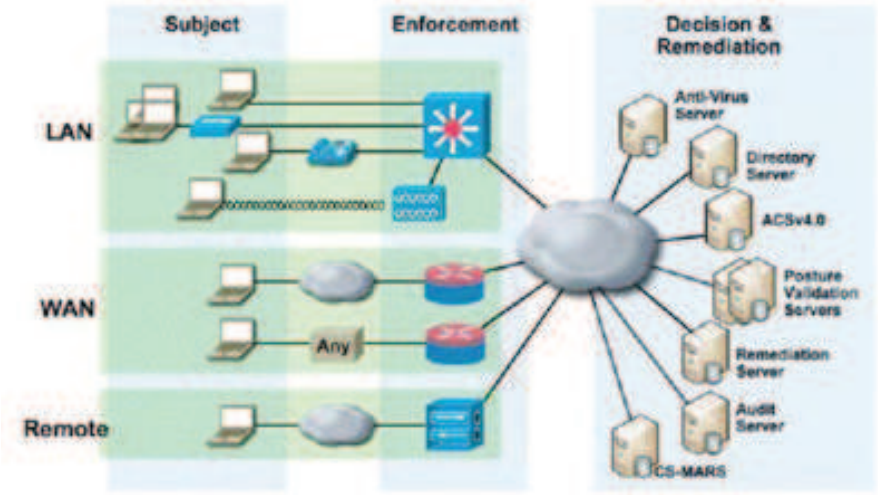

Figura 2. Descripción de la arquitectura CNAC.
Fuente: Cisco Systems, Inc, «Chapter: Posture Validation,» 7 Noviembre 2013. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/user/guide/ACS4_2UG/PstrVal.html#wp134759.

En cuanto a servidores Cisco, se utiliza el Access Control Server que se ha desarrollado para tal fin, completando con interfaces de verificación, auditor*í*a 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.

2.5.1 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:

Cisco Trust Agent (CTA). 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 trasmite 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 [21]. Las características del Cisco Trust Agent son: 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 respaldado 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. 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 3 muestra la descripción de arquitectura del Cisco Trust Agent.

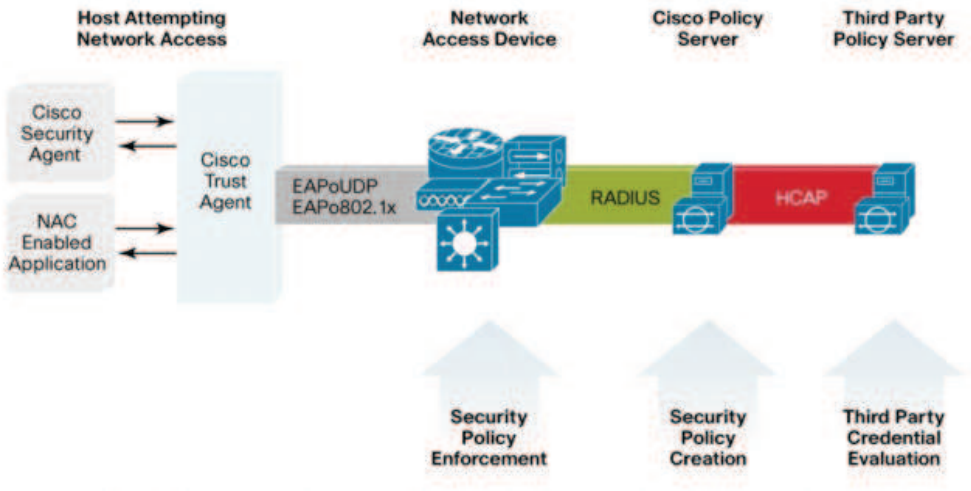

Figura 3. Cisco Trust Agent. Descripción de la arquitectura.
Fuente: Cisco Systems, Inc, «Chapter: Posture Validation,» 7 Noviembre 2013. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/user/guide/ACS4_2UG/PstrVal.html#wp134759.

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.

Cisco Secure Access Control Server. Cisco Secure Access Control de servidor (SCA) [22] 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. 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. El

apoyo a bases de datos externas, los servidores de postura y servidores de auditoría centralizan el control de la política de acceso y le permite integrar sistemas de control de acceso e identidad.

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 solo para dispositivos de punto final y de confianza compatibles (tales como PCs, servidores y PDAs), y pueden restringir el acceso de dispositivos no compatibles [23]. El servidor de validación de postura se utiliza para determinar si un *host* permite el acceso a un dispositivo. 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 4 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.

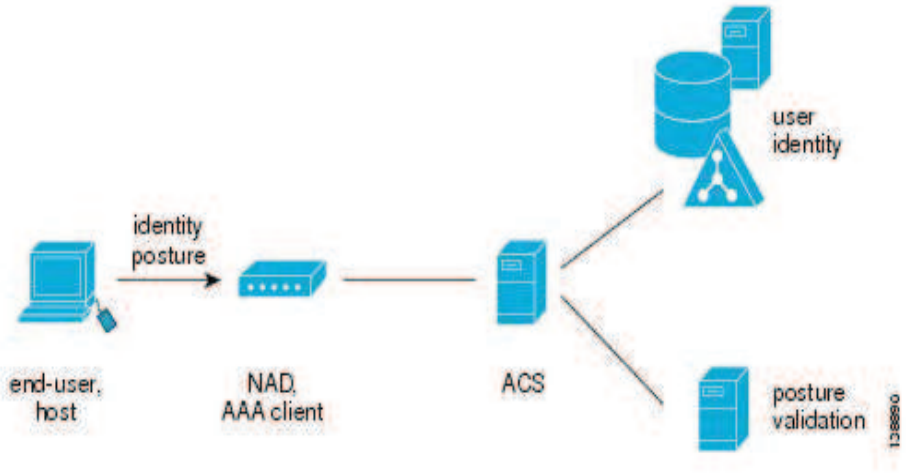

Figura 4. Servidor de validación de postura.
Fuente: A. Westin, «Privacy and Freedom,» 3 1 1968. [En línea]. Available: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.

Servidor de Auditoría. 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. 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. 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 5 muestra cómo los servidores de auditoría encajan en la topología típica.

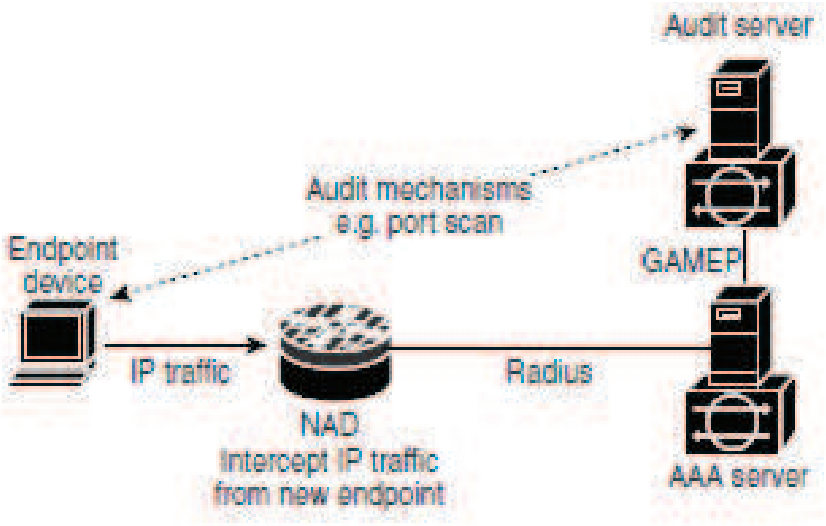

Figura 5. Servidores de auditoría.
Fuente: Cisco Systems, Inc, «Cisco Secure Access Control Server Solution Engine,» 2006. [En línea]. Available: http://www.cisco.com/c/en/us/products/security/secure-access-control-server-solution-engine/index.html.

Para comprender gráficamente cómo interactúan cada uno de los componentes de la solución de Cisco, se presenta a continuación la Figura 6.

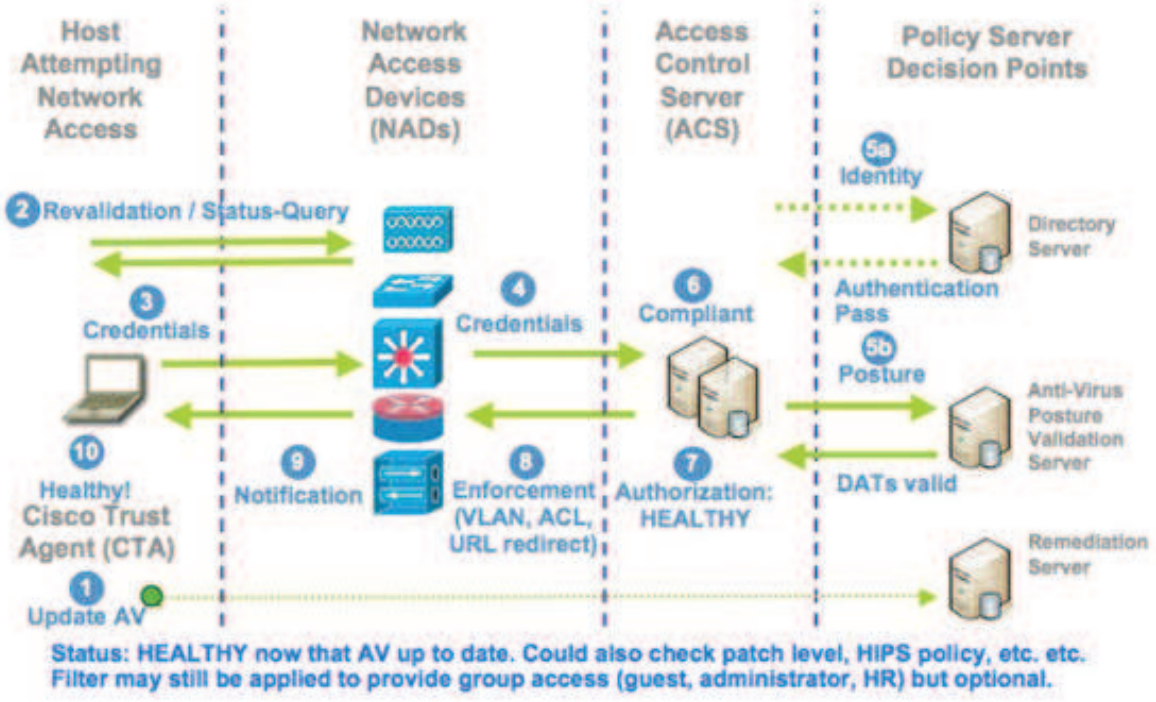

Figura 6. Funcionamiento de Cisco Network Asset Collector.
Fuente: E. Feitosa, L. Oliveira, B. Lins y A. M. Junior, «Security information architecture for automation and control networks.,» 8th Brazilian Symposium of Information Security and Computer Systems, pp. 17-30, 2008.

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 este 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 puesto 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 [23]. 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).

3. Metodología

Tipo de Enfoque	Recolección de datos	Instrumento de recolección de datos	Análisis	Fundamentación
Cualitativo Inductivo.	Orientada a proveer de un mayor entendimiento de los significados y experiencias de las personas.	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.	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.

Tabla 3. Metodología implementada en la investigación.

4. Resultados

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.

4.1 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 con fines de brindar un mejor servicio a los diferentes perfiles de usuario.

4.2. 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 y presentando un amplio cuadro comparativo entre lo que se tiene actualmente, lo que se requiere implementar para la solución y lo que se debe adquirir, 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.

4.3 Etapa de verificación

En esta etapa 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. Los resultados obtenidos en esta etapa de verificación permiten evidenciar el grado de satisfacción relacionado con las características de hardware y software con las que cuentan los dispositivos de red actuales pertenecientes a la infraestructura de red de la UNAB. Los resultados finales obtenidos fueron:

Diagnóstico del estado actual de la infraestructura de red de la UNAB

Este documento muestra el diagnóstico que se realizó una vez se llevó a cabo el levantamiento de la información. El 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 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.

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 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 ocho fases consecutivas, para poder 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.

Fase 1. Comprender la arquitectura NAC. En esta fase se describe de manera general cómo 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 entre 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.

5. 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 tecnología 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 ayudará a las organizaciones a protegerse de 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, esta solución resuelve de manera inicial la problemática presentada en la Red de la Universidad Autónoma de Bucaramanga - UNAB que 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.

Referencias

[1] V. Frias-Martinez, S. . J. Stolfo y A. D. Keromytis, «Behavior-Based Network Access Control: A Proof-of-Concept.,» de Information Security, Springer-Verlag Berlin, 2008, pp. 175-190.

[2] Cisco Networking Academy, CCNA Exploration 4.0 accediendo a la wan, 2009.

[3] International Organization for Standardization - ISO, «ISO/IEC 27001 - Information security management,» 2013. [En línea]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[4] M. Nakhjiri y N. Nakhjiri, AAA and Network Security for Mobile Access: Radius, Diameter,EAP,PKI and IP Mobility., 2005.

[5] J. Carreño Gallardo, «Seguridad en Redes Telemáticas,» McGraw-Hill, 2004, pp. 35-36.

[6] Cisco, «Cisco,» 2014. [En línea]. Available: http://www.cisco.com/en/US/products/ps6128/index.html.

[7] International Organization for Standardization - ISO, «ISO/IEC 27005:2011,» 2011. [En línea]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742.

[8] Information Commisioner's Office-ICO, «Bring your own device (BYOD),» 2014. [En línea]. Available: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf.

[9] Information Security Media Group, «Mobile: Learn from Intel's CISO on Securing Employee-Owned Devices,» 2016. [En línea]. Available: http://www.govinfosecurity.com/webinars/mobile-learn-fromintels-ciso-on-securing-employee-owned-devices-w-264.

[10] L. Spandas, «Citrix favours selective BYOD program,» 2012. [En línea]. Available: http://www.zdnet.com/article/citrix-favours-selective-byod-program/.

[11] O. Rege, «Bring Your Own Device: Dealing With Trust and Liability Issues,» 17 Agosto 2011. [En línea]. Available: http://www.forbes.com/sites/ciocentral/2011/08/17/bring-your-own-device-dealing-with-trust-and-liability-issues/#7cf605625182.

[12] K. Johnson y B. L. Filkins, «SANS Mobility/BYOD Security Survey,» Marzo 2012. [En línea]. Available: http://www.sans.org/reading_room/analysts_program/mobilitysec-survey.pdf.

[13] D. A. Wills, «Bring Yout Own Device: The Facts and the Future,» 2013.

[14] Novenca Security Systems, «Control de Acceso,» 2015. [En línea]. Available: http://www.novenca.com/site/index.php?option=com_content&view=article&id=86&Itemid=164.

[15] Creative Commons Attribution Share-Alike 3.0 License, «Control de acceso criptográfico,» 2016. [En línea]. Available: https://galiciacuamatzi.wikispaces.com/4.4+Control+de+acceso+criptogr%C3%A1fico.

[16] A. Córdoba Téllez y G. Durán Martínez, «Diseño de un sistema de control de acceso con Radius configurado en un sistema operativo Linux para una LAN inalámbrica,» México, 2010.

[17] Cisco, «Cisco IOS and NX-OS EOL Redirect page,» 21 Junio 2013. [En línea]. Available: http://www.cisco.com/c/en/us/td/docs/ios/redirect/eol.html.

[18] Cisco System, Inc, «802.1X,» 2014. [En línea]. Available: http://www.cisco.com/c/en/us/tech/lan-switching/802-1x/index.html.

[19] Cisco Systems, Inc, «Cisco Trust Agent 2.0,» 2005. [En línea]. Available: http://www.cisco.com/c/en/us/products/collateral/security/trust-agent/product_data_sheet0900aecd80119868.html.

[20] Cisco Systems, Inc, «Cisco Secure Access Control Server Solution Engine,» 2006. [En línea]. Available: http://www.cisco.com/c/en/us/products/security/secure-access-control-server-solution-engine/index.html.

[21] Cisco Systems, Inc, «Chapter: Posture Validation,» 7 Noviembre 2013. [En línea]. Available: 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.

[22] E. Feitosa, L. Oliveira, B. Lins y A. M. Junior, «Security information architecture for automation and control networks.,» 8th Brazilian Symposium of Information Security and Computer Systems, pp. 17-30, 2008.

[23] A. Westin, «Privacy and Freedom,» 3 1 1968. [En línea]. Available: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.

Sobre los Autores

Alexa María Ramírez Ardila. Estudiante en la Maestría en Telemática de la Universidad Autónoma de Bucaramanga.

José Gregorio Hernández. Docente de la Universidad Autónoma de Bucaramanga.

Este artículo se cita:

IEEE

A. M. Ramírez A. and J. G. Hernández, “Guía metodológica para la implementación de políticas de control de acceso utilizando la plataforma de Cisco Network Admission Control (CNAC) en la Universidad Autónoma de Bucaramanga – UNAB,” Rev. Colomb. Comput., vol. 18, no. 1, pp. 46–60, 2017.

APA

Ramírez A., A. M., & Hernández, J. G. (2017). Guía metodológica para la implementación de políticas de control de acceso utilizando la plataforma de Cisco Network Admission Control (CNAC) en la Universidad Autónoma de Bucaramanga – UNAB. Revista Colombiana de Computación, 18(1), 46–60.