FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

PROPUESTA PARA LA MIGRACIÓN DE PLATAFORMA ACCESS CONTROL SERVER 3.3 A LA 5.5 EN TIGO BUSINESS, TEGUCIGALPA.

SUSTENTADO POR:

GLENDA YAMILETH VALLADARES ORTEZ

PREVIA INVESTIDURA AL TÍTULO DE
MÁSTER EN ADMINISTRACIÓN DE PROYECTOS

TEGUCIGALPA, F.M., HONDURAS, C.A.
ENERO 2015

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

LUIS ORLANDO ZELAYA MEDRANO

SECRETARIO GENERAL

ROGER MARTÍNEZ

VICERECTOR ACADÉMICO

MARLON ANTONIO BREVÉ REYES

DECANA DE LA FACULTAD DE POSTGRADO

DESIREE TEJADA

PROPUESTA PARA LA MIGRACIÓN DE PLATAFORMA DE CONTROL DE ACCESO EN TIGO BUSINESS, TEGUCIGALPA.

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN ADMINISTRACIÓN DE PROYECTOS

ASESOR METODOLÓGICO
ANA MARGARITA MAIER ACOSTA

ASESOR TEMÁTICO
LUIS FERNANDO GARCÍA

MIEMBROS DE LA TERNA
CARLOS ZELAYA OVIEDO
CARLOS PÉREZ
HECTOR BERRIOS

FACULTAD DE POSGRADO

PROPUESTA PARA LA MIGRACIÓN DE PLATAFORMA DE CONTROL DE ACCESO 3.3 A LA 5.5 EN TIGO BUSINESS, TEGUCIGALPA

AUTOR:

Glenda Yamileth Valladares Ortez

Resumen

El propósito de este estudio es generar una propuesta para migrar la plataforma de control de acceso Cisco Secure Access Control Server 3.3 a la versión más reciente que es la 5.5 en Tigo Business Tegucigalpa en un ambiente de redundancia, con los procedimientos adecuados para lograrlo de manera exitosa. Se comprende la importancia de dicha migración para resolver los problemas que presenta la plataforma 3.3, siendo la que está en producción. Se detalla la situación actual del uso de plataforma ACS a nivel mundial, de Latinoamérica y de Tigo Business, detallando cada variable relacionada para el procedimiento de migración. Así como, la base de datos, interfaz, beneficios, ventajas, debilidades comparación de versión 3.3 y 5.5. De igual manera, se detalla la norma ISO 27001, que es la que regula y asegura la seguridad de la información en una empresa, tomando en cuenta el control de cambios de forma segura, es así como Tigo Business cuenta con un comité de control de cambios en base a esta norma, la cual se debe considerar al momento de crear el procedimiento para migrar la plataforma en un ambiente de redundancia. El resultado de esta investigación, es proponer un procedimiento para realizar la migración de la plataforma Cisco Secure ACS 3.3 a la 5.5 en un ambiente de redundancia, con el objetivo de contar con soporte y garantía por parte de Cisco, estabilidad en la plataforma, contando

con una secundaria y de ese modo resolver los problemas presentados actualmente en dicha plataforma.

Palabras claves: Migrar, redundancia, debilidades, norma, soporte y garantía.

PROPOSAL FOR MIGRATION CONTROL ACCESS CONTROL SERVER 3.3 TO 5.5 IN TIGO BUSINESS, TEGUCIGALPA

By:

Glenda Yamileth Valladares Ortez

Abstract

The main purpose of this study is to generate a proposal to migrate the platform Cisco Secure Access Control Server 3.3 to the latest version 5.5 of Tigo Business Tegucigalpa, in a redundancy environment, with proper procedures to achieve so successful, realizing the importance of this migration to solve the problems of the platform 3.3, which is still in production. The current use of ACS platform worldwide, Latin America and Tigo Business, detailing each variable related to the migration procedure. As the database interface, benefits, advantages, weaknesses comparing version 3.3 and 5.5. Similarly, ISO 27001, which is what regulates and ensures the security of information in an enterprise, taking into account the change control safely, so as Tigo Business has a control committee is detailed changes based on this standard, which should be considered when creating the procedure to migrate the platform in an atmosphere of redundancy. The result of this research is to propose a method for migrating from Cisco Secure ACS 3.3 to 5.5 platform in an atmosphere of redundancy, in objective to have support and warranty by Cisco, stable platform, counting with secondary and thereby solve the problems currently presented on that platform.

Keywords: Migrate, redundancy, weaknesses, standard, support and warranty.

DEDICATORIA

A Dios por permitirme nuevas oportunidades en mi vida, logrando finalizar mi carrera de manera satisfactoria.

De igual manera a mis padres que siempre me han brindado su apoyo a lo largo de mi carrera y vida personal, por sus sabios consejos y motivación para emprender nuevas oportunidades.

Glenda Yamileth Valladares Ortez

AGRADECIMIENTO

A Dios, por darme sabiduría para finalizar esta etapa, por proveer y bendecirme día con día.

A mis padres por los valores que me inculcaron de seguir superándome, por su apoyo y ayuda.

A mis hermanas por su apoyo constante y ánimo.

A mis amigos que me dieron aliento y por el apoyo incondicional.

Y finalmente a UNITEC por su aporte a mi crecimiento y desarrollo profesional, con la ayuda de catedráticos especializados.

ÍNDICE

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

La tecnología tiene una peculiaridad de avanzar día con día, de forma acelerada, es por eso que plataformas como las de Cisco, cambian rápidamente de versiones y de esta manera, corregir errores de las versiones anteriores en las actuales, la mayoría de empresas tratan de centralizar su manera de ingresar a los equipos de forma segura y confiable, evitando la autenticación local en cada equipo por parte de los usuarios.

En el primer capítulo del presente documento se especifica el antecedente del problema y de la repercusión de un procedimiento para migrar la plataforma Cisco Secure Access Control Server 3.3 a una versión actual, considerando los objetivos específicos para justificar dicha problemática y ser llevada a cabo, apoyándose en variables de investigación.

En el segundo capítulo, se detallan las teorías que fundamentan la plataforma Cisco Secure ACS3.3 y 5.5, la arquitectura utilizada en ambas, la base de datos, que es una parte fundamental de las plataformas para almacenar los usuarios y equipos de red para autenticación, debilidades de la versión 3.3 y así mismo el tipo de interfaz que utiliza. En el caso de la versión 5.5 los beneficios de contar con dicha versión y las ventajas, así mismo, una comparación de la versión 3.3 y la 5.5. De igual manera, se menciona la norma ISO 27001:2005 adoptada por Tigo Business para seguridad de información y referencia en otros países sobre dicha plataforma.

Y en el capítulo tres, se detalla la metodología utilizada, incluyendo las variables, el diseño de la investigación, las técnicas y procedimientos que han sido necesarios para recolectar la información del estudio y los limitantes del mismo.

El cuarto capítulo posee los resultados obtenidos de la metodología implementada y el quinto capítulo las conclusiones y recomendaciones del estudio.

1.2. ANTECEDENTES DEL PROBLEMA

1.2.1. PLATAFORMA CISCO SECURE ACCESS CONTROL SERVER

Las empresas de telecomunicaciones con redes extendidas necesitan de sistemas de autenticación centralizados que faciliten la administración de acceso de modo que el alta y baja de usuarios no incurra en configurar todos los equipos de la red para que el usuario tenga o no acceso al mismo. Cisco lanzó al mercado la plataforma Cisco Secure Access Control Server 2.6, siendo esta la primera plataforma de control de acceso por parte de Cisco, de esta manera se podía contar con una forma de autenticación segura para ingresar a los equipos en red (Cisco, 2014b).

Tigo fue la primera empresa de telefonía móvil en el mercado hondureño, iniciando sus servicios oficialmente el 15 de septiembre de 1996 con la misión de ofrecer al pueblo hondureño la nueva y moderna tecnología de Comunicación Móvil, Tigo implementó la primera plataforma de control de acceso usada en la empresa, siendo está la Cisco Secure ACS (Access Control Server) 3.1, el cual vino a ser el método de autenticación para los equipos de la red y poder asegurar el ingreso a los mismos. Luego se hizo una mejora migrándose a la versión 3.3, que es la versión actual de la plataforma de control de acceso en Tigo Business.

Las plataformas de control de acceso brindan disponibilidad de la información y es importante ya que al no tener acceso a ella en tiempo real cuando es necesario, puede causar pérdidas más grandes en una empresa de telecomunicaciones, la cual gestiona la mayoría de sus procesos por plataformas y equipos de redes.

Tener redes seguras no es un lujo, es una necesidad que crece día con día, así como reducir la cantidad de riesgos que se puedan dar, mitigando con mejores prácticas los incidentes que pueda ocasionar pérdidas considerables en la organización.

1.2.2. ISO 27001:2005

Existen estándares de seguridad de la información, como ser ISO 27001, la cual certifica las empresas que de acuerdo a una serie de requisitos que deben cumplir para

poder lograr dicha certificación y ser reconocidas como empresas que tienen su información de manera segura, dando un valor agregado para sus clientes.

Tigo fue recertificada el presente año 2014, debido al cumplimiento de los estándares solicitados por esta norma, es así como se puede posicionar en una de las pocas empresas con certificación ISO.

1.2.3. TIGO

Tigo es la marca GSM que Millicom International Cellular S.A (MIC), lanza al mercado, en el rubro de telefonía celular, en sus operaciones de Latinoamérica (El Salvador, Guatemala, Honduras y Paraguay) y África. Las operaciones de MIC conectan aproximadamente a 392 millones de personas alrededor del mundo. Fue la primera empresa de telefonía móvil en el mercado hondureño, iniciando sus servicios oficialmente el 15 de septiembre de 1996.

Tigo siempre enfatiza en cada negociación el servicio y la atención personalizada; misión que ha destacado en el ámbito económico y social del país. Ha establecido un puente con sus clientes y el mundo entero, permitiéndole hacer de su celular una herramienta de trabajo como oficina móvil y recibir a su vez mensajes de texto desde cualquier parte del mundo, Tigo continua creciendo, incrementando su capacidad y la eficiencia de la red, desarrollando nuevos productos que permitan el acceso a avanzados servicios de comunicación de datos.

Ofrece en la actualidad novedosos servicios y además es una de las pocas empresas en el mundo entero en ofrecer tres opciones de comunicación: CDMA, GSM y 3G. Los clientes podrán escoger aquella tecnología que mejor se adapte a sus necesidades, todo al mejor precio y buen servicio.

Tigo, cuenta con la versión 3.3 de la plataforma Cisco Secure Access Control Server, la cual está obsoleta en el mercado, sin contar con soporte y garantía por parte del proveedor. Es importante que una empresa como Tigo cuente con plataformas más actualizadas, asegurando a sus clientes seguridad en el servicio que brinda.

1.3. DEFINICIÓN DEL PROBLEMA

1.3.1. ENUNCIADO DEL PROBLEMA

Tigo Business cuenta con la plataforma Cisco Secure Access Control Server 3.3, mediante la cual se tiene acceso a todos los equipos de la red, y de esta manera autentican los usuarios. La plataforma está obsoleta, ya no cuenta con garantía ni soporte y es necesario poder migrar a una versión más reciente como lo es la 5.5 para evitar vulnerabilidades.

Así mismo, la plataforma muestra inestabilidad al momento de crear usuarios, cambiar los perfiles, agregar o eliminar equipos de la red, sin tener claro el problema ya que no se puede contactar al personal de Cisco para soporte, debido a que la plataforma salió del mercado y de contar con garantía, como de soporte.

La necesidad de contar con plataformas no obsoletas, ayuda a brindar mayor disponibilidad, seguridad y acceso a los equipos en red y por ende ofrecer un mejor servicio al cliente, sin dudas de la integridad de lo que reciben por parte de Tigo, así mismo, cumplir con las normas establecidas por la institución, aplicando la política de obsolescencia.

Es por eso que la necesidad por seguir un procedimiento para migrar la plataforma es indispensable para mantener una red segura, integra y estable.

1.3.2. FORMULACIÓN DEL PROBLEMA

Tigo Business, cuenta con una plataforma Cisco Secure Access Control Server 3.3 la cual está obsoleta en el mercado y ya no cuenta con soporte ni garantía para problemas al momento de agregar, editar o eliminar usuarios o equipos, por lo cual es necesario migrar a una versión más reciente en una ambiente de redundancia.

¿Qué procedimiento se debe seguir para migrar de la plataforma Cisco Secure Access Control Server 3.3 a la 5.5 en un ambiente de redundancia?

1.3.3. PREGUNTAS DE INVESTIGACIÓN

1. ¿Cuáles son las debilidades de la plataforma Cisco Secure Access Control Server 3.3?
2. ¿Cuáles son los problemas que se van a corregir al migrar la plataforma de la versión 3.3 a la 5.5?
3. ¿Qué se logra al colocar la plataforma Cisco Secure ACS 5.5 en un ambiente de redundancia?
4. ¿Qué tipo de consideraciones se deben tomar en cuanto a la certificación ISO 27001 al momento de migrar la plataforma?

1.4. OBJETIVO DEL PROYECTO

1.4.1. OBJETIVO GENERAL

Facilitar la actualización de la plataforma 5.3 mediante un procedimiento para realizar la migración de la plataforma Cisco Secure Access Control Server a la versión 5.5 en un ambiente de redundancia.

1.4.2. OBJETIVOS ESPECÍFICOS

- Determinar las debilidades de la plataforma Cisco Secure Access Control Server 3.3.
- Describir los problemas que se solucionan en la migración de la plataforma ACS 3.3 a la 5.5.
- Identificar los logros que se obtiene con la migración de la plataforma 3.3 a la 5.5 en un ambiente de redundancia.
- Especificar las consideraciones que se toman en cuenta al momento de migrar la plataforma con respecto a la certificación ISO 27001.

1.5. JUSTIFICACIÓN

Las empresas deben brindar disponibilidad de la información, siendo este un caso importante para poder migrar la plataforma Cisco ACS en un ambiente de redundancia, logrando de esta manera, reducir el tiempo de respuesta del servicio ante

una falla crítica. De esta manera, entra en gestión el Cisco ACS secundario mientras el principal está siendo revisado para volver a entrar en gestión y normalizar la operación.

Así mismo, el Cisco ACS 3.3 es una plataforma que está obsoleta, que ya no cuenta con garantía ni soporte. Además, muestra problemas en los cuales no puede eliminar completamente algunos usuarios, cuando es necesario darles de baja y errores al momento de efectuar cambios en las configuraciones de los equipos que se han ingresado en la misma.

Si con la migración estos problemas mencionados vuelven a suceder, se contaría con equipo bajo soporte y garantía, brindando mayor disponibilidad y eficiencia en la plataforma de acceso de Tigo Business. Sin lugar a duda, la mejora continua en base a las buenas prácticas y procesos, permiten respaldar la seguridad de la información en una empresa.

Seguir las normas que Tigo Business ha implementado, servirán para poder llevar a cabo de la mejor manera, el procedimiento para la migración del Cisco ACS en un entorno de redundancia, sin afectar la gestión de la red según lo estipule el comité de control de cambios.

CAPÍTULO II. MARCO TEÓRICO

2.1. SITUACIÓN ACTUAL

2.1.1 ANÁLISIS DEL MACRO-ENTORNO

La Plataforma Cisco Secure Access Control Server es un producto de Cisco usado a nivel mundial para el control de acceso de los usuarios a los equipos de una manera centralizada, como el siguiente caso:

- **UNIVERSIDAD DE GRANADA**

La Universidad de Granada junto con Cisco crearon un campus virtual inalámbrico, en el cual permiten a sus alumnos el acceso inalámbrico de la universidad, basando sus plataformas en las soluciones de Cisco, el sistema de conexión remota es de 2,000 usuarios, la Universidad estudia el uso del usuario final ya que hacen uso de Cisco Secure Access Control Server por medio del servidor Radius que este contiene (Cisco, 2002)

"Dentro de la idea de globalización de los servicios, estamos analizando la posibilidad de ponerlo en producción con VPN's y PPTP contra el servidor de Radius de Cisco Secure ACS, que será el que accederá a la base de datos centralizada de Oracle." (Ruiz, 2002)

Cisco cuenta con producto y soporte para países de Europa, América Latina, África, el Pacífico de Asia.

- **CISCO SECURE ACCESS CONTROL SERVER**

Migrar la plataforma de control de acceso a una nueva versión en un ambiente de redundancia, posibilita la mejora en la disponibilidad de la información en el tiempo que se solicita, Cisco Secure ACS (Access Control Server) es una plataforma que cumple con los requisitos de seguridad y ofrece una mejora en la configuración eliminando problemas de la versión 3.3. "Esta aplicación permite el control total sobre toda la autenticación, autorización y el manejo y configuración de registro (AAA) basado en Cisco" (*Managing Cisco Network Security (Second Edition)*, 2002, p. 633).

Cisco Secure ACS cuenta con 14 versiones para todos los países a los cuales les provee a nivel mundial, a continuación se muestran 2 gráficos de dichas versiones con las fechas finales de venta y las fechas finales de soporte para cada una de ellas:

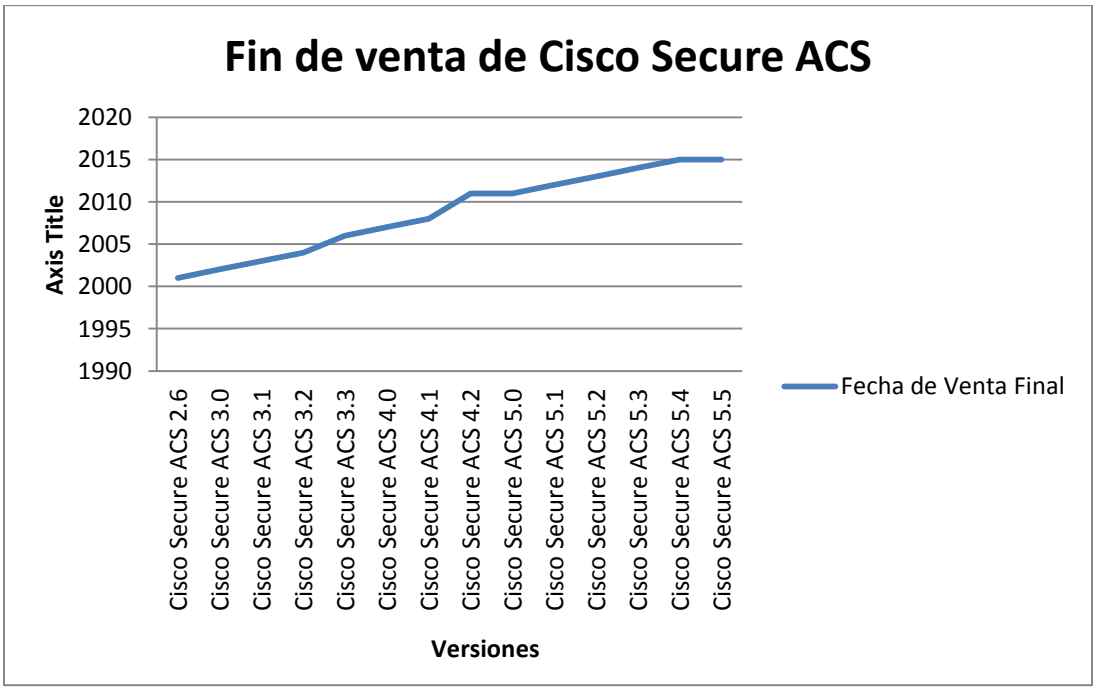

Figura 1. Fecha de ventas Final de Cisco Secure ACS

Fuente: (Cisco, 2014b)

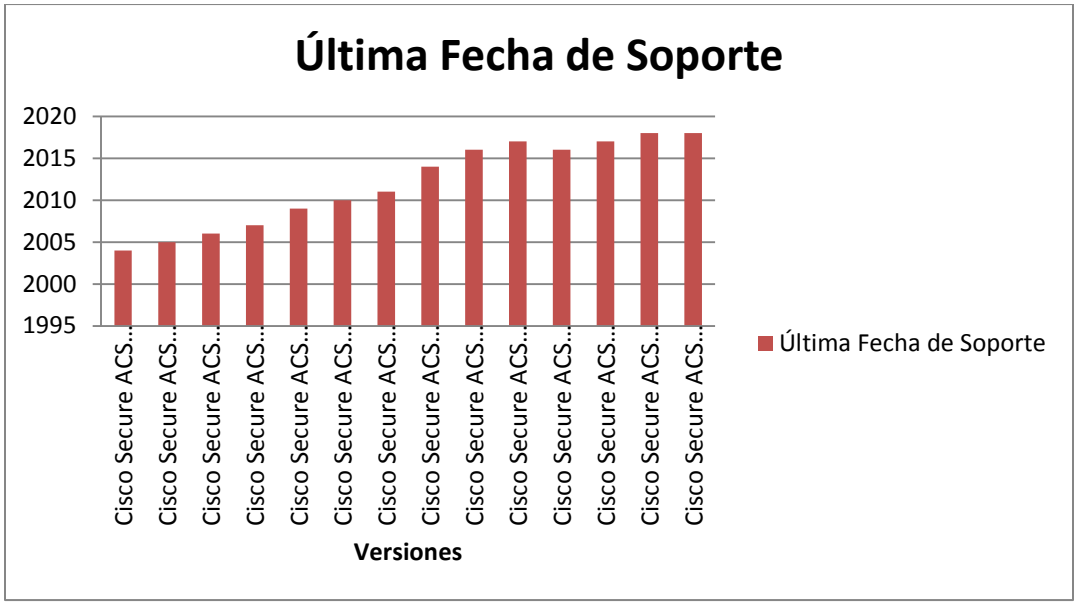

Figura 2. Última fecha de soporte de Cisco Secure ACS

Fuente: (Cisco, 2014)

- **ARQUITECTURA AAA**

La arquitectura AAA por sus siglas Autenticación, Autorización y Administración; es la forma en la que un usuario solicita acceso a los recursos de la red y este confirma la identidad de dicho usuario por el método de autenticación correspondiente. Con el ACS existen diferentes métodos entre el server y los equipos en red que funcionan para autenticar. Para poder incrementar la seguridad, los encargados de administrar la plataforma pueden usar protocolos como ser TACACS+ (Sistema de Control de Acceso del Controlador de Acceso a Terminale) y RADIUS (Remote Authentication Dial-In User Service). (*Managing Cisco Network Security (Second Edition)*, 2002).

En la autorización, se debe asignar una dirección IP o un filtro con el objetivo de definir qué tipo de protocolos o aplicaciones serán necesarias, pero la autorización debe ir en conjunto con la autenticación. (J & Bertolín, 2008). En sí, este método trata de otorgar privilegios a los usuarios que lo solicitan, permitiendo o rechazando la solicitud, dependiendo de los ACL (Listas de Control de Acceso) de este modo, se asegura que solo aquellos que tienen el permiso del acceso puedan ingresar.

Y finalmente, los registros, los cuales se encargan de recolectar detalles del sistema e información de los comandos ejecutados por los usuarios y almacenarlos en el servidor central, estos pueden ser usados para ver intentos de intrusión, anomalías o comando ejecutados que no son permitidos a ciertos usuarios y de esta manera poder tomar medidas contra dichas actividades no autorizadas. (Dooley & Brown, 2007).

Los registros son una parte importante para poder mitigar riesgos y disminuir cualquier cantidad de incidentes que se puedan presentar para dañar la estabilidad de la operación diaria de la empresa en la gestión de la red.

En la figura 1. Se muestra un ejemplo práctico de la arquitectura AAA usando un ACS (Santuka, Banga, & Carroll, 2010)

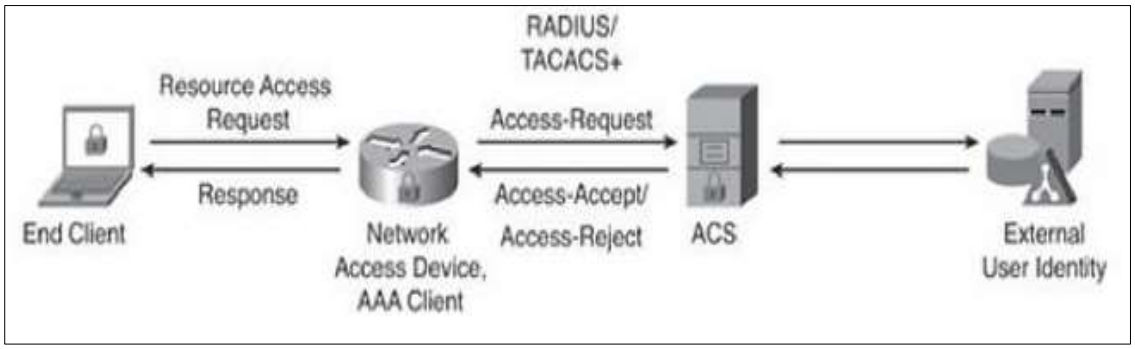

Figura 3. Escenario AAA usando ACS

2.1.2 ANÁLISIS DEL MICRO-ENTORNO

Las empresas de algunos países de América Latina, que cuentan con plataformas, se ven obligados a cambiar a versiones recientes, migrando dichas plataformas, ya sean por normas, soporte o estándares. En el caso de México, cuenta con la Plataforma de México, según el artículo 46 del reglamento interior de la Secretaria de Gobernación, se debe diseñar manuales o estándares que influyen en el soporte y mantenimiento para la plataforma. (SEGOB, 2013). Es aquí cuando después de cierto periodo de tiempo las plataformas se vuelven obsoletas y es importante migrar a nuevas versiones que cuenten con soporte por expertos.

Debido a los cambios en la tecnología las empresas se ven obligadas a migrar las plataformas con las cuentan, haciendo uso de normas y políticas internas, con el objetivo de mantener sus operaciones estables y seguras, como lo es el caso de la plataforma Cisco Secure Access Control Server.

A continuación se menciona un ejemplo de un país que ha optado por el uso de la plataforma ACS:

BUENOS AIRES

En Buenos Aires, la Escuela de Dirección de Negocios de la Universidad Austral hizo un cambio total en su red en el cual se refleja la implementación del ACS para temas de validación como parte de la actualización de la red así como plataformas con equipos PIX 515. Centralizaron en el ACS, las VLANs dinámicas y la VPN, ya que estas se encontraban bajo un mismo nivel en cuanto a su validación (Cisco, 2004). Sin duda, que tener sistemas de autenticación centralizados como el ACS ayuda a las empresas a realizar sus operaciones de maneras más prácticas.

Cisco es considerada en América Latina la empresa que ocupa el primer lugar en seguridad en el mercado, y es importante para cualquier organización, obtener servicios de empresas prestigiosas, un reporte de una firma de inteligencia de mercado y consultoría en Tecnologías de la información menciona que “Cisco refuerza su posición como líder, con una participación del 25.4% del mercado de seguridad en la región durante la primera mitad del 2104.” (Cisco, s. f.-b)

Hoy en día, es importante contar con empresas que brinden seguridad en sus productos y servicios, de modo, que los clientes se sientan satisfechos. En América Latina, Cisco cuenta con oficinas en los países (Cisco, 2014):

- Miami
- Venezuela
- El Salvador
- República Dominicana
- Puerto Rico
- Perú

- Panamá
- México
- Ecuador
- Costa Rica
- Colombia
- Chile
- Brasil
- Argentina

2.1.3 ANÁLISIS INTERNO

Según Tigo (2011), La migración de las plataformas deben pasar por un proceso de aprobación técnica en el cual se especifiquen las carencias del sistema y de este modo pasar a revisión por parte del CCC (Comité de Control de Cambios) enviando un SMOP (Service Metod of Procedure) en el cual se debe detallar lo siguiente:

- Nombre del proyecto a ejecutarse
- Si afecta la seguridad de la información
- Tipo de cambio que se realiza
- Objetivo General y específicos del proyecto
- Topología de equipos que se implementan (si aplica).
- Impacto del proyecto
- Responsables del proyecto
- Requerimientos para la ejecución
- Procedimiento
- Cronograma de actividades
- Pruebas
- Procedimiento de Rollback
- Diagrama Final (si aplica)
- Verificación del funcionamiento

El CCC después de recibir el SMOP evalúa los riesgos que se pueden presentar en la migración de la plataforma y que pueda ser crítico para la gestión de la red, determinando si deben agregar algunos pasos importantes, hacer correcciones, si se rechaza el cambio que se desea realizar o se aprueba en base a las políticas y juicio de expertos.

El comité está conformado por el Jefe de Administración de la Red de Producción, Jefes de Mantenimiento e Instalaciones de Tegucigalpa y San Pedro Sula, así mismo, el Jefe de Technical Support Center y de la Especialista de Plataformas de Producción. El comité de control de cambios es un equipo capaz de tomar decisiones en base a su conocimiento y posición que desempeñan en Tigo Business.

Luego de tomar una decisión unánime se refleja en una minuta informando su aprobación o rechazo, se envía de igual forma, las fechas en las que se realizarán las ventanas de mantenimiento, si el cambio requiere la compra deberán seguirse el lineamiento de proceso de compras y finalmente informar a todas las partes interesadas. (Tigo, 2011)

Cisco, no cuenta con oficinas en Honduras, pero cuenta con soporte para el mismo en países de Centroamérica como ser, Costa Rica y El Salvador. Es importante tomar en cuenta este tipo de consideraciones al momento de obtener equipos de seguridad en la empresa para ser utilizado y que al momento de presentar un problema, este pueda contar con soporte para resolverlos,

Tigo Business, es una empresa certifica con ISO 27001:2005, por lo tanto debe asegurarse de contar con equipos de seguridad, como lo son los de Cisco, una empresa prestigiosa a nivel mundial, que permite que los equipos puedan ser parte para cumplir con las normas de seguridad establecidas por la empresa, con el fin de brindar a sus clientes, productos y servicios seguros.

A continuación, se detalla la visión, la misión y los valores que posee Tigo Business:

Visión de Tigo

Nuestros clientes son tan importantes para nosotros, que hemos invertido todos nuestros recursos, esfuerzo, capacidad, y esmero para brindarle un mayor servicio, creando estructuras sólidas e innovadoras que les aseguren un soporte inmediato al momento de hacer uso de los beneficios de la tecnología móvil celular, buscando satisfacer las necesidades de comunicación que tienen todos y cada uno de nuestros usuarios.

Misión de Tigo

Ampliaremos nuestra misión y seguiremos creciendo al reinvertir nuestras ganancias en el diseño, creación y mantenimiento de nuevos productos que provean servicios de calidad, siempre ubicando nuestros recursos disponibles a la vanguardia de la tecnología y preparándonos para brindarle siempre las creaciones e innovaciones que traen consigo el tocar puertas del siglo XXI.

Valores de Tigo

- Compromiso con la visión y misión.
- Honestidad y Transparencia.
- Lealtad y Sentido de pertinencia.
- Responsabilidad Social y Ambiental.
- Comunicación efectiva.
- Pro actividad, Creación e Innovación.

2.2 TEORÍAS

2.2.1 CISCO SECURE ACS 3.3

Cisco Secure ACS 3.3 es una versión de la plataforma de control de acceso, que contiene la arquitectura AAA para los dispositivos de red, cuenta con una base de datos local, con esta plataforma se puede administrar de forma efectiva las cuentas de usuarios, así como, la administración por grupos, colocando niveles y manejándose de

manera global o individual, se pueden hacer restricciones por horas y por el tipo de equipos a los que se van a ingresar.

Los protocolos usados por el ACS 3.3 son el TACACS+ y RADIUS que proporcionan el AAA, así mismo, incluye servicios de CSAdmin, que ofrece una interfaz HTLM (HyperText Markup Lenguage) para poder administrar el ACS, servicios de autenticación, sincronización con base de datos externas, registros, monitoreo, comunicación entre los clientes TACACS+ AAA y el servicio de autenticación, de igual manera para clientes RADIUS y estos servicios pueden detenerse o iniciarse individualmente. («User Guide for Cisco Secure ACS for Windows Server Version 3.3 - System Configuration», s. f.)

A continuación se muestra una comparación entre los protocolos usados por el ACS (Paquet, 2012):

Tabla 1. Comparación de TACACS+ y RADIUS

	TACACS+	RADIUS
Funcionalidad	AAA separados	Combina la Autenticación y la autorización
Protocolo de Transporte	TCP	UDP
CHAP	Bidirecional	Unidireccional
Compatibilidad con el protocolo	Soporta Multiprotocolos	No ARA, no NetBEUI
Confidencialidad	Encripta el paquete entero	Encriptación de la contraseña
Personalización	Proporciona la autorización de los comandos de routers por usurio o por grupo	no tiene la opcion de autorizar comandos de routers por usuarios o por grupos
Registros/Contabilización	Limitada	Extensa

2.2.1.1 BASE DE DATOS

En el ACS 3.3 la base de datos es muy importante, ya que de esta depende para el tamaño de base de los usuarios, distribución, requisitos y todo lo que aporta a como se utiliza el Cisco ACS. Pueden usarse base de datos locales o base de datos externas,

en el caso del Cisco Secure ACS 3.3 la base de datos que se maneja es la local, dependerá del administrador decidir qué tipo de base de datos usará.

La base de datos local de Cisco Secure ACS proporciona soporte completo de características. Así mismo, la velocidad máxima para la autenticación. Puede tener problemas de escalabilidad regionales que pueden ser minimizados mediante la replicación de la base de datos, sin embargo, esa replicación requiere una relación primario/secundario entre los sistemas de Cisco Secure ACS. («Cisco Secure Access Control Server Deployment Guide», s. f.)

Las bases de datos externas que pueden ser usadas son (Paquet, 2012, p. 168).:

- Windows Database
- Generic LDAP
- External ODBC Databse
- LEAP Proxy RADIUS Server
- RADIUS token server
- RSA SecurID Token Server

2.2.1.2 DEBILIDADES

A medida pasa el tiempo, los errores en las plataformas son más comunes y este es el caso para Cisco Secure ACS 3.3 ya que esta plataforma no cuenta con soporte, ni garantía, debido a que es vieja y ya salió del mercado, la vida útil fue en Febrero del 2006 y la última fecha de soporte fue en Agosto del 2009. Por lo cual, la solución de problemas se lleva realiza sin la ayuda de expertos, maximizando el tiempo de resolución de falla.

Es importante considerar que la vida útil de las plataformas no exceda el tiempo en el que las mismas se encuentran en producción, para poder evitar problemas que se puedan ir presentando y así, contar con plataformas más estables, seguras y que cuenten con soporte por expertos y garantía.

2.2.1.3 INTERFAZ HTML

La interfaz HTML que tiene el Cisco Secure ACS tiene tres ventanas que son la navegación, el área de configuración y el de visualización. En el área de navegación están los botones («User Guide for Cisco Secure ACS for Windows Server Version 3.3 - System Configuration», s. f.):

- User Setup, en este es donde se agregan, editan o eliminan los usuarios, de la misma manera, aquí se puede ver el listado de usuarios que han sido agregados, asignarlos a un grupo o editar las configuraciones necesarias para el usuario.
- Group Setup, aquí se configuran los protocolos y servicios para los grupos de usuarios, en el cual se permite o deniega algunos comandos.
- Shared Profile Components, es en el cual se agregan y editan las restricciones y se aplican los ACL (Listas de Acceso).
- Network Configuration, aquí se configuran los equipos de la red, con sus respectivos nombres, IPs, llaves y grupo al que pertenece.
- System Configuration, es donde se configuran los servicios del sistema.
- Interface Configuration, es aquí donde se muestran u ocultan las características y opciones que se van a configurar.
- Administration Control, en esta parte se configuran todas las políticas de acceso, que usuarios tienen permisos para editar o agregar usuarios a la plataforma, así como la de los grupos, comandos y administración en general.
- External User Databases, en esta parte se configuran las bases de datos externas, políticas de usuarios desconocidos y los grupos de mapeo.
- Reports and Activity, se muestra en esta ventana los LOGs o registros de acceso, los intentos fallidos de los usuarios a los equipos, y los registros de comandos ingresados a los equipos de la red que autentican con el Cisco Secure ACS.

La interfaz HTML facilita de forma gráfica las configuraciones necesarias para ser realizadas en la plataforma de control de acceso como lo es el Cisco Secure ACS, a continuación se muestra una imagen de la interfaz HTML (Laet & Schauwers, 2005).:

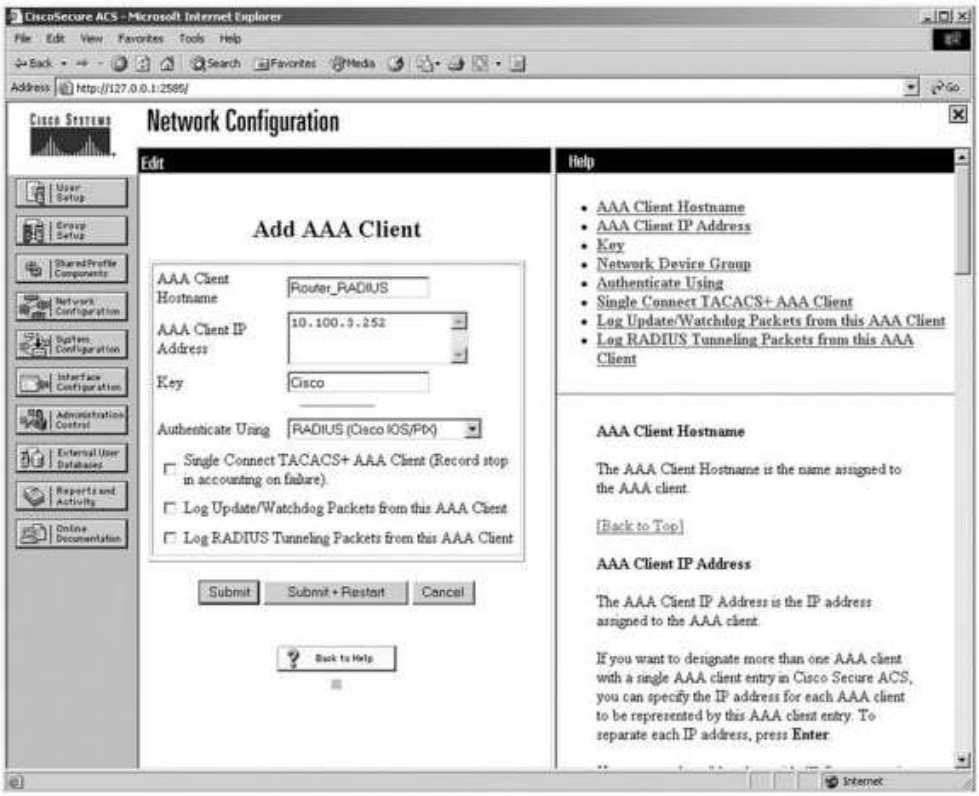

Figura 4. Cisco Secure Access Control Server 3.3

2.2.2 CISCO SECURE ACS 5.5

La plataforma Cisco Secure ACS 5.5 es una versión mejorada de la 3.3 que corrige varios problemas que esta versión presentaba, esta también se basa en la estructura AAA, ofrece un modelo de políticas basado en reglas que controlan de manera dinámica el acceso a la red y de este modo satisfacer aquellas necesidades de las políticas complejas. También es compatible con los protocolos TACACS+ y RADIUS, a diferencia que es compatible con el RADIUS VSAs (Vendor-Specific Atributtes).

La versión del ACS 5.5 es similar a la versión 4, ya que estas constan de plataformas primarias y secundarias, la forma de la replicación de la configuración se efectúa en los secundarios, de esta manera, se asegura la estabilidad de la plataforma ya que al fallar la primaria, la secundaria toma el rol de la principal y de su configuración, dejando disponible el servicio de la misma.

La interfaz de usuario es basada en web, así mismo, cuenta con una interfaz de línea de comandos (CLI). “CLI es una aplicación informática que actúa como interface para comunicar al usuario con el sistema operativo mediante pantalla completa o ventana que espera ordenes escritas por el usuario en el teclado” (García, 2010).

Se puede manejar un solo ACS, pero lo más recomendable es manejar dos plataformas ACS para que se puedan gestionar las solicitudes de autenticación, autorización y registro, en redundancia, así mismo, se puede asignar como colector de registro, para monitorear uno de los ACS, o bien, el primario.

La disponibilidad al balancear la carga de los ACS primario y secundario, sería mayor que al tener un solo ACS y simplificaría la gestión de cada solicitud AAA, lo recomendable es ubicarlos de manera regional y de esta manera, se evita que algún desastre natural pueda afectar ambos ACS, aplicando buenas prácticas en la redundancia.

Tabla 2. Roles del ACS Server

ACS Server Roles	Role Descriptions
Primary	Configuration changes performed on the primary ACS server are replicated to all the secondary ACS servers in the deployment. At a time, you can have only one ACS server as the primary server.
Secondary	All ACS servers that receive configuration changes from the ACS primary server, are secondary servers.
Log Collector	ACS primary or secondary server that is also the log collector for the Monitoring and Report Viewer. There can only be one log collector in a deployment. Other ACS deployments (servers not synchronized with this deployment) cannot send ACS logs to this server.

Fuente: («Migration Guide for Cisco Secure Access Control System 5.5 - ACS 5.5 Deployment Overview [Cisco Secure Access Control System 5.5]», s. f.)

2.2.3 MIGRACIÓN DE PLATAFORMAS ACS

La migración de una plataforma a una versión reciente puede ser de mucha ayuda para corregir problemas y al mismo tiempo evitar la obsolescencia de los equipos.

2.2.3.1 BENEFICIOS

Corregir los problemas de la versión 3.3 mediante migración de versión, así mismo, contar con soporte para los problemas que se puedan ir presentando a medida que la plataforma entre en gestión, de igual manera, contar con el aporte de resolución de problemas por expertos, minimizando el tiempo de respuesta.

Cumplir con las normas ISO 27001 y la política de obsolescencia, en la cual se garantiza que la vida útil de los servidores y plataformas no sobrepase el tiempo que se encuentra en operación en Tigo Business, en el cual se deberá contemplar las consideraciones relevantes para la toma de decisión de la sustitución de equipo que esté por entrar en obsolescencia.

Un despliegue ACS puede obtener un mayor procesamiento de solicitudes de autenticación, autorización y registro con la ayuda de un segundo ACS, ya que estos pueden ser implementados para otras funciones más específicas, como se colector de los registros, procesamiento de solicitudes y el primario podría quedar en rol de cambios en configuraciones, haciendo más eficiente el procesamiento de las mismas. («Migration Guide for Cisco Secure Access Control System 5.5 - ACS 5.5 Deployment Overview [Cisco Secure Access Control System 5.5]», s. f.)

2.2.3.2 VENTAJAS DE LA MIGRACIÓN

Las ventajas de la migración de versión 3.3 a 5.5 es contar con una garantía y soporte para el equipo, de igual manera, un mejor rendimiento, plataforma HTML mejorada, independencia de los problemas del servidor Windows físico antiguo. Si la red pierde gestión por una falla, contar con una plataforma redundante beneficia la disponibilidad de la misma, así como, el acceso a la información que esta contiene y que es de vital importancia para la empresa.

La mejora en la base de datos local, permitiendo que la información este integra y que pueda ser modificada cuando se solicite sin tener problemas al ser guardada y que está pueda ser de manera exitosa, de tal forma, que se pueda con los usuarios y configuraciones de los equipos en producción. Las ventajas de poder migrar las plataformas a una nueva versión es que estas poseen mejoras de las versiones anteriores, facilitando a los usuarios el uso del mismo, corrigiendo riesgos y optimizando recursos.

Además, las plataformas Cisco ACS al contar con un servidor de autenticación RSA SecureID Token, brindan más seguridad en cuanto a las contraseñas de los usuarios, ya que estos poseen un Token en el cual la contraseña cambia cada 60 segundos agregando un código de cuatro dígitos que deberá ser aprendido por el usuario, de tal forma, que no se puedan compartir las contraseñas, aumentando de esta manera el nivel de seguridad en la autenticación de los equipos de la red, cumpliendo las normas establecidas de la seguridad de la información.

2.2.3.3 COMPARACIÓN DE VERSIONES

A continuación, una lista de comparaciones de funcionamiento de las versiones de los Cisco ACS, con respecto a las políticas de contraseñas (Cisco, s. f.-a):

Tabla 3. Lista de comparación de funciones

Feature	ACS 3.x and 4.x	ACS 5.5	Notes
Identity Store Support			
Internal	Yes	Yes	
Active Directory	Yes	Yes	
LDAP	Yes	Yes	
RDBMS	Yes	No	
RSA SecurID	Yes	Yes	
Other One-time Password Servers	Yes	Yes	Uses RADIUS interface to OTP server
AAA Proxy Support			
RADIUS proxy	Yes	Yes	Includes EAP Proxy
TACACS+ proxy	Yes	Yes	
Logging Destinations			
ACS View	Yes	Yes	
Syslog	Yes	Yes	
ODBC	Yes	No	ACS 5.5 provides View log data synchronization with an external database for archival purposes

Para poder realizar una migración de la versión 3.3, debe actualizarse el ACS a una versión 4.x y luego a la versión 5.5, las diferencias de las versiones a la 5.5 son la replicación, que antes el bloque hacia una replicación en cascada, sin importar la magnitud del cambio que se efectuará, se replicaba todo el bloque, las actualizaciones de las contraseñas TACACS+ se recibe únicamente el servidor primario, mientras que la versión 5.5 no existe el tipo de replicación en cascada, los cambios de las configuraciones se pueden hacer solo en el server principal y las actualizaciones de las contraseñas TACACS+ se pueden obtener de cualquier instancia del ACS. (Cisco, s. f.-a)

En cuanto a las identidades de almacenamiento, la diferencia radica en que la versión 5.5 no soporta conectividad de Bases de Datos abiertas (ODBC), como lo hacían las versiones 3 y 4. El objetivo de ODBC es que sin importar de qué aplicación

quieran acceder, esta podrá lograrlo, aunque se conecte de cualquier sistema de gestión de base de datos (SGBD) (Chick, 2011).

2.2.4 ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. («¿Qué es norma ISO 27001? | 27001Academy», s. f.)

En el caso de Tigo Business, está certificada por ISO 27001, pasando por una auditoria este año 2014, logrando cumplir los estándares necesarios para poder recertificarse, dando un valor agregado a la empresa y a sus procesos, así como a la seguridad de la información que es un activo de suma importancia para la empresa, así mismo, asegura la confidencialidad, integridad y disponibilidad de la misma. Uno de los principales objetivos es que aumenta la credibilidad al reducir riesgos de fraude, pérdida o revelación de información (Alexander, 2005)

El alcance de ISO 27001 en Tigo business es:

- Control de cambios
- Monitoreo
- Aprovisionamiento (Instalaciones)
- Mantenimiento
- Auditoria de Ancho de Banda.

Para aplicar un cambio en la red de Tigo Business, como ser la migración de la plataforma Cisco Secure ACS 3.3, se debe seguir una serie de requerimientos para poder cumplir con las normas especificadas por ISO 27001, mediante la aplicación de políticas establecidas por la empresa en base a los procesos que deben seguir para poder mitigar riesgos, evitar la falta de disponibilidad en la empresa y de la gestión de la red.

Parte de los controles de ISO 27001:2005, son la Gestión de seguridad de red, en el cual se asegura la información que puede estar almacenada en la red, de igual manera la infraestructura de soporte, esto protegiéndolo de personal no autorizado, evitando fugas de información, siguiendo el procedimiento adecuado del proceso según lo indique la norma.

El control de accesos, es muy importante ya que determina quienes son las personas que cuentan con privilegios para poder acceder a determinados equipos, se define una política de control tomando en cuenta los requerimientos de seguridad, en la parte de gestión de usuarios, se desea asegurar que cada usuario cuente con los permisos de acuerdo a su perfil para definir si él podrá ser autorizado o no autorizado, de esta manera se evitan permisos innecesarios que puedan poner en riesgo el sistema de la empresa y restringir en base a privilegios y a la capacidad de conexión de los mismos. (Alexander, 2007).

2.3 CONCEPTUALIZACIONES

Parte de la investigación, es contar con apoyo de conceptos esenciales para el estudio, a continuación los conceptos y definiciones importantes:

- **Política de seguridad.** Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de la política general y, por tanto, ha de ser aprobada por la dirección. (López, 2010).

- **Autenticación.** Capacidad de una de las partes de una transacción para verificar la identidad de la otra parte. (Laudon & Laudon, 2008).

- **TCP/IP (Transmission Control Protocol/ Internet Protocol).** Es un protocolo de enrutamiento que garantiza un servicio fiable, orientado a la conexión para un grupo importante de octetos. Internet Protocol, proporciona un sistema de entrega de paquetes sin conexión y no fiable. (Atelin & Dordoigne, 2007).

- **Cisco Secure ACS (Access Control Server).** Es una plataforma de control de la política de acceso que ayuda a cumplir con los requisitos regulatorios y

corporativos en crecimiento. («Cisco Secure Access Control Server for Windows - Products & Services», s. f.-b).

- **DNS (Sistema de Nombre de Dominio).** Maneja la asignación de nombres dentro de internet. (Tanenbaum, 2003).

- **Base de datos.** Sistema computarizado para llevar registros. (Date & Faudón, 2001).

- **SGBD.** Sistema gestor de base de datos, es la información almacenada, que cumple una serie de características y restricciones, pero para que esa información pueda ser almacenada y el acceso a la misma satisfaga las características exigidas a una base de datos, es necesario que exista una serie de procedimientos, un sistema software que se capaza de llevar a cabo la labor. (Cabello, 2010)

- **RSA.** Es un algoritmo que provee una contraseña cada 60 segundos, la cual puede ser usada una sola vez. («RSA Token Server and SDI Protocol Usage for ASA and ACS», s. f.).

- **Firewall.** Son medio eficaces de protección de un sistema o red local frente a las amenazas de seguridad provenientes de la red. (Stallings, 2004).

- **Confidencialidad.** Servicio del sistema que nos garantiza que sólo podrán acceder a la información los usuarios autorizados. (Balado, 2005).

- **Integridad.** Garantiza que el contenido del mensaje no ha sido alterado durante la comunicación, asegurando que el mensaje enviado por el emisor es exactamente el mismo que ha recibido el receptor. (Pérez, 2008).

- **Disponibilidad.** El grado en que un dato está en el lugar, momento, y forma en que es requerido por el usuario autorizado. (Garreta, 2003).

- **Gateway.** Permite a dispositivos con diferentes protocolos comunicarse entre sí. (Com, 2007).

- **Análisis de Riesgos.** Identifica los peligros que afectan la seguridad, determinar su magnitud e identificar las áreas que necesitan salvaguardar. (J & Bertolín, 2008).

CAPÍTULO II. METODOLOGÍA

3.1 CONGRUENCIA METODOLÓGICA

3.1.1 LA MATRIZ METODOLÓGICA

Tabla 4. Matriz Metodológica

TITULO	PROBLEMA	PREGUNTAS DE INVESTIGACIÓN	OBJETIVO		VARIABLES	
			GENERAL	ESPECIFICO	INDEPENDIENTE	DEPENDIENTE
Migración de plataforma Access Control Server 3.3 a la 5.5 en Tigo Business, Tegucigalpa.	No existe procedimiento para migración de plataforma.	1. ¿Cuáles son las debilidades de la plataforma Cisco Secure Access Control Server 3.3?	Proporcionar el procedimiento para realizar la migración de la plataforma Cisco Secure Access Control Server 3.3 a la versión 5.5 en un ambiente de redundancia.	Determinar las debilidades de la plataforma Cisco Secure Access Control Server 3.3.	Debilidades de Cisco Access Control Server 3.3	Procedimiento para migrar la plataforma Access Control Server 3.3 a 5.5
		2. ¿Cuáles son los problemas que se van a corregir al migrar la plataforma de la versión 3.3 a la 5.5?		Describir los problemas que se solucionan en la migración de la plataforma ACS 3.3 a la 5.5	Problemas	
		3. ¿Qué se logra al colocar la plataforma Cisco Secure ACS 5.3 en un ambiente de redundancia?		Identificar los logros que se obtiene con la migración de la plataforma 3.3 a la 5.3 en un ambiente de redundancia.	Logros de la migración	
		4. ¿Qué tipo de consideraciones se deben tomar en cuanto a la certificación ISO 27001 al momento de migrar la plataforma?		Especificar las consideraciones que se toman en cuenta al momento de migrar la plataforma con respecto a la certificación ISO 27001.	Consideraciones en base a ISO 27001	

3.1.2 OPERACIONALIZACIÓN DE LAS VARIABLES

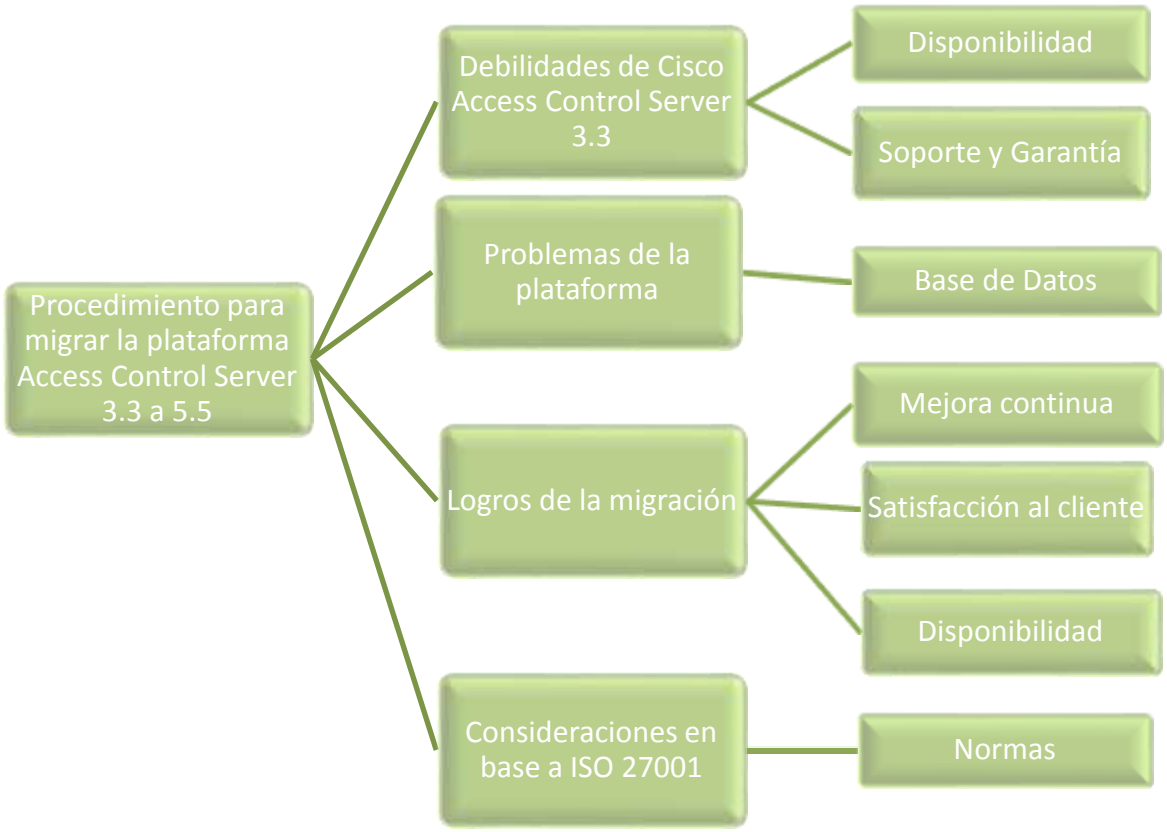

Figura 5. Diagrama de las variables

Tabla 5. Variable

VARIABLE INDEPENDIENTE	DEFINICION		DIMENSIONES	INDICADORES	ITEMS	UNIDAD
	Conceptual	Operacional				
Debilidades de Cisco Access Control Server 3.3.	Las debilidades en las plataformas son un decaimiento que expone la seguridad del mismo.	La disponibilidad de la información puede ser en una debilidad grave para la empresa.	Disponibilidad de la información.	Redundancia.	¿Por qué no se cuenta con redundancia de la plataforma? ¿Por qué razón se considera necesario una redundancia en la migración?	Abiertas
Problemas de la plataforma.	Los problemas de la plataforma son aquellos que impiden su estabilidad.	Los problemas se basarán en la base de datos local de la plataforma.	Base de Datos.	Adición, Edición y eliminación de usuarios.	¿Cuáles son los problemas al adicionar, editar o eliminar un usuario o equipo?	Base de Datos

				Estabilidad.	¿Cómo afecta la estabilidad de la plataforma a estos problemas con la base de datos?	Base de Datos
Logros de la migración	Los logros de una migración son aquellos que producen resultados satisfactorios.	La migración podrá lograr mejoras.	Mejora continua.	Versión nueva	¿Podrá mejorar los problemas en la base de datos, la migración a una versión nueva?	Abiertas
			Satisfacción al cliente	Preferencia	¿Cómo podrán sentirse satisfechos los clientes?	Abiertas
			Disponibilidad	Redundancia	¿Podrá la migración y la redundancia de la plataforma a lograr mayor disponibilidad?	Abiertas

Consideraciones en base a ISO 27001	Las consideraciones en base a ISO 27001 son los pasos que se deben seguir para ser implementados.	Realizar la migración siguiendo las normas necesarias	Normas	Políticas	¿Qué políticas aplican para la migración ?	Abiertas
				Control de cambios	¿Cuáles son los procedimientos para el control de cambios con respecto a la migración ?	Abiertas
				Accesos Remotos	¿Existirá algún cambio en la forma de autenticación de los usuarios?	Abiertas
VARIABLE DEPENDIENTE	**DEFINICION**		**DIMENSONES**	**INDICADORES**	**ITEMS**	UNIDAD
	Definición	**Operacional**				
Migrar la plataforma Access Control Server 3.3 a 5.5.	Es sustituir una plataforma por otra, ya sea, pasando de una	Es buscar la mejora continua de los procesos de acceso a la red mediante la aplicación de	Mejora	Financieros	¿Qué tan importante es para la empresa invertir en la segurida	Abiertas

	versión menor a una mayor o viceversa.	normas de seguridad para beneficio de la organización.	continua		d de la informaci ón?	
				Continuidad	¿Con qué frecuenci a se expone la continuid ad del negocio por fallas en la plataform a? ¿Qué grado de importan cia tienen esas fallas? ¿Cómo afecta la estabilida d de la plataform a?	Abiertas
			Normas de seguridad	Aplicación de las normas	¿Qué medidas se toman para aplicar las normas?	Abiertas

				Requisitos técnicos en procesos	¿Cómo se verifica que los procesos cumplan los requisitos técnicos de seguridad? ¿Existen métodos a seguir?	Abiertas

3.2 ENFOQUE Y MÉTODOS

El enfoque utilizado es el cualitativo, ya que se requiere estabilidad en el Cisco Access Control Server, recopilando información de documentos importantes, así como, la recolección de buenas prácticas en base a ISO 27001, realizando métodos de investigación en Tigo Business, aplicando entrevistas. Este método lo definen Sampieri, Collado y Lucio (2010) como el que "Utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación." (p. 7) De igual forma, se hará un análisis de la base de datos, con el objetivo de dar respuesta a las preguntas de esta investigación.

3.3 DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación es no experimental, transversal ya que solo se aplican: la recolección de datos y su análisis respectivo, sin formulación de hipótesis debido a la naturaleza de este estudio, con el fin de llegar a los resultados fijados en un tiempo único. Según Sampieri, Collado y Lucio, lo definen como "la recolección de datos en un solo momento, en un tiempo único. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado." (Hernandez Sampieri et al., 2010, p. 151)

3.3.1 POBLACIÓN

La población de la investigación estará limitada a empleados de Operaciones Técnicas de Tigo Business Tegucigalpa, que está constituido de la siguiente manera:

- Un Gerente de Operaciones Técnicas.
- Un Jefe de Instalaciones y Mantenimiento.
- Un Supervisor de Mantenimiento.
- Cinco Técnicos de Instalaciones.
- Seis Técnicos de Mantenimiento.
- Un Jefe de TSC (Technical Support Center).
- Un Supervisor de TSC.
- Un Técnico Especialista de TSC.
- Doce Técnicos de TSC.

- Un Administrador de Red de Producción.
- Un Analista de Calidad de Red.
- Un Especialista de Plataformas de Producción.

3.3.2 MUESTRA

La muestra es no probabilística, la cual toma un subgrupo de la población que se ha definido en la investigación y que tiene la misma oportunidad para ser seleccionados (Hernandez Sampieri et al., 2010) la cual se tomará de la siguiente manera:

- Entrevistas:
  - U n participante del área gerencial
  - Dos de la parte de Administración de la red de producción
  - Dos participantes de área de TSC (Technical Support Center)

- Análisis de base de datos:

  Se hará un análisis mensual de las fallas por adición, edición y eliminación de usuarios y equipos que están en la plataforma ACS 3.3.

3.4 TÉCNICAS E INSTRUMENTOS APLICADOS

En esta sección se aplicaron técnicas cualitativas de recolección de datos, “ocurre en ambientes naturales, y cotidianos de los participantes o unidades de análisis.” (Hernandez Sampieri et al., 2010)

3.4.1 TÉCNICAS E INSTRUMENTOS

Los instrumentos son aquellos implementadas para poder obtener la información necesaria para la investigación, las utilizadas en este estudio son:

- Entrevista

  La entrevista constó de preguntas abiertas, con el objetivo de recolectar la mayor cantidad de información para lograr la migración de la plataforma de manera estable, los instrumentos se dividieron de la siguiente manera:
  - Una entrevista para el área gerencial. (Ver Anexos 5)

- Dos entrevistas para el departamento de Red de Producción. (Ver Anexos 1 y 2)
- Dos entrevistas para el TSC. (Ver Anexos 3 y 4)

- Documentos

  Este instrumento se basa en revisar las normas y buenas prácticas que deben seguirse para migrar la plataforma ACS sin causar riesgos en Tigo Business.

3.4.2 PROCEDIMIENTOS

- Se elaboraron las preguntas abiertas para la entrevista en las áreas de la Red de Producción, de Gerencia y del Technical Support Center.
- Estas se elaboraron con respecto a las variables.
- Se hicieron las entrevistas y se recolectó la información.
- Se hizo un análisis de procedimientos para migración.
- Se recolectó la información necesaria para respaldar los problemas encontrados.
- Se realizó un análisis de la base de datos, de acuerdo a las fallas de equipos y usuarios en la plataforma.

3.5 FUENTES DE INFORMACIÓN

3.5.1 FUENTES PRIMARIAS

La fuente de información primaria se obtuvo de entrevistas y del análisis de la base de datos, así mismo, de las lecturas técnicas, manuales de Cisco para migración de ACS, políticas y normas ISO 27001.

3.5.2 FUENTES SECUNDARIAS

Las fuentes de información secundarias fueron de lecturas técnicas, artículos de Cisco y libros.

3.5.3 LIMITANTES DEL ESTUDIO

La principal limitante es la disponibilidad del personal para poder ser entrevistado y poder completar la información para el estudio, ya que se deseaba entrevistar a 8 y solo se pudo entrevistar a 5.

CAPITULO IV. RESULTADOS Y ANÁLISIS

En este capítulo se dan a conocer los resultados obtenidos de la investigación, por medio del uso de herramientas de recolección de datos para los procedimientos de la migración.

4.1. RESULTADO DE LAS ENTREVISTAS:

A continuación los resultados de las entrevistas realizadas:

- En base a las debilidades:
  - No se cuenta con redundancia en la plataforma porque en su tiempo no se estipuló la necesidad de implementar una, sin embargo, es necesario.

  - La red de Tigo Business, cuenta en su mayoría con redundancia, de modo, que si hay alguna afectación de tráfico, esta se migra por otra ruta redundante, evitando que exista tal afectación en mayor grado, así se hacen las revisiones y el monitoreo respectivo para estabilizar la caída, así mismo, la redundancia de una plataforma actuaría de la misma manera, dando ventajas de estabilizarla mientras existe una redundante tomando el rol de la primaria.

- En base a los problemas:
  - Los problemas al adicionar, editar y eliminar un usuario y equipos es que no se guardan los cambios al momento de ejecutar la acción.

  - Con estas fallas la plataforma se ve afectada en el sentido de no contar a tiempo con el acceso a un equipo o de un usuario que expiró por el período estipulado y desea ser dado de alta nuevamente y la plataforma no realiza el cambio, esto hace que no se cuente con el usuario habilitado en el tiempo deseado.

❖ En base a los logros:

- Seguridad que los problemas presentados en la agregación, edición y eliminación de usuarios y equipos mejorara con la migración y que en caso de no mejorar se podrá contar con soporte y garantía en la nueva versión para poder resolverlos si estos se vuelven a presentar.

- Los clientes se sentirán satisfechos por el tiempo de respuesta efectivo y estabilidad en el servicio.

- Se cree que la migración de la plataforma a una nueva versión evitará problemas de disponibilidad, así mismo, implementar la redundancia de la plataforma proporcionará un mayor nivel de disponibilidad, ya que al momento de perder gestión en una plataforma, quedará activa la plataforma redundante, hasta que la principal sea restablecida.

❖ En base a las consideraciones de ISO 27001:

- Las políticas que aplican para la migración son la de obsolescencia y política de control de cambios.

- La forma de autenticación de los usuarios será la misma, no deberá existir cambio alguno después de la migración, sin embargo, al momento de ejecutar la ventana de migración de la plataforma lo usuarios deberán autenticar a los equipos en red de forma local, ya que la plataforma estará sin gestión durante el tiempo estipulado en la ventana.

- Los procedimientos que sigue el comité de control de cambios son:
  - Recibir el SMOP en el formato de Tigo Business solicitando la ejecución del cambio propuesto.
  - Se analizan los objetivos y el alcance del cambio.
  - Se incluyen diagramas iniciales, si aplican.
  - Tiempo de afectación que tendrá el cambio.

- Se verifica el impacto del proyecto.
- Requerimientos para la ejecución.
- Se evalúa el procedimiento a realizar.
- Se detalla el cronograma de actividades.
- Se analizan las pruebas para probar que todo quede estable.
- Y se exige un procedimiento de rollback, de este modo, se evitan problemas si la ventana no ejecuta según lo esperado.
- Se incluyen diagramas finales, si aplican.
- Se verifica el funcionamiento con o sin rollback.

❖ En base a la mejora continua:

- La importancia de invertir en seguridad para Tigo Business es vital para poder brindar a sus clientes satisfacción y confianza en sus servicios, de modo que, es una inversión no un gasto como lo ven otras empresas y es por eso que se cuenta con normas y estándares que certifican sus procesos.
- La frecuencia con la que se expone la continuidad del negocio por fallas en la plataforma en su totalidad ha sido menor que la frecuencia con la que fallan los problemas pequeños en los usuarios y equipos.
- El grado de importancia de fallas por usuarios y equipos en la agregación, edición y eliminación de los mismos es media ya que no afecta en la totalidad pero si afecta en la disponibilidad y cada segundo de gran importancia en una compañía de telecomunicaciones.
- La medida actual para cumplir con la norma es tener que eliminar por completo el equipo y darle de alta nuevamente para que los cambios se vean reflejados, así mismo, un usuario.
- La forma en la que se verifican los procesos, es mediante un comité de control de cambios, el cual está capacitado para determinar los requisitos de seguridad necesarios para ser ejecutados, en base a normas y políticas de la empresa.

4.2. ANÁLISIS DE LA BASE DE DATOS

Se realizó un análisis en la base de datos, para determinar las fallas por adición, edición y eliminación de usuarios y equipos al mes:

Tabla 6. Análisis de Base de Datos

Usuarios /Equipo	Fallas por adición mensual	Fallas por edición mensual	Fallas por eliminación mensual	Total de equipos/usuarios en red
Usuarios	13	25	8	116
Equipos	38	280	115	1013

A continuación se muestra el porcentaje mensual de las fallas en la plataforma Cisco Secure Access Control Server 3.3 por usuarios, según el análisis de la base de datos interna de la misma, mostrando un 40% del total de fallas mensuales:

Figura 6. Fallas mensuales de usuarios.

Así mismo, se muestra el porcentaje mensual de las fallas en la plataforma Cisco Secure Access Control Server 3.3 por equipos, según el análisis de la base de datos interna de la misma, mostrando un 43% del total de fallas mensuales:

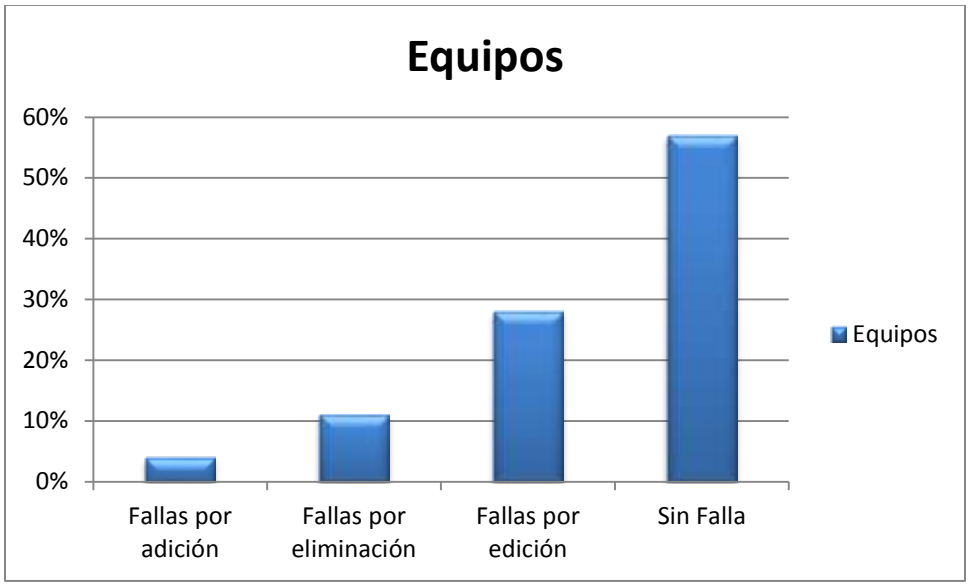

Figura 7. Fallas mensuales de equipos.

4.3. ANÁLISIS DE RIESGO

Se realizó un análisis de riesgo para determinar el valor del ACS, la tasación del activo se determinó en base a los estándares ISO 27001, especificando la afectación del producto/servicio por ausencia o degradación.

Para la evaluación de las amenazas se toma en cuenta que es un potencial para causar un incidente no deseado, los tipos de amenazas son:

- Desastres naturales (inundaciones, terremotos, huracanes, etc…)
- Humanos (falta de personal, error de mantenimiento, error de usuario)
- Tecnológico (fallas en el network, tráfico sobrecargado, fallas de hardware)
- Amenazas deliberadas.

En la evaluación de vulnerabilidades, se determina las siguientes:

- Ausencia del personal clave.
- Línea de cableado desprotegido.
- Ausencia de conciencia de seguridad.
- Política no clara de contraseñas.

- Falta de entrenamiento de seguridad.

La escala tomada en cuenta para la evaluación de riesgos, amenazas, vulnerabilidades e impacto de riesgo es:

- Muy Bajo: 1
- Bajo: 2
- Medio: 3
- Alto: 4
- Muy Alto:5

De acuerdo al resultado de la matriz de riesgo muestra los siguientes valores:

- Alto Riesgo: 12-16
- Medio Riesgo: 8-9
- Bajo Riesgo: 1-6

Por lo tanto, de acuerdo a la Matriz realizada para valoración del ACS, se puedo observar que tener equipos obsoletos presenta un riesgo alto, así como las ocurrencias en la base de datos, faltas de capacitaciones a los empleados, es por eso que migrar a una nueva versión evitaría un alto riegos de ocurrencias que afecten la imagen e impactos de servicio en Tigo Business.

Tabla 7. Matriz Análisis de Riesgo

Activos	Confindencialidad	Integridad	Disponibilidad	Propietario	Amenazas	Probabilidad	Vulnerabilidades	Posibilidad que amenazas exploten vulnerabilidades	Impacto del riesgo	P/ Ocurrencia Amenaza	Riesgo
ACS	4	3	4	ARP	Uso no autorizado de contraseña	1	Falta cumplimiento política seguridad	2	2	3	6
							Falta de claridad de las políticas de contraseñas	3	2	2	4
							Sin entrenamiento de la política	1	2	1	2
					Daño de Software /hardware	1	Cambios bruscos de voltaje	1	4	2	8
							Falta de Mantenimiento	3	3	4	12
							Obsolecencia	2	3	5	15
					Error Humano	1	Falta de Capacitacion	1	2	2	4
							Incorrecta asignación de accesos	1	3	1	3
							Carga laboral	3	3	2	6
					Perdida de Conexión	3	Falla de hardware	2	4	2	8
							Falla de energia	1	2	1	2
							Problemas de red de produccion	3	2	3	6
					Base de Datos	2	Corrupción	1	2	1	2
							Inestabilidad	3	4	3	12
							Fallas de conexión	2	3	4	12

4.4. ANÁLISIS FODA

Este análisis FODA se realizó con el objetivo de comprender las mejoras para el proceso de migración y los puntos actuales de Tigo Business:

4.4.1. FORTALEZAS

En la investigación realizada, se encontraron las fortalezas de la empresa para llevar a cabo el procedimiento de la migración de la plataforma Cisco Secure Access Control Server 3.3 a una nueva versión:

- El personal técnico de Tigo Business, del área de operaciones técnica, es capaz de analizar los procedimientos para una migración de plataforma por medio de un comité de control de cambios.
- Se siguen normas y políticas.
- Existen procedimientos de aprobaciones de cambios en la red, que asegura la disponibilidad, confiabilidad e integridad.
- El personal de operaciones técnicas está consciente de la necesidad de migrar la plataforma a una nueva versión que cuente con soporte y garantía en un ambiente redundante.

4.4.2. OPORTUNIDADES

Las oportunidades son las que ayudarán al cumplimiento del procedimiento para la migración y sus necesidades:

- Se sigue la norma ISO 27001:2005 para la seguridad de información.
- Se cuenta con políticas para cambios en la red y para equipos con obsolescencia.
- Se podrá contar con soporte y garantía para problemas futuros en la plataforma.
- Existe personal técnico con conocimiento de redes para realizar el procedimiento de migración.
- Se cuenta con proveedores en el país para la migración.

4.4.3. DEBILIDADES

Las debilidades y limitantes que se encontraron en la empresa Tigo Business son:

- Falta de acciones rápidas para solución de los problemas en la plataforma.
- Falta de personal en el área de administración de redes.

4.4.4. AMENAZAS

Las amenazas, que son la problemática para poder llevar a cabo el procedimiento de la migración de la plataforma son:

- Disponibilidad del personal para ejecutar el procedimiento de migración a una versión actual de la plataforma.
- Comité de control de cambios en desacuerdo para realizar la migración.
- Problemas en la ejecución del procedimiento y hacer rollback para evitar exceder el tiempo establecido para la ventana.

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.5 CONCLUSIONES

- Se determinaron las debilidades en plataforma Cisco Secure Access Control Server 3.3, siendo estas: Las fallas al agregar, editar y eliminar usuarios y equipos, así mismo, la falta de soporte y garantía en la misma, debido a que está fuera del mercado, siendo una plataforma obsoleta que al presentar fallas, no contaría con la ayuda de Cisco para atenderlas.
- Los problemas que se solucionarían en la migración de la plataforma ACS 3.3 a la 5.5, sería la inestabilidad y disponibilidad de los equipos y usuarios para resolver los problemas en la red, contando con redundancia en la plataforma y lograr mayor disponibilidad cuando esta se vea afectada por una caída.
- Los logros que se obtendrían con la migración de la plataforma 3.3 a la 5.5 en un ambiente de redundancia, es disponibilidad en caídas de la plataforma principal, quedando activa la secundaria o redundante para evitar que los usuarios entre de manera local a los equipos, sino que siempre, por medio de la autenticación por el ACS, disminución total de fallas por adición, edición y eliminación de usuarios y equipos.
- Las consideraciones que se toman en cuenta al momento de migrar la plataforma con respecto a la certificación ISO 27001, son llevadas a cabo por medio de un comité de control de cambios, que son los encargados de revisar por medio de un SMOP los procedimientos que se ejecutarán en la migración, rechazando o aprobando dicho procedimiento.

5.6 RECOMENDACIONES

- Tomar acciones de forma inmediata al momento de tener problemas que afecten la disponibilidad de la información.
- Migrar a versiones recientes las plataformas, con el fin de contar siempre con soporte y garantía para evitar problemas a futuro.
- Evitar la obsolescencia de plataformas que ayudan a la continuidad del negocio.
- Contar con capacitación de plataformas para el personal encargado de las mismas.

- Mayor disponibilidad del personal para ejecución del procedimiento de migración de la plataforma.
- Tomar en cuenta las sugerencias del comité con respecto al procedimiento, para realizar correcciones de forma que, no se pueda atrasar el proyecto y lograr de manera exitosa la migración.
- Si se muestran problemas en la ejecución del procedimiento y se debe hacer rollback, tomar nota de los errores para repogramar el proyecto, evitándolos en la futura ventana de mantenimiento.
- Colocar los Cisco Secure ACSs en lugares físicos diferentes, el primario en un nodo y el redundante en otro nodo, de este modo, se sigue la norma de continuidad de negocios.

CAPITULO VI. APLICABILIDAD

6.1 PROCEDIMIENTO PARA EFECTUAR LA MIGRACIÓN DE LA PLATAFORMA CISCO SECURE ACS 3.3 A LA 5.5 EN TIGO BUSINESS, TEGUCIGALPA.

6.2 INTRODUCCIÓN

En este capítulo se detalla el procedimiento para la migración de la plataforma Cisco Secure Access Control Server 3.3 a la versión 5.5 en Tigo Business, Tegucigalpa. De la investigación realizada en Tigo, se pudo obtener las normas y políticas que influyen en el procedimiento, determinando de esta manera la necesidad de efectuar la migración, así como, el grado de conocimiento del personal encargado de implementaciones y mantenimientos.

El plan de acción que se presenta a continuación, se enfoca en el procedimiento que se debe seguir en Tigo Business, para efectuar la migración de la plataforma Cisco Secure ACS a una nueva versión, en base a sus requerimientos. El objetivo principal es poder brindar un procedimiento a seguir, en base a las mejores prácticas de políticas y normas que son partes de la institución, de manera, que se pueda prever cualquier rechazo del procedimiento por el Comité de Control de Cambios.

De igual manera, se detalla el cronograma de ejecución, desde la instalación física de los equipos, las pruebas de funcionamiento y el procedimiento de rollback, en caso de que este aplique. Se incluye también, el presupuesto de la migración.

6.3 DESCRIPCIÓN DEL PLAN DE ACCIÓN

El plan de acción será de la siguiente manera:

Se realizará el SMOP solicitado por el Comité de Control de cambios, el cual debe ir los requerimientos necesarios en base a normas ISO 27:0001 para poder ser revisado en reunión y poder ser aprobado o rechazado, en el caso de ser rechazado se informa en una minuta las observaciones y se pueden tomar acciones para corregir y volver a ser enviado el SMOP para nueva aprobación.

El SMOP debe contener:

a. Se definirán el objetivo General y los objetivos específicos.

Objetivo General:

- Realizar la migración de la plataforma Cisco Secure ACS 3.3 a la 5.5 en un ambiente de redundancia, en Tigo Business, Tegucigalpa.

Objetivos Específicos:

- Describir la solución y los procesos de la migración.
- Documentar las configuraciones básicas de los equipos Cisco 1121.
- Integrar las plataformas ACS 5.5.
- Proceso de configuración.

b. Calendarización de proyecto

Fecha propuesta: 26, 27 y 28 de Enero

Hora propuesta: 22:00 Horas

Se consideran estas fechas debido a que la red se congela en la época de Diciembre y primera semana de Enero, de igual forma, se envía el SMOP en la segunda semana, el 14 de Enero, ya que el Comité se reúne todos los miércoles de manera semanal y si se necesitan realizar cambios se realizan en esa misma semana y se revisa el próximo miércoles, y no se ve afectada la fecha de ejecución de la migración.

La hora debe ser a las 22 horas o después, debido a la afectación de autenticación de usuarios a los equipos, es por eso que se considera esa hora.

c. Impacto del proyecto

El impacto que puede ocasionar la puesta en marcha de los nuevos ACSs, primario y el redundante, es una afectación de la autenticación de las sesiones

administrativas de los equipos de la red. El usuario podría tener problemas de autenticación o la limitación para la ejecución de comandos en equipos.

En caso de suceder lo mencionado anteriormente, el usuario podrá entrar de manera local a los equipos.

d. Responsables del proyecto

Será el Jefe de Administración de la Red de Producción y como personal involucrado, el Especialista de Plataformas de Producción.

e. Requerimientos para la ejecución:

Físicos:

- Espacio físico en racks para la instalación de los equipos, el principal deberá ir en un nodo diferente al redundante.
- El Nodo donde se instalarán los equipos, debe contar con las condiciones ambientales especificas por el fabricante.
- Se debe proporcionar alimentación eléctrica a los equipos, así como, protección ante interrupciones del servicio eléctrico o de variaciones del voltaje.
- Finalmente, brindar una conexión de red para el equipo primario y el redundante.

Red:

- Los equipos deben contar con una dirección IP estática única para cada uno.
- Todos los equipos de Tigo Business, deberán tener acceso a los equipos ACS en el protocolo que se designe por el Administrador de la Red de Producción.
- Se debe contar con acceso administrativo a todos los equipos en red con privilegio de administrador para poder efectuar los cambios en equipos.

f. Procedimiento:

- Verificación por parte del personal técnico, la capacidad de carga de los nodos a los cuales irán los ACSs.
- Instalación física de los equipos ACS 1121 Primario.

- Instalación física de los equipos ACS 1121 Redundante.
- Verificación de funcionamiento del ACS primario.
- Verificación de la integración del equipo.
- Aplicación de la plantilla de configuración en uno de los equipos de la red (un equipo que no esté en producción).
- Verificación del funcionamiento del equipo de red con los nuevos equipos ACS.
- Aplicación de la plantilla en los equipos de la red y seleccionar una cantidad de 30 equipos para realizar pruebas.
- Verificar el funcionamiento de los equipos seleccionados.
- Configuración básica de Equipo ACs:
    - Al encender los servidores de autenticación Cisco ACS 1121 no cuenta con la configuración inicial. Por lo tanto, será necesario inicializar los servidores con la configuración básica. Existen dos maneras, una es por el puerto de consola o al conectar un teclado y monitor.
    - Se asigna la dirección IP, la información del Gateway, servidores DNS, información de dominio, y la cuenta de usuario administrativo para loguearse por consola.
    - El último paso para inicializar la configuración es instalar la licencia del servidor, es necesaria una conexión HTTPS con el fin de accesar la interfaz GUI y realizar la instalación, el usuario y contraseña por defecto, se encuentran en el manual de Cisco.
    - El ACS redundante, debe ser activado de la misma manera que el primario, y al momento de finalizar, se debe registrar como servidor secundario, en la sección System Administration > Operations > Local Operations > Deployment Operations completando los campos y haciendo referencia al ACS primario, como se muestra en la siguiente figura.

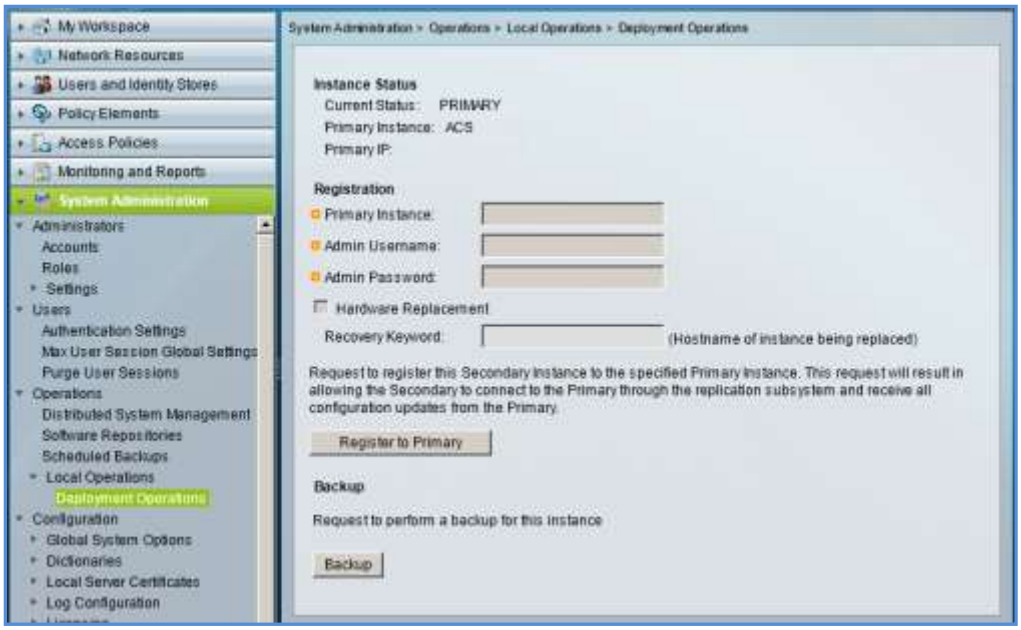

Figura 8. Interfaz Gráfica del ACS sección Deployment Operations.

- Después se debe ingresar al ACS primario y colocar el ACS redundante, como secundario.

➢ Configuración del cliente AAA:

El servidor ACS, solo responde a peticiones de clientes que se encuentren en su base de datos, por lo cual es necesario configurar cada cliente de AAA en el ACS. Para adicionar un cliente se va a la sección de configuración Network Resources > Network Devices and AAA Clients.

En la sección de configuración se debe asignar un nombre único al dispositivo, configurar la dirección IP y seleccionar los protocolos de autenticación a utilizar así como su clave compartida respectiva.

➢ Configuración de usuarios en la base de datos interna:

El ACS cuenta con una base interna de usuarios que puede ser utilizada como base principal o de respaldo en caso de fallo de comunicación con una base de usuarios externa. Para crear un usuario en la base de usuarios interna se va a la

sección de configuración Users and Identity Stores > Internal Identity Stores > Users y se hace click sobre el botón “Create”.

Se debe asignar un nombre único al usuario, es recomendable agregar una descripción con el nombre real del usuario y finalmente se configura la contraseña correspondiente. Opcionalmente se pueden crear grupos, para asignar a los usuarios a diferentes grupos y crear diferentes políticas de acceso.

- Plantilla de configuración para equipos Cisco:
  - Configuración de los nuevos ACS:

    R1X(config)#tacacs-server host (IP del ACS Primario) single-connection key 0 xxxxxx.

    R1X(config)#tacacs-server host (IP del ACS Redundante) single-connection key 0 xxxxxx.

  - Verificación del funcionamiento de los nuevos ACS:

    R1(config)#aaa group server tacacs+ prueba1

    R1(config-sg-tacacs+)#server (IP del ACS primario)

    R1(config)#aaa group server tacacs+ prueba2

    R1(config-sg-tacacs+)#server (IP del ACS redundante)

    R1#test aaa group prueba1 usuario clave legacy

    R1#test aaa group prueba2 usuario clave legacy

    Con esos comandos se mostrará si la prueba es exitosa o fallida.

  - Remoción del ACS 3.3 y comandos de prueba:

    R1(config)#no aaa group server tacacs+ prueba1

    R1(config)#no aaa group server tacacs+ prueba2

    R1(config)#no tacacs-server host (IP ACS 3.3)

g. Pruebas:

Aquí se detallan las pruebas de verificación de funcionamiento de la migración:

- Verificar que el equipo enciende y bootea normalmente.
- Verificación del acceso por medio de las sesiones de SSH y HTTPS.
- Verificación de la versión del software de ACS.
- Verificación de los roles primario y secundario de cada servidor.

h. Procedimiento del rollback:

Se incluye este procedimiento, en caso de fallar la migración, el cual consiste en eliminar la configuración de los equipos de red, los nuevos ACS 5.5 primario y redundante, dejando únicamente el ACS 3.3.

i. Verificación del funcionamiento de los ACSs

- Verificar que se puede autenticar las sesiones administrativas de los equipos de red utilizando los usuarios y contraseñas correspondientes.
- Verificar la redundancia a nivel de servidores ACS.
- Verificar el acceso a los equipos desde el puerto de consola.

6.4 CRONOGRAMA DE EJECUCIÓN

Tabla 8. Cronograma del procedimiento de migración

	Nombre	*Duración*	*Inicio*	*Terminado*	*Predecesores*
1	Elaboración de SMOP	2 días	05/01/2015	06/01/2015	
2	Revisión de SMOP en Comité de Control de Cambios	1 día	07/01/2015	07/01/2015	1
3	Verificación de energía en Nodos	1 día	09/01/2015	09/01/2015	2
4	Instalación física del equipo primario	1 día	26/01/2015	26/01/2015	3
5	Instalación física del equipo redundante	1 día	26/01/2015	26/01/2015	3
6	Encendido del equipo primario	1 día	26/01/2015	26/01/2015	4
7	Pruebas de verificación del funcionamiento del ACS 1121 primario.	1 día	26/01/2015	26/01/2015	6
8	Aplicación de la plantilla de configuración en uno de los equipos de la red	1 día	26/01/2015	26/01/2015	7
9	Verificación del funcionamiento del equipo con el Nuevo ACS.	1 día	26/01/2015	26/01/2015	8
10	Rollback (si aplica)	1 día	26/01/2015	26/01/2015	9
11	Encendido del equipo redundante	1 día	27/01/2015	27/01/2015	5
12	Pruebas de verificación del funcionamiento del ACS 1121 redundante	1 día	27/01/2015	27/01/2015	11
13	Pruebas de verificación de la integración del ACS redundante con los equipos de red	1 día	27/01/2015	27/01/2015	12
14	Rollback (si aplica)	1 día	27/01/2015	27/01/2015	13

15	Aplicación de la plantilla de configuración en los equipos de la red.	13 días	28/01/2015	13/02/2015	9;13
16	Verificación del funcionamiento de los equipos con los ACSs.	13 días	28/01/2015	13/02/2015	15
17	Remover ACS 3.3	1 día	16/02/2015	16/02/2015	16
18	Pruebas	1 día	16/02/2015	16/02/2015	16
19	Verificación del funcionamiento del ACS primario y del ACS redundante.	1 día	16/02/2015	16/02/2015	18

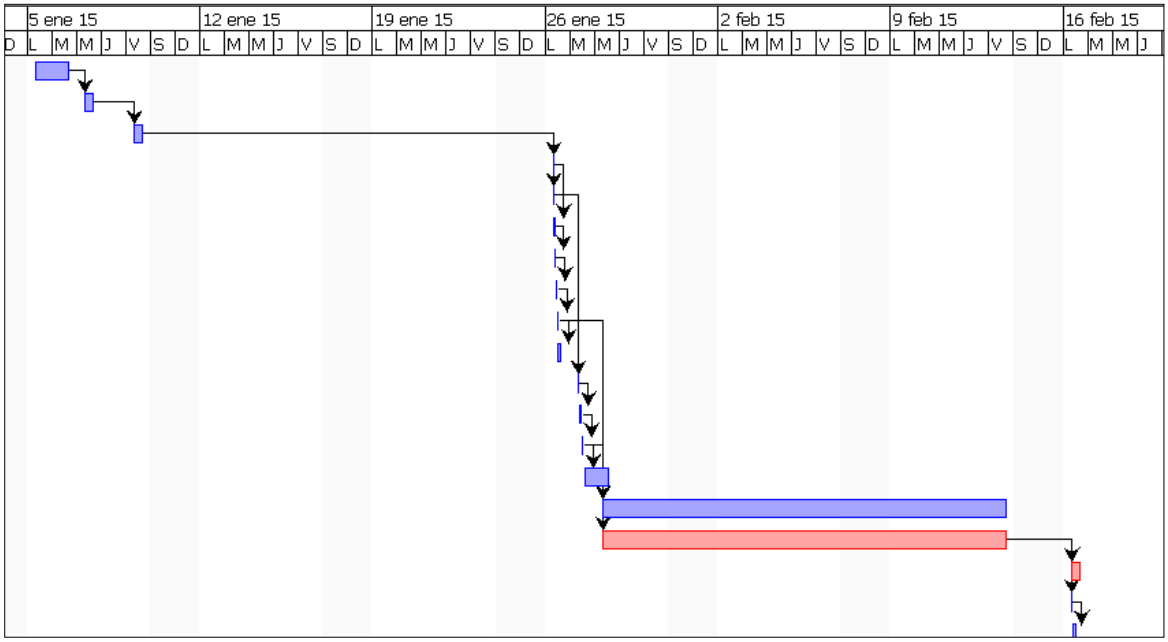

Figura 9 . Cronograma del procedimiento de migración

6.5 PRESUPUESTO

Tabla 9. Presupuesto

Descripción	Cantidad	Costo Unitario	Total
Ac power cord (north america), c13, nema 5-15p, 2.1m	2	$ 0.00	$ 0.00
Acs 1121 appliance with 5.x sw and base license	2	$ 9,926.24	$ 19,852.48
Shared supp 24x7x2 acs 1121 appliance with 5.5	2	$ 5,027.47	$ 10,054.94
Capacitation	1	$ 4,800.00	$ 4,800.00
Garantía de equipos	----	----	$ 10,054.94
Materiales de instalación	----	----	$ 1,000.00
Servicio de configuración e implementación	----	----	$13,756.87
TOTAL			$ 59,519.23

BIBLIOGRAFÍA

1 Alexander, A. G. (2005). Formación de auditores internos en sistemas de gestión de seguridad de información ISO 27001:2005.

2 Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información*. Alfaomega.

3 Atelin, P., & Dordoigne, J. (2007). *TCP/IP y protocolos de Internet*. Ediciones ENI.

4 Balado, E. S. (2005). *Estrategia para la implantación de nuevas tecnologías en PYMES: obtenga el máximo rendimiento aplicando las TIC en el ámbito empresarial*. Ideaspropias Editorial S.L.

5 Cabello, M. V. N. (2010). *Introduccion a Las Bases de Datos Relacionales*. Editorial Visión Libros.

6 Chick, D. (2011). *Todo lo que los administradores de red saber*. Douglas Chick.

7 Cisco. Un campus virtual inalámbrico al servicio de la comunidad académica (2002). Recuperado a partir de https://www.cisco.com/web/ES/publicaciones/02-10-Cisco-universidad-granada.pdf

8 Cisco. IAE (2004). Recuperado a partir de http://www.cisco.com/web/LA/docs/pdf/caso_exito_IAE.pdf

9 Cisco. (2014a). Oficinas Locales - Acerca de Cisco - Cisco Systems. Recuperado 11 de diciembre de 2014, a partir de http://www.cisco.com/web/LA/cisco/contactenos/oficinas/index.html

10 Cisco. (2014b, agosto 3). Cisco Secure Access Control Server for Windows - Products & Services. Recuperado 3 de agosto de 2014, a partir de http://cisco.com/c/en/us/products/security/secure-access-control-server-windows/index.html

11 Cisco. (s. f.-a). Migration Guide for Cisco Secure Access Control System 5.5 - Feature Comparision of ACS 3.x and 4.x with ACS 5.5 [Cisco Secure Access Control System 5.5]. Recuperado 11 de noviembre de 2014, a partir de http://cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-5/migration/guide/migration_guide/Appendix_C_Feature_Compare.html

12 Cisco. (s. f.-b). Noticias de Cisco para América Latina. Recuperado 11 de diciembre de 2014, a partir de http://newsroom.cisco.com/latamnetwork/

13 Cisco Secure Access Control Server Deployment Guide - prod_white_paper0900aecd80737943.pdf. (s. f.). Recuperado a partir de http://www.cisco.com/c/dam/en/us/products/collateral/security/secure-access-control-server-windows/prod_white_paper0900aecd80737943.pdf

14 Cisco Secure Access Control Server for Windows - Products & Services. (s. f.-a). Recuperado 3 de agosto de 2014, a partir de http://cisco.com/c/en/us/products/security/secure-access-control-server-windows/index.html

15 Cisco Secure Access Control Server for Windows - Products & Services. (s. f.-b). Recuperado 3 de agosto de 2014, a partir de http://cisco.com/c/en/us/products/security/secure-access-control-server-windows/index.html

16 Com, J. W. N. (2007). *Network Dictionary*. Javvin Technologies Inc.

17 Date, C. J., & Faudón, S. L. M. R. (2001). *Introducción a los sistemas de bases de datos*. Pearson Educación.

18 Dooley, K., & Brown, I. (2007). *Cisco IOS Cookbook*. O'Reilly Media, Inc.

19 García, J. J. H. (2010). *Guía básica de BSD para usuarios de Windows*. Lulu.com.

20 Garreta, J. S. S. (2003). *Ingeniería de proyectos informáticos: actividades y procedimientos*. Universitat Jaume I.

21 Hernandez Sampieri, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación* (5.ª ed.). MACGRAW-HILL INTERAMERICANA EDITORES.

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

23 Laet, G. D., & Schauwers, G. (2005). *Network Security Fundamentals*. Cisco Press.

24 Laudon, K. C., & Laudon, J. P. (2008). *Sistemas de información gerencial: administración de la empresa digital* (Décima.). Pearson Educación.

25 López, P. A. (2010). *Seguridad informática*. Editex.

26 *Managing Cisco Network Security (Second Edition)*. (2002). Rockland, MA, USA: Syngress Publishing. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10007030

27 Migration Guide for Cisco Secure Access Control System 5.5 - ACS 5.5 Deployment Overview [Cisco Secure Access Control System 5.5]. (s. f.). Recuperado 11 de noviembre de 2014, a partir de http://cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-5/migration/guide/migration_guide/Migration_Deploy.html

28 Paquet, C. (2012). *Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide*. Cisco Press.

29 Pérez, F. M. (2008). *Administración de servicios de Internet: De la teoría a la práctica*. Universidad de Alicante.

30 ¿Qué es norma ISO 27001? | 27001Academy. (s. f.). Recuperado 8 de noviembre de 2014, a partir de http://www.iso27001standard.com/es/que-es-iso-27001/

31 RSA Token Server and SDI Protocol Usage for ASA and ACS. (s. f.). Recuperado 3 de agosto de 2014, a partir de http://cisco.com/c/en/us/support/docs/security-vpn/secureid-sdi/116304-technote-rsa-00.html

32 Santuka, V., Banga, P., & Carroll, B. J. (2010). *AAA Identity Management Security*. Pearson Education.

33 SEGOB. (2013). DOF - Diario Oficial de la Federación. Recuperado 11 de noviembre de 2014, a partir de http://dof.gob.mx/nota_detalle.php?codigo=5294185&fecha=02/04/2013

34 Stallings, W. (2004). *Fundamentos de seguridad en redes aplicaciones y estándares* (2.ª ed.). Pearson Educación.

35 Tanenbaum, A. S. (2003). *Redes de computadoras*. Pearson Educación.

36 Tigo. (2011, marzo). Proceso de Comité de Control de Cambios.

37 User Guide for Cisco Secure ACS for Windows Server Version 3.3 - System Configuration: Basic [Cisco Secure Access Control Server for Windows]. (s. f.). Recuperado 11 de agosto de 2014, a partir de http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/3.3/user/guide/sba.html

ANEXOS

ENTREVISTAS REALIZADAS A TIGO BUSINESS:

1) ÁREA DE RED DE PRODUCCIÓN

Fernando García, Administrador de la Red de Producción

a) **¿Cuáles son los problemas al adicionar, editar o eliminar un usuario o equipo?**
b) **¿Podrá mejorar los problemas de agregación, edición y eliminación de usuarios y equipos en la migración a una versión nueva?**
c) **¿Podrá la migración y la redundancia de la plataforma lograr mayor disponibilidad?**
d) **¿Qué políticas aplican para la migración?**
e) **¿Existirá algún cambio en la forma de autenticación de los usuarios?**

2) ÁREA DE RED DE PRODUCCIÓN

Said Mejia, Analista de calidad de Red

a) **¿Cuáles son los problemas al adicionar, editar o eliminar un usuario o equipo?**
b) **¿Podrá mejorar los problemas de agregación, edición y eliminación de usuarios y equipos en la migración a una versión nueva?**
c) **¿Podrá la migración y la redundancia de la plataforma lograr mayor disponibilidad?**
d) **¿Qué políticas aplican para la migración?**
e) **¿Existirá algún cambio en la forma de autenticación de los usuarios?**

3) ÁREA DE TSC

a) **¿Cuáles son los procedimientos para el control de cambios con respecto a la migración?**
b) **¿Con qué frecuencia se expone la continuidad del negocio por fallas en la plataforma?**
c) **¿Qué grado de importancia tienen esas fallas?**

d) **¿Cómo afecta la estabilidad de la plataforma?**
e) **¿Qué medidas se toman para aplicar las normas?**

4) ÁREA DE TSC

a) **¿Cuáles son los procedimientos para el control de cambios con respecto a la migración?**
b) **¿Con qué frecuencia se expone la continuidad del negocio por fallas en la plataforma?**
c) **¿Qué grado de importancia tienen esas fallas?**
d) **¿Cómo afecta la estabilidad de la plataforma?**
e) **¿Qué medidas se toman para aplicar las normas?**

5) ÁREA GERENCIAL

Danys Rivera, Gerente de Operaciones Técnicas

a) **¿Qué importancia tiene para la empresa invertir en la seguridad de la información?**
b) **¿Cómo se verifica que los procesos cumplan los requisitos técnicos de seguridad?**
c) **¿Existen métodos a seguir?**
d) **¿Por qué no se cuenta con redundancia de la plataforma?**
e) **¿Por qué razón se considera necesario una redundancia en la migración?**
f) **¿Cómo podrán sentirse satisfechos los clientes?**