VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: "MEJORAMIENTO DE UNA SOLUCIÓN DE CONTROL DE ACCESO, REMEDIACIÓN, PROFILING Y SERVICIOS AAA PARA LA RED DE DATOS DEL MINISTERIO DE FINANZAS, ORIENTADAS AL CUMPLIMIENTO DEL ACUERDO NO. 166 DEL ESQUEMA DE GESTIÓN GUBERNAMENTAL DE LA INFORMACIÓN"

AUTOR: ZURITA ROSERO, WLADIMIR CÉSAR

DIRECTOR: SALAZAR CHACÓN, GUSTAVO DAVID

SANGOLQUÍ

2017

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

MAESTRÍA EN GERENCIA DE SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "MEJORAMIENTO DE UNA SOLUCIÓN DE CONTROL DE ACCESO, REMEDIACIÓN, PROFILING Y SERVICIOS AAA PARA LA RED DE DATOS DEL MINISTERIO DE FINANZAS, ORIENTADAS AL CUMPLIMIENTO DEL ACUERDO NO. 166 DEL ESQUEMA DE GESTIÓN GUBERNAMENTAL DE LA INFORMACIÓN" realizado por el señor WLADIMIR CÉSAR ZURITA ROSERO, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditado y autorizar al señor WLADIMIR CÉSAR ZURITA ROSERO para que lo sustente públicamente.

Sangolquí, 15 de noviembre del 2017

GUSTAVO DAVID SALAZAR CHACÓN

DIRECTOR

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORÍA DE RESPONSABILIDAD

Yo, ***WLADIMIR CÉSAR ZURITA ROSERO***, con cédula de identidad N° 1713224739, declaro que este trabajo de titulación "MEJORAMIENTO DE UNA SOLUCIÓN DE CONTROL DE ACCESO, REMEDIACIÓN, PROFILING Y SERVICIOS AAA PARA LA RED DE DATOS DEL MINISTERIO DE FINANZAS, ORIENTADAS AL CUMPLIMIENTO DEL ACUERDO NO. 166 DEL ESQUEMA DE GESTIÓN GUBERNAMENTAL DE LA INFORMACIÓN" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 15 de noviembre del 2017

WLADIMIR CÉSAR ZURITA ROSERO

C.C. 1713224739

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, ***WLADIMIR CÉSAR ZURITA ROSERO***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"MEJORAMIENTO DE UNA SOLUCIÓN DE CONTROL DE ACCESO, REMEDIACIÓN, PROFILING Y SERVICIOS AAA PARA LA RED DE DATOS DEL MINISTERIO DE FINANZAS, ORIENTADAS AL CUMPLIMIENTO DEL ACUERDO NO. 166 DEL ESQUEMA DE GESTIÓN GUBERNAMENTAL DE LA INFORMACIÓN"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 15 de noviembre del 2017

WLADIMIR CÉSAR ZURITA ROSERO

C.C. 1713224739

DEDICATORIA

Dedico este trabajo, a Jehová que guía a los hombres en el camino de sabiduría, porque de su palabra proviene la inteligencia y el conocimiento.

A mi esposa Karina, por amarme y apoyarme siempre.

A mi hija Alejandrita, que con sus ocurrencias e inocencia me alienta a seguir adelante.

A mis padres César y Mariana por amarme, cuidarme y guiarme en los caminos de la humildad y el trabajo.

A los autores de libros de autoayuda de todo el mundo que, mediante sus experiencias y conocimientos, mejoran la calidad de vida de las personas.

WLADIMIR CÉSAR ZURITA ROSERO

AGRADECIMIENTO

Le doy las gracias a Jehová, por guiarme en los caminos del éxito y el triunfo, en Cristo Jesús que me fortalece.

Agradezco, a todos mis profesores de la Universidad de la Fuerzas Armadas ESPE, por toda su experiencia y conocimiento impartidos.

Expreso mi cordial gratitud, al Ing. Gustavo Salazar, tutor de este trabajo, por compartir su predispoción, conocimiento y motivación.

Al Ministerio de Finanzas por el apoyo y facilidades brindadas para la culminación de este trabajo de tesis.

A mi esposa Karina y a mi Hija Alejandrita, por ser parte de mi vida y por comprender que en muchos casos para alcanzar una meta se debe sacrificar el hermoso tiempo de pasar en familia.

WLADIMIR CÉSAR ZURITA ROSERO

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El proyecto de tesis propone mejorar la solución actual de Control de Acceso, Remediación, Profiling y servicios AAA "Authentication, Authorization and Accounting" del Ministerio de Finanzas, a efectos de optimizar la accesibilidad a la información de la red de datos, aplicando políticas de forma fiable y complementando la seguridad de la infraestructura. Además de recopilar información en tiempo real de los eventos que transcurre en la red de datos con los usuarios y dispositivos, para de esta manera oriente a los responsables de la seguridad informática a tomar decisiones proactivas mediante la ejecución de políticas. Mediante la mejora de la solución actual, el Ministerio de Finanzas podrá cumplir de manera eficiente los dominios, controles y controles de dominio que el EGSI *"Esquema Gubernamental de Seguridad de Información"* basado en la norma técnica INEN ISO/IEC 27002, que dispone se implementen en las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva emitido mediante el Acuerdo No. 166 del 19 de septiembre de 2013.

PALABRAS CLAVE

- **PROTOCOLO AAA: (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING).**
- **REMEDIATION: PROCESO PARA SEPARAR FINALES.**
- **PROFILING: CAPACIDAD DE DIRECCIONAR UN DISPOSITIVO EN FORMA AUTOMÁTICA A UN SEGMENTO DE RED.**

ABSTRACT

The thesis project proposes to improve the current Access Control, Remediation, Profiling and AAA services "Authentication, Authorization and Accounting" of the Ministry of Finance, in order to optimize the accessibility of information in the data network, applying policies of Reliable way and complementing the security of the infrastructure. In addition to collecting real-time information on the events that occur in the data network with users and devices, in order to guide IT decision makers to make proactive decisions through the implementation of policies. By improving the current solution, the Ministry of Finance will be able to efficiently fulfill the domains, controls and domain controls that the EGSI "Government Information Security Scheme" based on the technical standard INEN ISO/IEC 27002 that it has implemented In the entities of the Central and Institutional Public Administration and that depend on the Executive Function issued by Agreement No. 166 of September 19, 2013.

KEYWORDS

- **PROTOCOL AAA (AUTHENTICATION, AUTHORIZATION AND ACCOUNTING)**
- **REMEDIATION: PROCESS TO SEPARATE FINAL DEVICES**
- **PROFILING: ABILITY TO ROUTE A DEVICE AUTOMATICALLY TO A NETWORK SEGMENT.**

CAPÍTULO I

INTRODUCCIÓN

Mejoramiento de una *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"*, orientadas al cumplimiento del acuerdo No. 166 EGSI.

1.1 Ubicación

El trabajo de mejoramiento de la Solución de Control de acceso, Remediación, Profiling y Servicios AAA se efectuará en el edificio matriz del Ministerio de Finanzas del Ecuador, como se visualiza en la siguiente Figura.

Provincia: Pichincha

Ciudad: Quito

Ubicación: Avenida 10 de agosto y Bolivia

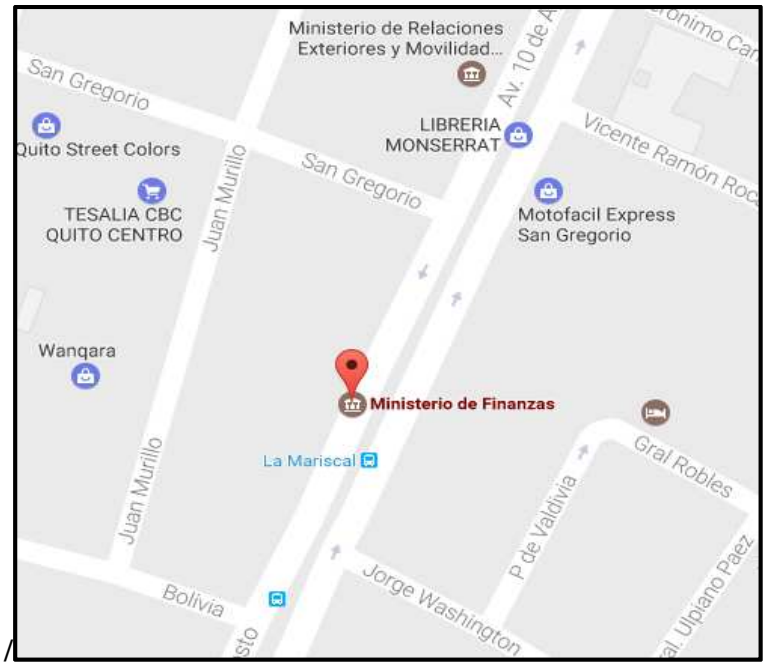


Figura 1 Ubicación Ministerio de Finanzas del Ecuador

Fuente: **(Google, s.f.)**

El Ministerio de Finanzas está ubicada en la ciudad de Quito, cantón Quito, como se indica en la siguiente Figura.

Figura 2 Ubicación en Quito

Fuente: **(Google, s.f.)**

1.2 Planteamiento del problema

La entidad del estado, denominada Ministerio de Finanzas del Ecuador, gestiona toda la información de las finanzas públicas del Ecuador. Actualmente esta institución cuenta con una red de datos parcialmente compleja debido a que su topología de datos provee el servicio de eSIGEF (Sistema de Gestión Financiera) a todas las instituciones del estado a nivel nacional.

Esta Cartera de Estado a fin de proteger la información que transita a nivel interno de la red, ha adquirido una solución de Control de acceso a la red denominada "Cisco ISE" [1]. La cual no ha sido correctamente explotado sus características en cuanto a salvaguardar la información.

Tampoco ha sido orientada al cumplimiento del Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública, se emitió el *"Esquema*

[1]**Cisco ISE:** Cisco Identity Services Engine (ISE) – Cisco.

Gubernamental de Seguridad de Información EGSI[2] basado en la ISO 27000" que dispone adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad de la información que se genera y custodia en diferentes medios y formatos en las entidades de la Administración Pública Central, y que dependen de la Función Ejecutiva.

Esta institución cuenta con varios despachos, subsecretarías, direcciones y oficinas en general, con puertos de datos inseguros, por tal motivo cualquier usuario interno o externo puede conectarse de manera física a un punto de datos libre y tener acceso a los segmentos de red institucionales, provocando una brecha de seguridad informática muy alta para esta Cartera de Estado. Por el motivo que la "Solución Cisco ISE - MINFIN" no se encuentra funcionando al 100%, con sus características de control de acceso a la red "NAC[3]" e identidades.

Esta Cartera de Estado posee un parque informático con sistemas operativos desde XP a Windows 10, Linux y Mac OS. Los cuales no cumplen los requisitos mínimos de actualizaciones, parches, antivirus y programas base institucionales para ingreso a la red de datos institucional.

Esta es una brecha de seguridad informática muy alta, debido a que computadoras infectadas con programas de escaneo de red y programas mal intencionados, pueden ingresar a la red datos y causar un daño masivo.

La característica de perfilamiento "Profiling[4]" está únicamente implementada para pocos usuarios del segmento de red VLAN 104 "mesa de ayuda" de esta Cartera de Estado.

Esta característica debe estar implementada en todos los segmentos de red de esta institución. Con el fin de que cada computador y dispositivos de red como, por

---

[2] **EGSI**: ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE INFORMACIÓN (EGSI) BASADO EN LA ISO 27000": ESTÁNDAR PARA LA SEGURIDAD DE LA

[3] **NAC**: NETWORK ACCESS CONTROL.

[4] **PROFILING**: ACCESO AUTOMÁTICO A SEGMENTO CORRESPONDIENTE.

ejemplo: impresoras, cámaras, access points, teléfonos IP, sistemas contra incendios, Thin Clients y lectores biométricos cuando se conecten a un punto de datos institucional se direccionen automáticamente al segmento que le corresponda.

De igual forma el segmento de remediación fue creado para que únicamente funcione en la VLAN 104 “mesa de ayuda” con el direccionamiento 192.168.1.0/24 como inicio.

Para brindar seguridad total en la red de datos del MINFIN[5], se debe incluir todos los segmentos de red de esta institución. Es decir, cuando los computadores y dispositivos que adquieran el direccionamiento IP en cualquier VLAN y no cumplan con los requisitos mínimos de acceso a la red como son: sistema operativo con parches actualizados, antivirus corporativo instalado con la última actualización de firmas de virus, no puedan acceder a la red institucional y permanezcan en la VLAN 309 remediación con el direccionamiento IP 10.9.0.0/16 únicamente con acceso a internet.

1.3 Formulación del problema a resolver

El Ministerio de Finanzas, cuenta con una *“Solución de Control de Acceso, Remediación, Profiling y servicios AAA para la red de datos del Ministerio de Finanzas”*. Esta solución se encuentra implementada desde 27 junio de 2015, bajo la administración de la Dirección de Tecnología y Comunicación DTCs[6], de esta institución.

Esta solución no se encuentra implementada en su totalidad en los segmentos de red institucional. Además, no está orientada al cumplimiento del acuerdo No. 166 de la Secretaria Nacional de la Administración Pública, del *"Esquema Gubernamental de Seguridad de Información EGSI Basado en la ISO 27000”*.

El presente trabajo de tesis mejorará la *“Solución de Control de Acceso, Remediación, Profiling y servicios AAA para la red de datos del Ministerio de*

5 MINFIN: MINISTERIO DE FINANZAS DEL ECUADOR
6 DTCS: DIRECCIÓN DE TECNOLOGÍAS Y COMUNICACIONES

Finanzas". Con la configuración de nuevas características que aún no han sido explotadas según la potencialidad de este equipo.

Estas características son: control de acceso en los puntos de datos de todas las áreas institucionales, postura mediante AAA en los dispositivos de red, remediación y perfilamiento de red.

Además, se configurará y creará un portal de acceso a invitados inalámbricos y alámbricos a la red. A fin de fortalecer la seguridad informática por todos los medios de comunicación de esta institución.

Con la configuración de la característica de BYOD[7], se tendrá mayor visibilidad de los dispositivos móviles que ingresan como por ejemplo: Smartphone, tablets, portátiles, ipads y otros dispositivos móviles que actualmente es muy complejo detectarlos.

Integrar todos los switches de acceso marca Cisco de capa 2, que se encuentran ubicados en los diferentes racks de comunicación de la institución, con el fin de hacer una solución integral y unificada.

Documentar y brindar una capacitación técnica explicando las nuevas características configuradas en la *"Solución Cisco ISE - MINFIN"* entregando manuales de configuración y procedimientos a los administradores de red de la DTCs, con el fin de tener una base de conocimiento amplia que perdure en el tiempo.

El núcleo del trabajo de tesis planteado es adaptar todas las características configuradas de la *"Solución Cisco ISE - MINFIN"* al cumplimento del *"Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública, del Esquema Gubernamental de Seguridad de Información (EGSI) Basado en la ISO 27000"*.

[7] **BYOD**: BRING ON DEVICE, TRAER SU PROPIO DISPOSITIVO DE CASA PARA REALIZAR TRABAJOS CORPORATIVOS.

1.4 Objetivos

1.4.1 Objetivo General

Fortalecer la seguridad informática del Ministerio de Finanzas, mejorando la *"Solución actual de Control de Acceso, Remediación, Profiling y Servicio AAA para la red de datos institucional*", a fin de brindar servicios tecnológicos con altos niveles de seguridad, disponibilidad y cumplimiento de políticas.

1.4.2 Objetivos Específicos

- Mejorar las características de remediación, Profiling y servicios AAA, actualmente configuradas en la red cableada e inalámbrica, a fin de tener mayor control y visibilidad de los dispositivos que ingresan a la red institucional.
- Contar con reportes que permita mostrar información en tiempo real los procesos de autenticación, accounting, cumplimiento de políticas, Profiling, acceso de invitados y sesiones de autenticación de todos los eventos que suceden a nivel de red.
- Documentar y brindar una capacitación a los funcionarios de la DTCs, de las nuevas características configuradas en la "Solución Cisco ISE - MINFIN".
- Adaptar todas las características mejoradas al cumplimiento de los controles EGSI, basados en la norma ISO 27002.

CAPÍTULO II

ESTADO DE LA CUESTIÓN

2.1 Metodologías de Administración de Proyectos

La constante evolución en la administración y manejo de proyectos en todo el mundo. Ha obligado a las distintas organizaciones y empresas dedicadas a este ámbito crear metodologías y estándares que apoyen a los gerentes de proyectos en su gestión de manera profesional.

A continuación, se realiza un detalle de las metodologías y estándares más usados a nivel mundial en la gestión y administración de proyectos de manera profesional.

- **Prince2:** Es una metodología que tuvo origen en Reino Unido. Actualmente ofrece certificaciones profesionales en procesos para la gestión de proyectos.
  Esta metodología es la más usada en países como: Australasia, Dinamarca y Holanda.
  Su distribución es muy práctica y se divide estructuralmente en principios, temáticas y procesos a fin de conseguir el éxito en la gestión de los proyectos.
- **Scrum/Agile**: Esta certificación ha tenido una gran aceptación en los últimos años. Además de un rápido crecimiento, por las ventajas que ofrece esta metodología respecto a la agilidad de manejo de procesos a diferencia de (Kanban, Scrum, Lean, XP entre otras).
  Scrum/Agile a diferencia de los estándares y metodologías como Prince2 o PMP, acredita la experiencia del profesional sin limitarse únicamente a los conocimientos teóricos.

En la Figura que se expone a continuación, se muestran las certificaciones más usadas referentes a la gestión y administración de proyectos en la actualidad.

Figura 3 Las mejores Certificaciones en Gestión de Proyectos

Fuente: **(LPS, 2015)**

Según (Mulcahy, 2013), las metodologías de administración de proyectos se fundamentan en el conocimiento de los conceptos básicos, lineamientos a seguir y el uso de la practica en la dirección profesional de proyectos.

La metodología de administración de proyectos adoptada para el desarrollo de esta tesis, se fundamenta en el estándar de PMBOK (Project Management Body of Knowledge), que traducido al español significa “El Extracto del saber de la Gestión de Proyectos”.

Además, es importante indicar que el PMBOK, no describe ninguna metodología a seguir, su enfoque esencial es llenar de conocimientos robustos y apropiados al administrador del proyecto.

El PM (Project Management – Administrador de Proyecto) determina los procesos adecuados y donde aplicarlos en el proyecto. Las mejores decisiones que se tomen al momento de administrar en el proyecto van a repercutir el éxito o fracaso del mismo.

En la Figura que se expone a continuación se explica el instrumento fundamental para triunfar en la administración de proyectos. Además de permitir conseguir los tres factores primordiales en un proyecto: alcance, tiempo y costos.

Figura 4 Factores Administración de Proyectos

Fuente: **(BS&T, 2011)**

2.2 Arquitectura de Control de Acceso Seguro

Según (Woland & Heary, 2013), pretende asegurar el acceso a una red corporativa, no únicamente asignándole un usuario y una clave. Ahora se pretende manejar contextos con factores de decisión la cual indica si los usuarios que están tratando de ingresar son corporativos o visitantes.

Permite tener mayor visibilidad y trazabilidad de donde y como los dispositivos cableados e inalámbricos están tratando de acceder a la red corporativa

Permite distinguir de manera eficiente si un usuario está accediendo a la red mediante un computador o un dispositivo móvil y además diferenciar la clase de política que se aplicaría en cada escenario.

Dentro de la arquitectura de control de acceso seguro a la red, existen conceptos muy importantes que son parte inherente al entendimiento de este trabajo. Y que se nombran a continuación:

- **Control de Acceso a la Red**

Según (Cisco, 2006) NAC: Network Access Control, tiene como principal funcionalidad asegurar que todos los dispositivos de una red corporativa como por ejemplo: computadores de escritorios, dispositivos móviles, cámaras de seguridad, teléfonos IP, lectores biométricos entre otros cumplan con ciertos lineamientos de seguridad informática para evitar amenazas de ingreso de virus, robo de información, ataques, escaneo de puertos entre otros.

- **Remediación**

Según (Woland & Heary, 2013) es una etapa previa antes de ingresar a una red corporativa. En la cual los dispositivos cableados o inalámbricos son direccionados a un segmento de red aislado VLAN de remediación a fin de frenar el ingreso y corregir los problemas que presentan estos dispositivos antes de ingresar a la red de producción.

En la etapa de remediación se encuentran dispositivos que no cumplen los requisitos mínimos de acceso a la red como, por ejemplo: antivirus, parches de seguridad y usuario de red corporativo. Los cuales únicamente pueden pasar a segmentos de red de producción cuando cumplan todos los requisitos y políticas de red establecidos en la corporación.

- **Postura**

Son factores de cumplimiento en cuanto a políticas de seguridad que los dispositivos cableados e inalámbricos deben cumplir al momento de ingresar a la red corporativa.

Por ejemplo, que los dispositivos cuenten con un antivirus, últimas actualizaciones de sistema operativo, versión mínima de sistema operativo, usuario de red corporativo, agentes de inventario entre otros que pueden ser establecidos por lineamientos internos institucionales.

En la siguiente Figura se exponen todos los factores que van a decidir si un dispositivo cableado o inalámbrico puede ingresar a los segmentos de red de producción, o a su vez únicamente ingresen a segmentos restringidos.

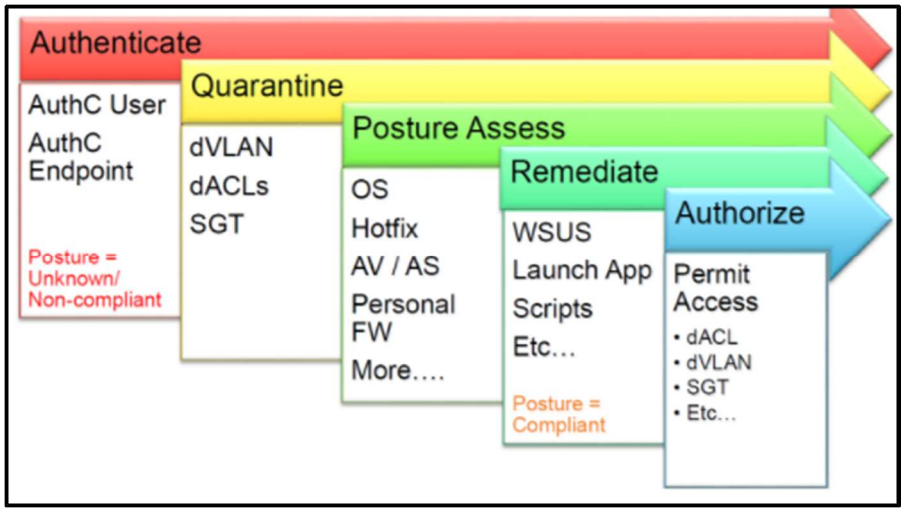


Figura 5 Pasos para efectuar Postura

Fuente: **(Cisco System, 2017)**

- **Identity Service Engine ISE**

Según (Cisco System, 2017) en términos generales es un servidor RADIUS[8] de última generación. Es un orquestador de varios servicios que Cisco System los proveía de manera independiente como son: Control de acceso a servidores **ACS[9]**, detección de que equipo se conecta a la red por perfil "**Profiling"**, Servidor de manejo de invitados, Administrador de Control de Acceso a la Red, RADIUS, Monitoreo, Reportera y Detección de fallas "**Troubleshooting"**.

Cisco integra todo este portafolio en un equipo llamado *"Identity Service Engine"* que estaba disperso en diferentes productos con el fin de facilitar la administración y primordialmente abaratar costos.

[8] **RADIUS:** COMPRUEBA QUE LA INFORMACIÓN ES CORRECTA UTILIZANDO ESQUEMAS DE AUTENTICACIÓN COMO PAP, CHAP O EAP

[9] **ACS:** CONTROL DE ACCESO A SERVIDORES

2.3 Función AAA Authentication, Authorization and Accounting

Según (Cisco System, 2017) la idea principal de la solución *"Identity Service Engine - ISE"* en cuanto al acceso AAA. Es proveer el acceso a una red de datos por cualquier medio alámbrico, inalámbrico o VPN[10] el cual debe estar controlado y monitoreado por esta solución.

El servicio AAA con la inteligencia de Cisco ISE, controla el acceso a la red de todo tipo de dispositivo como, por ejemplo: impresoras, cámaras de seguridad, lectores, en pocas palabras y resumiendo todo equipo que tenga una IP.

A continuación, se explica el significado de la función AAA Authentication, Authorization and Accounting.

- **Authentication (Autenticación)**

Es el proceso que define cual es el dispositivo que está tratando de ingresar a la red de datos corporativa. También indica que protocolo de control de acceso y autenticación usa como por ejemplo: autenticación con un directorio activo o usando el protocolo 802.1X[11].

- **Authorization (Autorización)**

Es el proceso que define que permisos de red tendrá un dispositivo al momento de conectarse a una red corporativa. Es decir, una vez que pasa el proceso de autenticación indica que usuario se conectó, tipo de dispositivo y sí cuenta con los permisos o privilegios necesarios para acceder a los segmentos de producción institucionales.

[10] **VPN:** RED VIRTUAL PRIVADA

[11] **802.1X**: PROTOCOLO DE CONTROL DE ACCESO A LA RED CREADO POR LA IEEE

En este caso de “Cisco ISE”, maneja el concepto de VLAN Dinámica, para el cual utiliza los usuarios de Directorio Activo mediante la comunicación con switches de acceso. Este proceso es realizado de manera automática direccionando el dispositivo del usuario para que acceda a la red de datos del segmento correspondiente.

- **Accounting (Contabilidad)**

Este proceso se encarga de llevar un registro de todas las conexiones realizadas por los dispositivos cableados e inalámbricos que trataron de ingresaron a la red corporativa. A medida de ejemplo indica: que dispositivo se conectó, a qué hora se conectó, a que switches se conectó, porque medio se conectó, si la conexión fallo entre otras opciones.

2.4 Protocolos de Authentication, Authorization and Accounting

Su función principal es ejecutar el control de acceso a la red de datos entre los cuales tienen mayor relevancia: RADIUS, TACACS+ y DIAMETER. Se distinguen uno de otro por sus funciones y capacidades.

Las organizaciones deberán escoger entre estos protocolos dependiendo la necesidad, flexibilidad y la arquitectura de red de datos.

En el siguiente detalle, se explica los protocolos AAA Authentication, Authorization and Accounting, que son parte fundamental para el entendimiento de este trabajo.

- **Protocolo RADIUS**

El protocolo RADIUS *(Remote Authentication Dial In User Service)* que en español significa *“Autenticación Remota para usuarios de Servicio Telefónico”*. Utiliza la arquitectura cliente servidor donde el servicio AAA, es administrado por uno o varios servidores específicos que cumplen la función de RADIUS.

En la siguiente Figura se explica cómo funciona el "*Protocolo RADIUS*" en una red de datos.

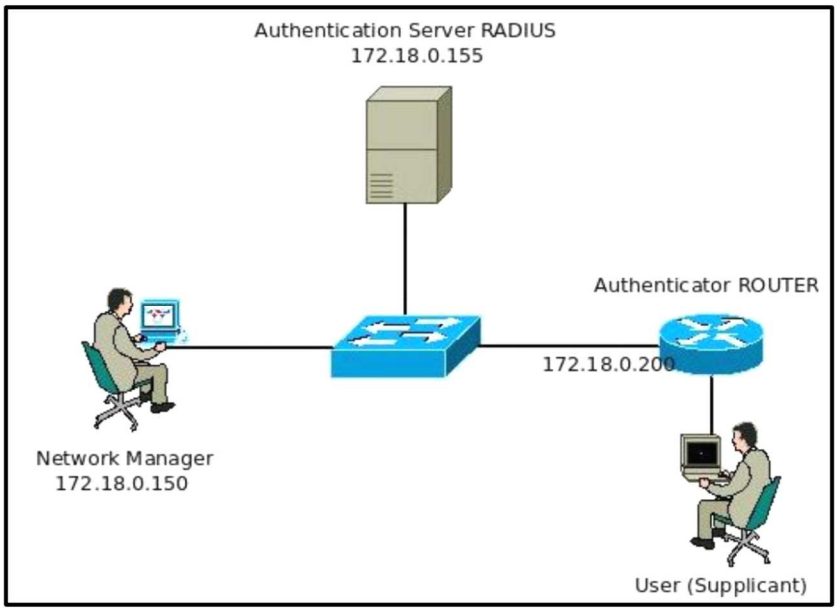


Figura 6 Proceso AAA

Fuente: **(S2Grupo, s.f.)**

- **Protocolo TACACS+**

Este protocolo está basado en *(Terminal Access Controller Access Control System)* que en español significa "*Sistema de Control de Acceso y Control de Acceso a Terminales*". La principal diferencia de TACACS+ con RADIUS radica en la separación de los procesos: autenticación y autorización según el perfil de usuario.

Este protocolo fue diseñado por Cisco. Al igual que RADIUS su funcionamiento radica bajo el concepto de cliente servidor y emplea TCP/IP[12].

En la siguiente Figura se explica el funcionamiento de los protocolos TACACS+ y RADIUS.

[12] **TCP/IP:** PROTOCOLO DE CONTROL DE TRANSMISIÓN/PROTOCOLO DE INTERNET

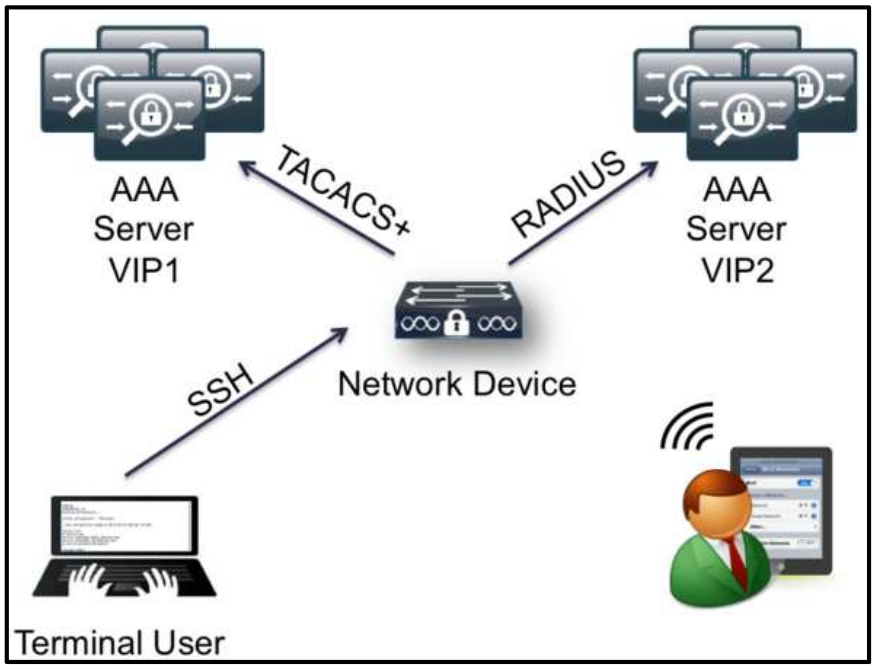


Figura 7 Proceso TACACS+ y RADIUS

Fuente: **(Woland A. , s.f.)**

- **Protocolo DIAMETER**

Desarrollado en 1998 y aprobado por la IETF[13] desde el año 2003. Este protocolo es creado para soportar la evolución de las nuevas tecnologías inalámbricas de control de acceso. Proporciona autenticación, autorización y contabilidad para usuarios móviles como, por ejemplo: portátiles, celulares, tablets entre otras tecnologías.

En la siguiente Figura se expresa la ejecución del protocolo DIAMETER, entre un cliente, un agente proxy y un servidor.

[13] **IETF**: ENTIDAD QUE REGULA LAS PROPUESTAS Y ESTÁNDARES DE INTERNET

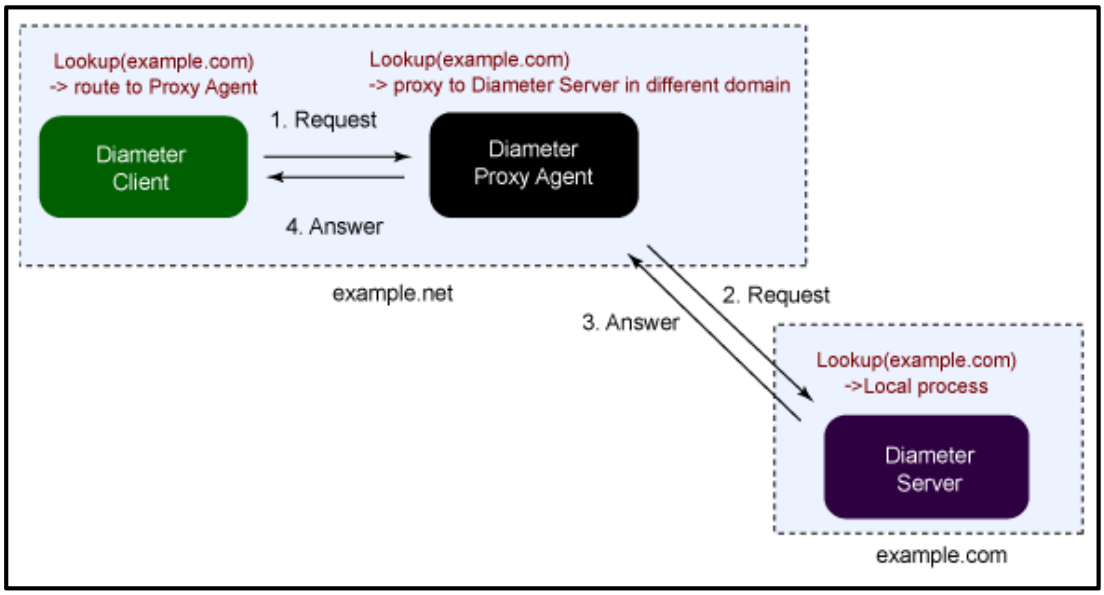


Figura 8 Ejecución protocolo DIAMETER

Fuente: **(Jeffrey, Jiang, Lin, 2006)**

2.5 Mecanismos de Control de Acceso

En el siguiente detalle, se realiza un análisis profundo del protocolo 802.1X sus características y componentes, como mecanismos de control de acceso a las redes de datos.

- **Protocolo 802.1X**

Este protocolo ejecuta el proceso de autenticación y control de acceso entre el cliente y el servidor, realiza la petición a un equipo de red como puede ser un switch o una controladora inalámbrica, para que finalmente *"Cisco ISE"* a través de su inteligencia indique si al dispositivo se deniega o permite el acceso a la red corporativa.

En la Figura que se expone a continuación, se explica los pasos que sigue un dispositivo que usa el protocolo 802.1X, hasta su autenticación.

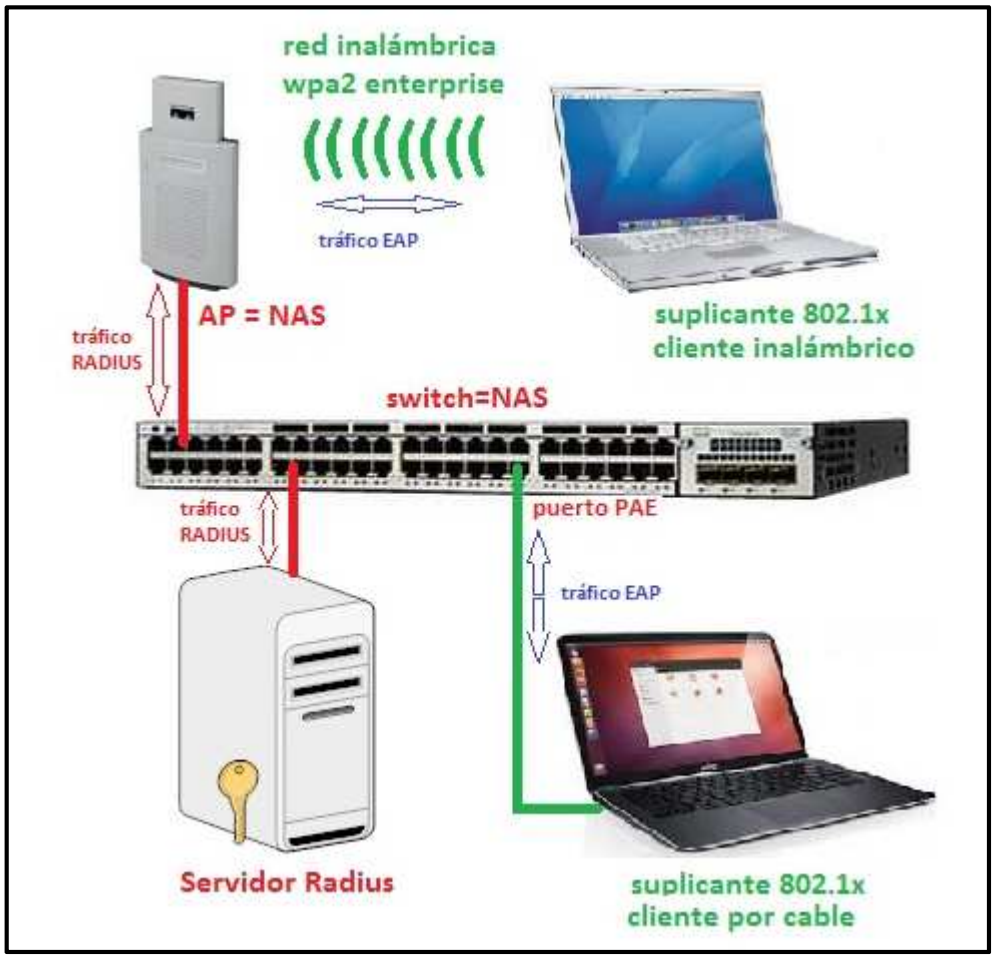


Figura 9 Ejecución del protocolo 802.1X

Fuente: **(Céspedes, 2013)**

Con la ayuda del protocolo EAP[14] *"Protocolo de Autenticación Extensible"* permite la transmisión de datos entre los equipos de comunicación y dispositivos finales.

- **Componentes 802.1X**

Entre las características relevantes que utiliza el protocolo 802.1X podemos mencionar las siguientes:

- **Protocolo estándar para la industria (RFC3380 , IEEE[15])**

[14] **EAP:** PROTOCOLO DE AUTENTICACIÓN EXTENSIBLE, AYUDA A MÉTODOS DE AUTENTICACIÓN MÁS USADOS EN TECNOLOGÍAS DE ACCESO A LA RED

[15] **IEEE:** INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS

- ✓ Permite reconocer usuarios, dispositivos y sus funciones en la red
- ✓ Proporcionar acceso de invitados fácil y seguro
- ✓ Simplifica el acceso a dispositivos no autenticados
- ✓ Permite auditar e informar que dispositivo ingresan a la red de datos

Los componentes relevantes que utiliza el protocolo 802.1X podemos mencionar las siguientes:

- ✓ **Servidor ACS[16] de Cisco:** Administración central de políticas
- ✓ **802.1X Suplicante:** Proporciona credenciales al cliente para el ingreso a la red de datos (podría ser independiente o suplicante del propio Sistema Operativo)
- ✓ **Perfilamiento NAC:** Descubrimiento de puntos finales, perfiles y monitoreo de comportamiento
- ✓ **Servidor de invitado de NAC:** Registro de acceso para invitados seguro

En Figura que se representa a continuación se exponen los componentes que intervienen en el funcionamiento del protocolo 802.1X.

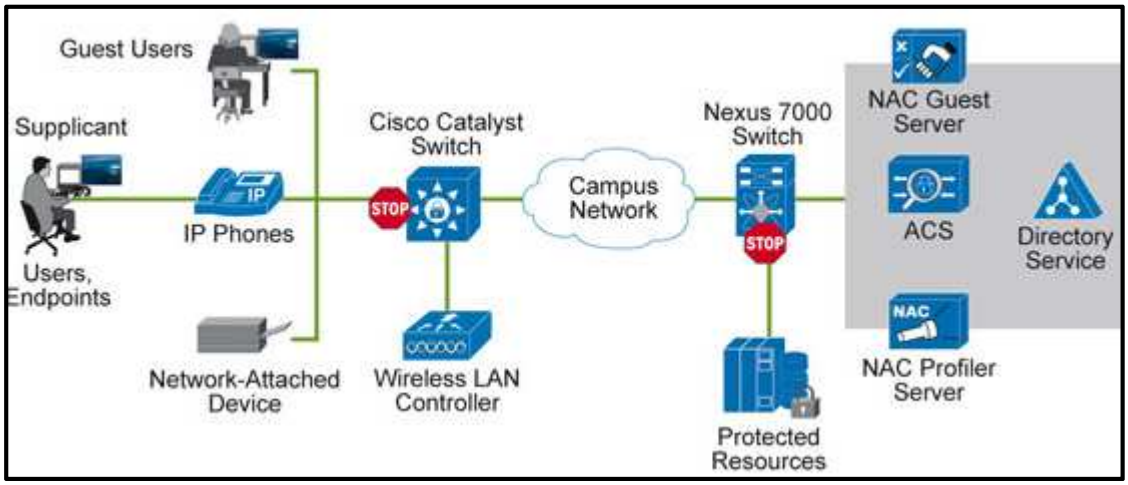


Figura 10 Componentes protocolo 802.1X

Fuente: **(Sanbower, s.f.)**

[16] **ACS:** ACCESO DE CONTROL SEGURO

- **Modo Monitor**

Permite activar todos los procesos de autenticación por medio de *"Cisco ISE"*, sin embargo, no va a causar una denegación de servicio al dispositivo que trate de ingresar a la red de datos corporativa. Este modo es usado en implementaciones de bajo impacto.

- **MAC Authentication Bypass MAB**

Existen algunos dispositivos que no soportan el protocolo 802.1X, en una red corporativa como, por ejemplo: impresoras, lectores biométricos, zero clientes, cámaras de seguridad entre otros.

Para lo cual Cisco utiliza *"MAC Authentication Bypass MAB"* que consiste en registrar todas las mac address de los dispositivos que van a ingresar a la red de datos corporativa. Los dispositivos registrados van a ingresar a la red de datos sin ningún tipo de restricción.

En la Figura que se representa a continuación, se explica el funcionamiento de un dispositivo antes y después de utilizar MAB (MAC Authentication Bypass)

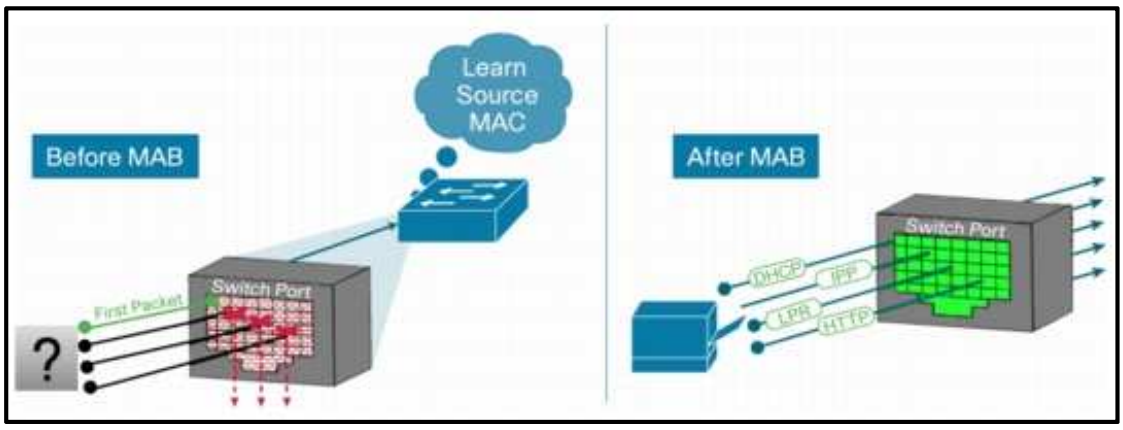


Figura 11 Procedimiento MAB

Fuente: **(Cisco Systems, 2015)**

En la Figura que se muestra a continuación, se explica el registro de impresoras a través de MAB (MAC Authentication Bypass) en la solución de Cisco – ISE del Ministerio de Finanzas.

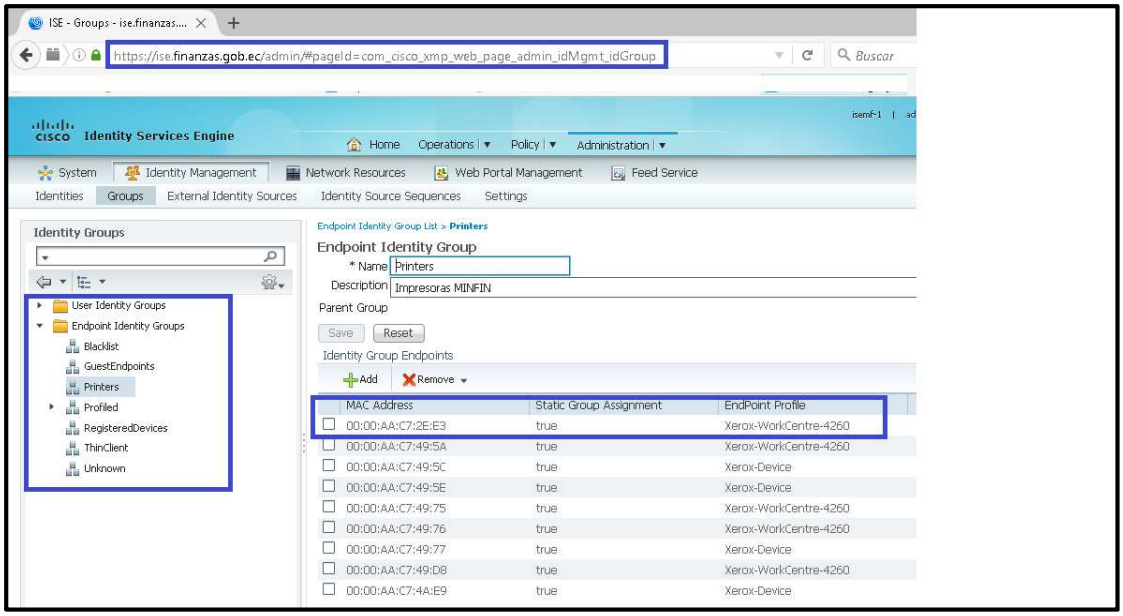


Figura 12 Dispositivos MAB integrados Cisco ISE – MINFIN

Fuente: **(Diseño Propio, 2017)**

- **Profiling**

Identifica y clasifica los dispositivos de acuerdo a su tipo como, por ejemplo: computadores personales, impresoras, thin clients, cámaras web entre otros.

Profiling puede llegar a un nivel de profundidad muy amplio que puede distinguir que marca, modelo de dispositivo ingreso a la red de datos. Permitiendo tener mayor visibilidad para ejecutar controles de los dispositivos permitidos y no permitidos el ingreso a la red de datos.

Cisco ISE, tiene una base de datos muy extensa de marcas y modelos de dispositivos cableados e inalámbricos que constantemente se está actualizando con la nube. Esto es con el fin de poderlos clasificar dentro de las redes de datos corporativas sin mayores inconvenientes.

- **Centralización de Autenticación Web**

Según (Cisco System, 2017) la autenticación web, es usado para visitantes y usuarios que tengan problemas con el protocolo 802.1X, en sus dispositivos.

Consiste en desplegar un portal web en el dispositivo del usuario, en la cual debe ingresar las credenciales asignadas para ingreso a la red de datos corporativa.

Esta característica es una ventaja muy amplia para las personas de soporte técnico corporativo. Debido a la agilidad y flexibilidad en la asignación de credenciales de acceso a la red a los usuarios de visita.

- **Bring your Device BYOD**

Según (Cisco System, 2017) *"Bring your Device BYOD"* permite el acceso a dispositivos de los usuarios corporativos que no pertenecen a la organización.

Entre estos dispositivos tenemos: smartphones, tablets portátiles entre otros, que desean ingresar a la red de datos cumpliendo los lineamientos establecidos en la corporación de forma segura.

En la siguiente Figura, que se muestra a continuación. Expresamos el uso de BYOD *"Bring your Device BYOD"* en las redes de datos empresariales.

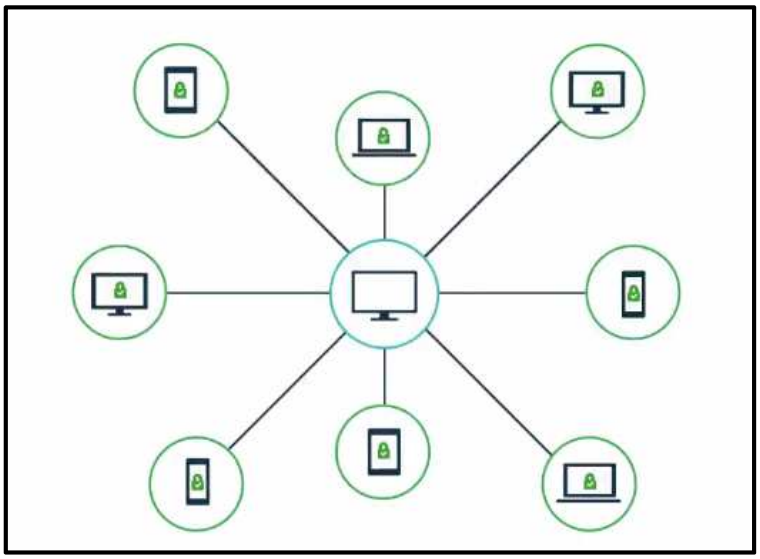


Figura 13 “Bring your Device BYOD”

Fuente: **(Cisco System, 2017)**

- **TrustSec Ejecución de Políticas en la Red**

Según (Cisco System, 2017) TrustSec, se puede explicar cómo la ejecución de políticas de seguridad en la red de datos.

Cisco TrustSec, brinda a la red de inteligencia, mediante políticas basadas en control de acceso, identidad en la red de datos, confidencialidad en la información e integridad en los datos corporativos.

Para entender TrustSec, debemos identificar qué papel cumplen ciertos usuarios dentro de la empresa. Además, que dispositivos de red usan para acceder a la información de la empresa.

Normalmente sino se posee la tecnología adecuada se tendría un sin número de listas de control de acceso y reglas. A fin de permitir o denegar el acceso de los dispositivos ligados a los usuarios autorizados para ingresar a la red corporativa.

TrustSec, de manera automática distingue y clasifica el tipo de dispositivo que tiene autorización para ingresar a la red de datos corporativa.

Cisco Identity Service Engine, mediante la tecnología TrustSec, detecta si un dispositivo de usuario está infectado para separarlo inmediatamente de la red de datos de producción y enviarlo a un grupo aislado *"Remediación"*.

En la siguiente Figura que se muestra a continuación. Representamos como TrustSec de Cisco facilita el acceso a una red de datos dependiendo el papel que cumple el usuario en la corporación, mediante el uso de cualquier dispositivo.

Figura 14 Tecnología TrustSec de Cisco

Fuente: **(Cisco System, 2017)**

Hasta el momento existen tres formas de ejecución de políticas de seguridad usando TrustSec:

- **A Nivel de dACL Listas de Control de Accesos Dinámicas**

Su funcionamiento es como una lista de Control de Acceso normal, permite o deniega el tráfico a ciertos segmentos de una red de datos. La diferencia radica que *"Cisco ISE"* maneja de forma inteligente y dinámica las listas de control de acceso.

- **A Nivel de VLAN**

Radica principalmente en segmentar una red de datos a fin de fortalecer la seguridad de acceso entre segmentos. Por ejemplo, el acceso a la VLAN de invitados no debe tener acceso a los segmentos VLAN de producción.

En la siguiente Figura se expresa la segmentación básica de una red de datos por VLAN.

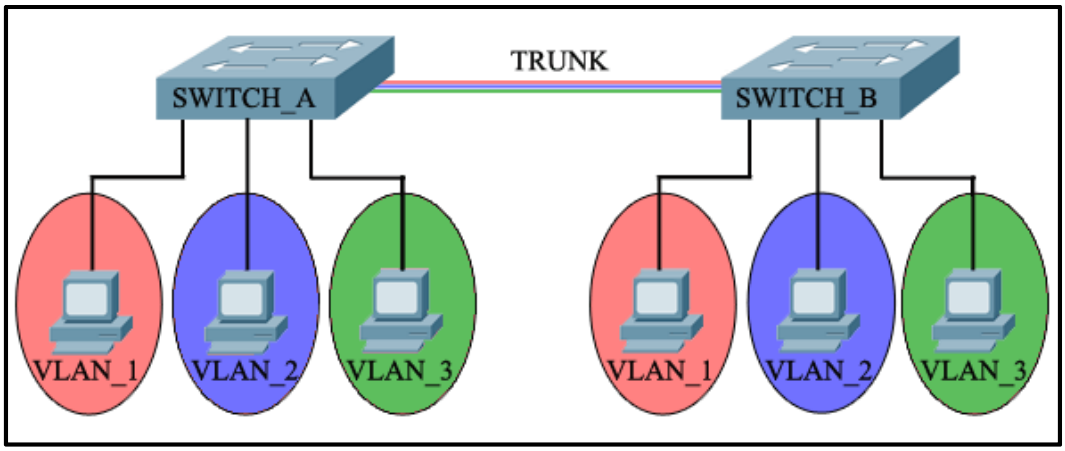


Figura 15 Segmentación básica de una red de datos

Fuente: **(Djebbouri , 2015)**

- **A Nivel de Security Group Access SGA**

Funciona mediante el uso de identificadores “Tagging - marcado” es una forma más inteligente de identificación de tráfico que circula por una red de datos. Cisco ISE es la parte inteligente que etiqueta el tráfico de un usuario que ingresa a la red, y a su vez envía órdenes a los equipos de red tales como: switches de acceso, controladora inalámbrica entre otros, para la ejecución de lineamientos de acceso.

- **Administración de Dispositivos Móviles MDM**

Según (Cisco System, 2017), Mobile Device Management MDM, realiza la funcionalidad de postura en dispositivos móviles, es decir cuando un equipo móvil

trata de ingresar a una red corporativa a través de un contralor inalámbrico es detectado automáticamente por *"Cisco ISE"*.

Su funcionamiento radica en la instalación de una aplicación en el dispositivo móvil que interactúa con *"Cisco ISE"*, para verificar los lineamientos establecidas de acceso a la red, permitiendo o denegando su ingreso.

Además, si el dispositivo móvil que ingresó a la red de datos es robado o extraviado, puede ser borrado remotamente con la integración de fabricantes de terceros, como, por ejemplo: Antivirus, Directorio Activo de Microsoft entre otros. Con el fin de no comprometer la integridad de la información de la institución.

2.5 Arquitectura de Despliegue

Según (Woland & Heary, 2013) *"Cisco ISE"*, puede ser desplegado a través appliances[17] o máquinas virtuales, considerando la cantidad de equipos de red que ingresaran a la red de datos corporativa. Además es recomendable instalar los appliances *"Cisco ISE"* en redundancia mediante HA[18], para precautelar la alta disponibilidad de los servicios que transitan a través de la red de datos corporativa.

Para mejorar la administración, balanceo de carga y rendimiento de ISE, hay la opción de dividirlo en nodos separados, como se indica a continuación:

- **Policy Administration Node PAN**

Es el encargado de recibir las políticas de administración y la interfaz gráfica de todos los cambios realizados.

17 **APLIANCES**: HARDWARE DESTINADOS A FUNCIONES ESPECIFICAS
18 **HA**: ALTA DISPONIBILIDAD

- **Policy Service Node PSN**

Recibe las peticiones de autenticación y evalúa todos los parámetros para definir si permite o deniega el acceso a la red.

- **Monitoring and Throubleshooting MnT**

Este nodo se encarga únicamente de la reportera y al registro de las conexiones de los dispositivos de red.

- **Network Access Device NAD**

Es la encargada de la administración de todos los dispositivos que ingresan en la red de datos corporativa.

En la siguiente Figura se expone una de las formas como el appliance “Cisco ISE”, puede agrupar sus nodos PAN, MnT y PSN para obtener mayor eficiencia y alta disponibilidad

Figura 16 Agrupación de Nodos Cisco ISE

Fuente: **(Cisco System, 2017)**

2.6 Solución Cisco ISE

Es una plataforma de última generación diseñada por Cisco Systems[19] para el control de políticas de acceso en las redes de datos empresariales. Además, permite

[19] **CISCO SYSTEMS:** EMPRESA LÍDER MUNDIAL EN VENTA, CONSULTORÍA Y MANTENIMIENTO DE EQUIPOS DE TELECOMUNICACIONES

mejorar la seguridad en la infraestructura de red cableada, inalámbrica y en algunos casos VPNs, dependiendo de las características de sus equipos de seguridad perimetral.

Identity Service Engine ISE, es la versión mejorada de su antecesor Cisco NAC, permite tener mayor visibilidad en tiempo real y trazabilidad de los dispositivos que ingresan a nuestra red de datos corporativa.

Es una plataforma que puede instalarse de dos formas en una red de datos. Mediante appliances[20] o máquinas virtuales.

Entre elegir la opción de appliances o máquinas virtuales va a depender primordialmente del rendimiento y la cantidad de usuarios que se van a manejar dentro de una red de datos corporativa.

En la siguiente Figura se muestra un appliance (Hardware) de la solución "*Cisco ISE"*.

Figura 17 Appliance Cisco ISE

Fuente: **(Cisco System, 2017)**

- **Características de Cisco ISE**
  - ✓ Indica quién, qué, cuándo, dónde y cómo un dispositivo ingresó a la red datos de la organización no importa el medio ya sea cableado o inalámbrico.
  - ✓ Reporterita avanzada de los dispositivos que ingresan a la red de datos en la organización.
  - ✓ Trazabilidad de todos los eventos de conexión de los dispositivos que ingresan a la red de datos de la organización.

[20] **APPLIANCE:** HARDWARE DEDICADO PARA UN SOFTWARE ESPECIFICO

- ✓ Automatización de la red de datos mediante las características de postura, perfilamiento y autenticación.
- ✓ Manejo de portales cautivos para la facilitar el ingreso a la red de datos especialmente a usuarios invitados.
- ✓ Integración de varios equipos de telecomunicaciones para para fortalecer y unificar la red de datos en un solo cuerpo.
- ✓ Inventario de marca y modelo de los dispositivos que ingresan a la red de datos.
- ✓ Flexibilidad para aplicar la característica BYOD "trae tu propio dispositivo de casa" por la gestión de lineamientos de seguridad antes de que el dispositivo ingrese a la red de datos corporativa.
- ✓ Auditoria de los dispositivos móviles que ingresan a la red de datos.
- ✓ Segmentación de manera automática redireccionando al dispositivo que ingresó a la red de datos a la VLAN correspondiente.
- ✓ Utilización de dACL "Listas de control de acceso descargables" facilitando la automatización en los equipos de telecomunicaciones.
- ✓ Gestión de políticas de acceso para brindar mayor seguridad a los usuarios.
- ✓ Clasificación de tráfico por dispositivo de manera automática.
- ✓ Alta disponibilidad dependiendo el esquema que se utilice para su implementación.

- **Beneficios de Cisco ISE**

Las redes de datos empresariales ya no están limitadas únicamente para conexión de dispositivos únicamente es sus propias instalaciones. Ahora con las nuevas tecnologías de datos han evolucionado más allá de lo imaginable en la forma de cómo vivimos y trabajamos.

Las cosas como el IoT[21] "Internet of Things" que traducido al idioma español significa "El Internet de las Cosas" ha transformado la manera de vivir y trabajar.

[21] **IoT:** INTERNET DE LAS COSAS

También el acceso a los recursos críticos de las compañías desde más dispositivos sin importar la ubicación geográfica.

Las empresas deben soportar la proliferación de dispositivos habilitados para el ingreso a segmentos de datos críticos.

A medida que las redes de datos modernas se expanden, existe la necesidad de proteger el acceso a la información ante amenazas de seguridad y violaciones. Aumentando la necesidad de adquirir recursos y soluciones de seguridad con el fin de salvaguardar la información.

Para adelantarse a las amenazas a través de la visibilidad y control es necesario tener un enfoque diferente para administrar y salvaguardar la información, Cisco Identity Service Engine (ISE) es la solución.

En la siguiente Tabla se expone los beneficios más importantes que impactan a las redes de datos corporativos al adquirir una solución de "*Cisco Identity Service Engine (ISE)"*

Tabla 1
Solución Cisco Identity Service Engine (ISE)

Característica	Beneficio
Centralizar y Unificar	Los dispositivos que intervienen para proporcionar el servicio de datos. A fin de robustecer la visibilidad y trazabilidad.
Usuarios Finales	Proporcionar el acceso seguro a la red de datos, indiferentemente el tipo de conexión que se use: Por ejemplo inalámbrica, por cable de datos o VPN.
Visibilidad	Obtener información precisa e identificación en tiempo real de los dispositivos que están accediendo a la red de datos. A fin de reducir la visibilidad de dispositivos desconocidos.
Usuarios Invitados	Facilita la experiencia de acceso a usuarios invitados, por la facilidad, gestión y agilidad en la creación y personalización de portales de acceso.
Reducir el riesgo	Visibilidad profunda de los dispositivos y aplicaciones de los usuarios que acceden a la red de datos.

Continúa

Control Dinámico	Asegura que únicamente los dispositivos y personal autorizado obtengan acceso a los servicios de red corporativos.
Acceso físico seguro	Acceso seguro en las conexiones inalámbricas, cableadas o VPN, por sus características de remediación y perfilamiento de dispositivos y usuarios.
TrustSec	Distingue y clasifica el tipo de dispositivo que tiene autorización para ingresar a la red de datos corporativa. Direccionando dinámicamente al segmento de red correspondiente, sin la complejidad de múltiples VLANs o la necesidad de rediseñar la red.
Detección y Mitigación de amenazas	Transforma una red de datos convencional en un solo cuerpo por medio de la unificación de todos los equipos de red. A fin de obtener mayor visibilidad para detectar y mitigar las amenazas.
Trae tu propio dispositivo (BYOD)	Integrar dispositivos no corporativos por la fácil configuración y el uso de portales de autoservicio.
Integración	Mejora su eficacia con la ayuda de equipos correlacionadores de eventos SIEM[22] de otros fabricantes. A fin de realizar comparaciones de eventos con otros sistemas de seguridad como por ejemplo: antivirus, firewalls, UTMs, IPS entre otros.
Robustecer autenticación	Interacción con el Directorio Activo y Entidades certificadoras de Windows. Para obtener visibilidad de los usuarios corporativos.
Mobile Device Management (MDM)	Permite administrar y monitorear dispositivos móviles como, por ejemplo: Celulares. Tablets, Ipads entre otros dispositivos.
Ahorro de dinero	Prevención contra amenazas reduciendo gastos de expertos para solucionar problemas de vulnerabilidades, consultorías de Ethical Hacking, Infecciones etc.

- **Comparación entre Cisco NAC vs Cisco ISE**

Según explicaciones anteriores *"Cisco ISE" "Identity Service Engine"* es la versión mejorada de Cisco NAC *"Network Access Control"*.

En la siguiente Tabla se mencionan las características más importantes entre las soluciones de Cisco NAC y Cisco ISE.

[22] **SIEM:** SECURITY INFORMATION AND EVENT MANAGEMENT EN ESPAÑOL ADMINISTRADOR DE EVENTOS E INFORMACIÓN DE SEGURIDAD

Tabla 2
Comparaciones entre Cisco NAC y Cisco ISE

Característica	NAC "Network Access Control".	ISE "Identity Service Engine".
Servidor de DHCP	Disponible	No Disponible
Servicio de Postura en equipos y dispositivos	No Disponible	Disponible
Postura basada en condiciones definidas	No Disponible	Disponible
Cliente para inspección de políticas	No Disponible	Disponible
Descubrimiento de Host basada en condiciones	No Disponible	Disponible
Agente de perfil basado en condiciones	No Disponible	Disponible
Portal de Servicio de Invitados	No Disponible	Disponible
Personalización de portales de Autenticación WEB	No Disponible	Disponible
Grupo de Accesos de Seguridad	No Disponible	Disponible
Listas de control de acceso descargables	No Disponible	Disponible
Registro de dispositivos	No Disponible	Disponible
Servicio de Perfilamiento	No Disponible	Disponible
Centralización de autenticación WEB	No Disponible	Disponible
Unificación de Tecnologías CISCO	No Disponible	Disponible
Integración con NAC, servicios de administración, monitoreo y servicios	No Disponible	Disponible
RADIUS	No Disponible	Disponible
Syslog	Disponible	No Disponible
DHCP	Disponible	Disponible
Netflow	Disponible	Disponible
Monitoreo y Reportería integrada	No Disponible	Disponible
Integración Sensor IOS	No Disponible	Disponible
Integración con Postura, Invitados, Servicios AAA	No Disponible	Disponible
Posibilidad de Cluster		Disponible
Alta Disponibilidad Activo-Pasivo/Pasivo-Activo	Disponible	Disponible
Licenciamiento	Limitado por recolección de datos	Por dispositivo
Herramientas para diagnostica de problemas	Básica	Avanzada
Notificación de Alertas	No Disponible	Disponible

Continúa

y Alarmas		
Reporte de Actividad de Perfilamiento y Postura	No Disponible	Disponible
Elementos para políticas diccionarios y condiciones	No Disponible	Disponible
Administración de dispositivos Móviles	No Disponible	Disponible
Manejo de Identidades	No Disponible	Disponible
Diccionario de fabricantes de dispositivos	No Disponible	Disponible
Diccionario de software de fabricantes	No Disponible	Disponible
Inventario en línea de dispositivos que ingresan a la red	No Disponible	Disponible
Integración con unidades certificadoras de otros fabricantes	No Disponible	Disponible
Utilización de MAB para dispositivos	Básico	Avanzado
Integración con Directorio Activo de Windows	Básico	Avanzado
Inventario de Software de dispositivos que ingresan a la red	No Disponible	Disponible
Integración con switches de otras marcas mediante 802.1X para la autenticación de dispositivos	No Disponible	Disponible
Métricas en línea del número de dispositivos que ingresaron a la red	No Disponible	Disponible
Integración con servidores SIEM externos para mayor detalle de Reportería	No Disponible	Disponible

Fuente: (Cisco System, 2017)

2.7 Esquema de Gestión de Seguridad de la Información EGSI

2.7.1 Referencias Legales

Mediante el Acuerdo No. 166 de la Secretaría Nacional de la Administración Pública, se emitió el *"Esquema Gubernamental de Seguridad de Información (EGSI)"*basado en la norma técnica INEN ISO/IEC 27002, que dispone adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad de la información que se genera y custodia en

diferentes medios y formatos las entidades de la Administración Pública Central y que dependen de la Función Ejecutiva.

Normas de Control Interno en la sección "*410-10 Seguridad de Tecnología de información*" donde se dispone que, "*La Unidad de Tecnología de la Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas de medios físicos y la información que se procesa mediante sistemas informáticos (…)".*

Normas de Control Interno en la sección *"410-12 Administración de Soporte de Tecnología de Información"* donde se dispone que, *"La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen"* considerando los siguientes aspectos:

"(...) 2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad".

"(...) 5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos."

"6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas".

"(...) 11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes

sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

Según Registro Oficial Acuerdo Ministerial No. 254, sobre la Organización y Administración del Ministerio de Finanzas entre las atribuciones y responsabilidades de la Dirección de Tecnologías y Comunicación establece que: "*Proveer servicios tecnológicos para solventar las necesidades institucionales internos referentes a comunicaciones (...)".* y *"Establecer políticas de uso y seguridad para acceder a un recurso de información y comunicaciones.*

2.7.2 Principios Básicos y Definiciones orientadas a la Seguridad Informática

Seguridad de la Información significa “proteger” la información de los distintos tipos de amenazas y vulnerabilidades que podrían atacarla; preservarla mediante un conjunto de acciones que permitan proteger los activos de información de los riesgos inherentes a su exposición en los siguientes casos:

- **Confidencialidad**: Asegura que solo quienes estén autorizados puedan acceder a la información, de acuerdo con la Ley Orgánica de Transparencia y Acceso a la Información Pública – LOTAIP.
- **Integridad:** Asegura que la información y sus métodos de proceso sean exactos y completos.
- **Disponibilidad:** Asegura que los usuarios autorizados tengan acceso a la información cuando lo requieran.

Además, la seguridad de la información considera los conceptos de:

- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantizar el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación:** Asegura que una copia sólo se realice una vez, a menos que se especifique lo contrario, e impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** Evita que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Confiabilidad de la Información**: Que sea generada adecuadamente para sustentar la toma de decisiones y la ejecución de las funciones.
- **Legalidad:** Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto las organizaciones.
- **Vulnerabilidad:** Se puede definir como una debilidad sea de hardware o de software que puede ser aprovechada para dañar o atacar sino es corregida en su debido momento
- **Amenaza:** Es el elemento que aprovecha una vulnerabilidad para infringir contra la seguridad de un activo informático de las organizaciones.
- **Riesgo:** Probabilidad de ejecución de una amenaza, vulnerabilidad comprometiendo los activos de información, y a su vez produciéndose un incidente informático.

  Mediante la siguiente fórmula se puede entender los Riesgos, Amenazas y Vulnerabilidades.

Riesgo = **Probabilidad** de que una **Amenaza** explote una **Vulnerabilidad** de un **Activo** generando un **Impacto**

En la siguiente Figura se muestra gráficamente que el *"Riesgo"* es igual a la "*Probabilidad"* de que una **"***Amenaza"*. Cuando se explota una **"***Vulnerabilidad"* de un **"***Activo"* se genera un **"***Impacto"*.

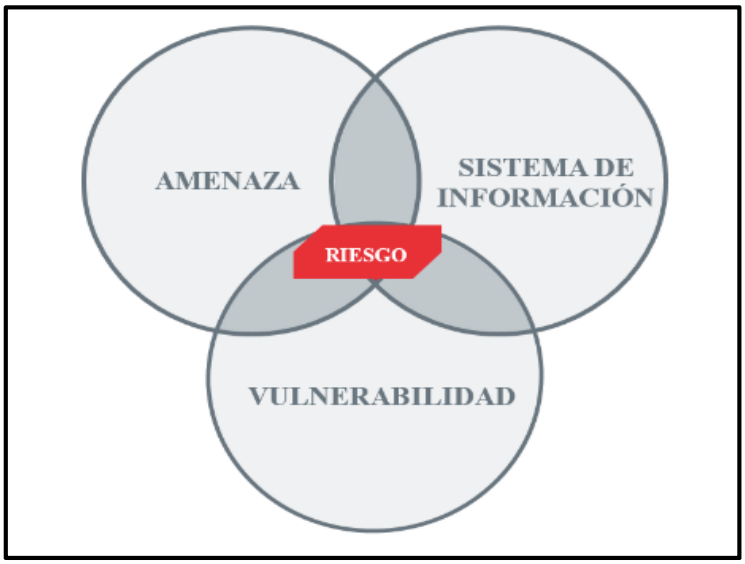


Figura 18 Riesgo Amenaza Vulnerabilidad

Fuente: **(Incibe, 2017)**

La seguridad de la información se consigue identificando y reconociendo los riesgos a los que se encuentran expuestos sus activos de información, mismos que deberán ser tratados mediante la planificación, implantación, monitoreo, revisión y mejora continua de un conjunto adecuado de controles tales como políticas, normas, procedimientos, estándares, estructuras organizativas, software e infraestructura.

En la siguiente Figura, se representa el triángulo de los pilares fundamentales de la seguridad de la información.

Figura 19 Pilares de la Seguridad Informática

Fuente: **(Sasia, 2011)**

2.7.3 Sistema de Gestión de Seguridad de la Información SGSI

Es un parte del sistema de gestión enfocándose en el riesgo empresarial que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Significa que se va a dejar de operar de una manera intuitiva y se tomará el control de los sistemas de información, sobre la propia información que maneja en las organizaciones.

- **Esquema de Gestión Gubernamental de Seguridad de la Información EGSI**

Está diseñado y acoplado para el cumplimiento de ciertas directrices y políticas para la Gestión de Seguridad de la Información en el Sector Público ecuatoriano

Es importante mencionar que el *"Esquema de Seguridad de la Información EGSI"* adopta sus directrices basado en el esquema INEN ISO/IEC 27002, mas no las reemplaza.

2.7.4 Normas ISO/IEC 27000

Es un conjunto de estándares en fase de desarrollo por la ISO que traducido al español significa *"Organización Internacional para la estandarización"* e IEC *"Comisión Internacional Electrotécnica"* que proporciona un esquema para gestión de la seguridad de la información en cualquier tipo de entidad, ya sea pública o privada.

Las *"NORMAS ISO/IEC 27000"* se fundamentan primordialmente en proteger la información que transita en una organización, mediante el uso de una gestión adecuada de la seguridad de la información.

- **Origen Normas ISO/IEC 27000**

Aparece por primera vez en el año de 1995 con el nombre de BS 7799, por la empresa BSI (Entidad de normalización británica) con el objetivo de proporcionar a cualquier empresa sea pública o privada, un conjunto de buenas prácticas para la gestión de la seguridad de la información.

En el año de 2005, este esquema fue publicada por la ISO como estándar y a su vez revisado y actualizado por esta misma organización.

En la siguiente Figura se explica el origen y la evolución de la Norma ISO/IEC 27000.

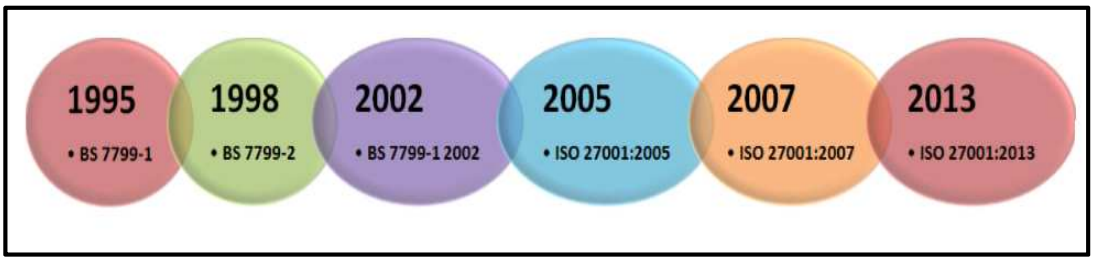


Figura 20 Origen y Evolución Norma ISO/IEC 27000

Fuente: **(ISOTools Excellence, 2013)**

- **Familia Norma ISO/IEC 27000**

La norma ISO 27000 orientado a la *"Gestión de Seguridad de la Información"* cuenta con una extensa familia que se menciona a continuación:

- **NORMA ISO 27000**

Es un vocabulario estándar para la Gestión de Seguridad de la Información. Actualmente se encuentra en desarrollo a fin de brindar mejores alternativas en cuanto a la esquematización y metodologías de aseguramiento de la información en las entidades públicas o privadas.

- **NORMA ISO 27001**

Es la certificación que deben obtener las organizaciones. Es una norma que especifica los requisitos para la implantación del sistema de *"Gestión de Seguridad de la Información"*.

Es necesario resaltar que es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

La norma ISO 27001 se publicó como estándar internacional en octubre del 2005.

- **NORMA ISO 27002**

Es el código de buenas prácticas para la *"Gestión de Seguridad de la Información",* se fundamenta en describir los objetivos de control y controles recomendables en implementaciones de seguridad de la información.

Consta de 11 dominios con 39 objetivos de control y 133 controles. Actualmente esta norma no es certificable.

- **NORMA ISO 27003**

Son directrices para la implementación de un sistema de gestión de seguridad de la información. Al igual que la norma ISO 27002 en la actualidad no se encuentra certificada.

- **NORMA ISO 27004**

Son métricas para la gestión de seguridad de la información es la que proporciona recomendaciones de quién, cómo y cuándo realizar mediciones de seguridad de la información.

Esta norma fue publicada el 15 de diciembre de 2009. Hasta el momento no se encuentra certificada.

- **NORMA ISO 27005**

Esta norma trata la gestión de riesgos de seguridad de la información. Es la que proporciona recomendaciones, lineamientos, métodos y técnicas de evaluación de riesgos de seguridad en la información referente al soporte del proceso de gestión de riesgos de la norma ISO 27001.

Esta norma fue publicada en su primera versión el 15 de junio de 2008 y actualizada el 1 de junio de 2011. Actualmente esta norma no se encuentra certificada.

- **NORMA ISO 27006**

Esta norma específica los requisitos específicos para la certificación de un sistema de gestión de seguridad de la información y es usada en conjunto con la norma 17021.

Esta norma fue publicada en su primera versión el 1 de marzo de 2007 y actualizada el 1 de diciembre de 2011.

- **NORMA ISO 27007**

Es una guía para auditar el sistema de gestión de seguridad de la información. Actualmente se encuentra en preparación y no es certificable.

- **NORMA ISO 27799**

Es una guía para implementar las ISO 27002 en organizaciones y empresas dedicados al ámbito de la salud.

- **NORMA ISO 27031**

Permite a las organizaciones orientar en temas de Tecnologías de la Información y Comunicaciones ajustadas a la continuidad de negocios.

Esta Norma fue publicada el 1 de marzo de 2011. Actualmente esta norma no se encuentra certificada.

- **NORMA ISO 27032**

Es una guía para apoyar a las organizaciones referente a temas de seguridad cibernética, y ciberataques.

Esta norma fue publicada el 16 de julio de 2012. Actualmente esta norma no se encuentra certificada.

- **NORMA ISO 27035**

Esta norma profundiza las actividades de detección, reportes y evaluación de incidentes de seguridad de la información y sus vulnerabilidades.

2.7.5 Beneficios implementación Norma INEN ISO/IEC 27000

A continuación, se mencionarán los beneficios más importantes que trae la implantación de la ISO 27000 en las organizaciones:

- Creación de buenas prácticas referente a la *"Gestión de Seguridad de la Información"* de manera metodológica y estructurada.
- Reducción de riesgo de pérdida, robo o daño de la información que circula en las organizaciones.
- Mejora de los procesos y reducción de gastos operativos y de consultorías.
- Incremento de la satisfacción de los usuarios internos, externos y motivación de los empleados de la organización.

2.7.6 Profundización Norma INEN ISO/IEC 27002

La norma INEN ISO/IEC 27002, es profundizada en este punto debido a que es parte fundamental del presente proyecto de tesis.

Según (ISO 27000, 2012) es la norma internacional INEN ISO/IEC 27001 "mejorada" orientada a la Seguridad de la Información que cubre todo tipo de organizaciones.

Esta norma específica los requisitos para establecer, implementar, supervisar y mejorar el sistema de Seguridad de la Información. Además, es la solución de mejora continua más adecuada para evaluar los diferentes riesgos tales como: incendios, inundaciones, sabotajes, vandalismo, acceso indebido no deseados, virus informáticos, ataques de intrusión, denegación de servicio entre otros.

Esta norma nos permite establecer las estrategias y controles adecuados que aseguren una permanente protección de la información. Es importante indicar que la INEN ISO/IEC 27002, está basado bajo en concepto del Ciclo Deming "Planificar, Hacer Verificar y Actuar".

En la siguiente Figura que se muestra a continuación se representa el *"Ciclo Deming"*, en sus fases de Actuar, Planificar, Revisar, Hacer.

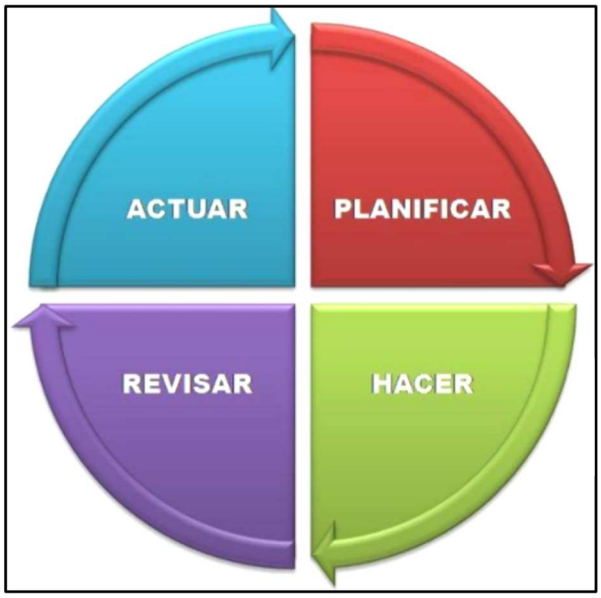


Figura 21 Ciclo Deming PHVA

Fuente: **(Metodoss.com, s.f.)**

Según (ISO 27000, 2012) actualmente, la última edición del año 2013, ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles .

En la siguiente Tabla que se expone a continuación se representa los Dominios, Objetivos de Control y Controles de la ISO 27002 de la última modificación vigente.

Tabla 3
ISO/IEC 27002:2013: Dominios, Objetivos y Controles

Dominios (14)	**Objetivos de Control (35)**	**Controles (114)**
5. POLÍTICAS DE SEGURIDAD	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información
		5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna.	6.1.1 Asignación de responsabilidades para la segur. de la información.
		6.1.2 Segregación de tareas.
		6.1.3 Contacto con las autoridades.

Continúa

		6.1.4 Contacto con grupos de interés especial
		6.1.5 Seguridad de la información en la gestión de proyectos.
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad
		6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes.
	7.2 Durante la contratación.	7.1.2 Términos y condiciones de contratación.
		7.2.1 Responsabilidades de gestión.
		7.2.2 Concienciación, educación y capacitación en seguridad de la información.
		7.2.3 Proceso disciplinario
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos.
		8.1.2 Propiedad de los activos.
		8.1.3 Uso aceptable de los activos
		8.1.4 Devolución de activos.
	8.2 Clasificación de la información	8.2.1 Directrices de clasificación.
		8.2.2 Etiquetado y manipulado de la información.
		8.2.3 Manipulación de activos.
	8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles
		8.3.2 Eliminación de soportes
		8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS	9.1 Requisitos de negocio para el control de accesos.	9.1.1 Política de control de accesos.
		9.1.2 Control de acceso a las redes y servicios asociados
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios.
		9.2.2 Gestión de los derechos de acceso asignados a usuarios.

Continúa

		9.2.3 Gestión de los derechos de acceso con privilegios especiales
		9.2.4 Gestión de información confidencial de autenticación de usuarios.
		9.2.5 Revisión de los derechos de acceso de los usuarios.
		9.2.6 Retirada o adaptación de los derechos de acceso
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación.
	9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información.
		9.4.2 Procedimientos seguros de inicio de sesión
		9.4.3 Gestión de contraseñas de usuario
		9.4.4 Uso de herramientas de administración de sistemas.
		9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.	10.1 Controles criptográficos	10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos.
		10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.	11.1 Áreas seguras.	11.1.1 Perímetro de seguridad física.
		11.1.2 Controles físicos de entrada.
		11.1.3 Seguridad de oficinas, despachos y recursos
		11.1.4 Protección contra las amenazas externas y ambientales
		11.1.5 El trabajo en áreas seguras.
		11.1.6 Áreas de acceso público, carga y descarga
	11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos
		11.2.2 Instalaciones de suministro.
		11.2.3 Seguridad del cableado

Continúa

		11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
12. SEGURIDAD EN LA OPERATIVA.	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación.
		12.1.2 Gestión de cambios.
		12.1.3 Gestión de capacidades 12.1.4 Separación de entornos de desarrollo, prueba y producción
	12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso
	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.
	12.4 Registro de actividad y supervisión.	12.4.1 Registro y gestión de eventos de actividad
		12.4.2 Protección de los registros de información
		12.4.3 Registros de actividad del administrador y operador del sistema.
		12.4.4 Sincronización de relojes.
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas.
		12.6.2 Restricciones en la instalación de software.
	12.7 Consideraciones de las auditorías	12.7.1 Controles de auditoría de los sistemas de información.

Continúa

	de los sistemas de información.	
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.
		13.1.2 Mecanismos de seguridad asociados a servicios en red.
		13.1.3 Segregación de redes.
	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información
		13.2.2 Acuerdos de intercambio
		13.2.3 Mensajería electrónica.
		13.2.4 Acuerdos de confidencialidad y secreto
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
		14.1.3 Protección de las transacciones por redes telemáticas
	14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.1 Política de desarrollo seguro de software.
		14.2.2 Procedimientos de control de cambios en los sistemas.
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
		14.2.4 Restricciones a los cambios en los paquetes de software
		14.2.5 Uso de principios de ingeniería en protección de sistemas.
		14.2.6 Seguridad en entornos de desarrollo.
		14.2.7 Externalización del desarrollo de software.
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas
		14.2.9 Pruebas de aceptación.
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en pruebas.

Continúa

15. RELACIONES CON SUMINISTRADORES.	15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores.
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros.
		15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos.
		16.1.2 Notificación de los eventos de seguridad de la información
		16.1.3 Notificación de puntos débiles de la seguridad.
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
		16.1.5 Respuesta a los incidentes de seguridad.
		16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	17.1 Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información.
		17.1.2 Implantación de la continuidad de la seguridad de la información.
		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	17.2 Redundancias	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
18. CUMPLIMIENTO.	18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.
		18.1.2 Derechos de propiedad intelectual (DPI).
		18.1.3 Protección de los registros de la organización.

Continúa

		18.1.4 Protección de datos y privacidad de la información personal.
		18.1.5 Regulación de los controles criptográficos.
	18.2 Revisiones de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información
		18.2.2 Cumplimiento de las políticas y normas de seguridad.
		18.2.3 Comprobación del cumplimiento.

Fuente: (ISO 27000, 2012)

Esta tesis adaptará la *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"* para el cumplimiento de ciertos dominios, objetivos de control y controles del *"Esquema Gubernamental de Seguridad de Información (EGSI)"* basado en la norma INEN ISO/IEC 27002.

CAPÍTULO III

3.1 Introducción

El Ministerio de Finanzas es una de las principales instituciones financieras a nivel de estado que invierte anualmente en proyectos de seguridad informática para asegurar y salvaguardar la información institucional.

Al igual que instituciones como el Banco Central, Servicio de Rentas Internas, Corporación Financiera Nacional y Banco Ecuador que su principal activo es la "información" que circula a través de en sus redes internas y externas de datos.

Esta Cartera de Estado es una entidad pública encargada de la administración del Sistema de Gestión Financiera – eSIGEF, que cuenta con varios módulos financieros como por ejemplo: eSIPREN[23], SPRYN[24], eSByE[25] y Nomina SIGEF Institucional. Estos módulos reflejan información con alto grado de confidencialidad. Los cuales no pueden ser divulgados o extraídos sin consentimiento de las autoridades y responsables de esta información.

Por la criticidad y confidencialidad de la información del "*Sistema de Gestión Financiera eSIGEF"* que circula por la red interna de datos de esta institución. La Dirección de Tecnologías y Comunicaciones DTCs, con el fin de precautelar estos datos de manera proactiva decidió emprender el proyecto para la "*Implementación de una solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la Red de Datos del Ministerio de Finanzas"*.

El contrato para la implementación de esta solución fue suscrito entre el Ministerio de Finanzas y el proveedor el 28 de enero de 2015 en la ciudad de Quito y culminado en una primera etapa (básica) el 27 de julio de 2015.

---

[23] **eSIPREN:** Sistema Presupuestario Nacional

[24] **SPRYN:** Subsistema Presupuestario de Remuneraciones y Nómina

[25] **eSByE:** Sistema de Bienes y Existencias

- **Misión**

Contribuir al cumplimiento de los objetivos de desarrollo del país y a una mejor calidad de vida para las y los ecuatorianos, a través de una eficaz definición, formulación y ejecución de la política fiscal de ingresos, gastos y financiamiento público; que garantice la sostenibilidad, estabilidad, equidad y transparencia de las finanzas públicas.

- **Visión**

En el año 2017, la entidad rectora de las finanzas públicas será reconocida a nivel nacional e internacional por su gestión de calidad, confianza, eficacia y eficiencia en la prestación de sus servicios; integrada por personas competentes y comprometidas con la ética, responsabilidad, transparencia y rendición de cuentas en beneficio de las ecuatorianas y los ecuatorianos.

- **Valores Institucionales**

Los valores y principios que sustentan la planificación estratégica del Ministerio de Finanzas constituyen pilares fundamentales de la gestión técnica del comportamiento de las personas que conforman esta Cartera de Estado:

- ✓ **Respeto**: El Ministerio de Finanzas tiene como premisa fundamental el precautelar los intereses del Estado ecuatoriano y los derechos de los ciudadanos, de sus usuarios, de sus proveedores, de su personal y de otros grupos humanos, brindando siempre los servicios públicos de su competencia con calidad, cordialidad y oportunidad.
- ✓ **Solidaridad**: Son las acciones socialmente responsables que el Ministerio de Finanzas impulsa a fin de mejorar la redistribución del ingreso y contribuir al buen vivir de las ecuatorianas y los ecuatorianos.
- ✓ **Transparencia**: Las acciones que realiza el Ministerio de Finanzas son transparentes y están al alcance de todas las ecuatorianas y ecuatorianos, para

lo cual cumple las normas de transparencia y cuenta con estrategias de comunicación adecuadas que permiten entregar información oportuna, comprensible y actualizada.

- ✓ **Honestidad e Integridad**: Este valor constituye una condición fundamental de las personas que conforman el Ministerio de Finanzas, pues garantiza una gestión transparente, confiable, orientada a la excelencia, al cumplimiento de resultados y a la rendición de cuentas, y comprometida con los principios constitucionales y del buen vivir.

- **Localidades del Ministerio de Finanzas:** El Ministerio de Finanzas del Ecuador cuenta con localidades en las ciudades de Quito, Guayaquil y Cuenca, como se referencia a continuación:

Localidad Matriz

Se encuentra ubicada en la ciudad de Quito, en la avenida 10 de agosto y Bolivia, sector La Mariscal.

El edificio matriz del esta Cartera de Estado cuenta con 575 servidores públicos a la fecha. Repartidos en las diferentes Coordinaciones, Subsecretarías y Direcciones, como se indica en la siguiente Figura de organigrama interno institucional.

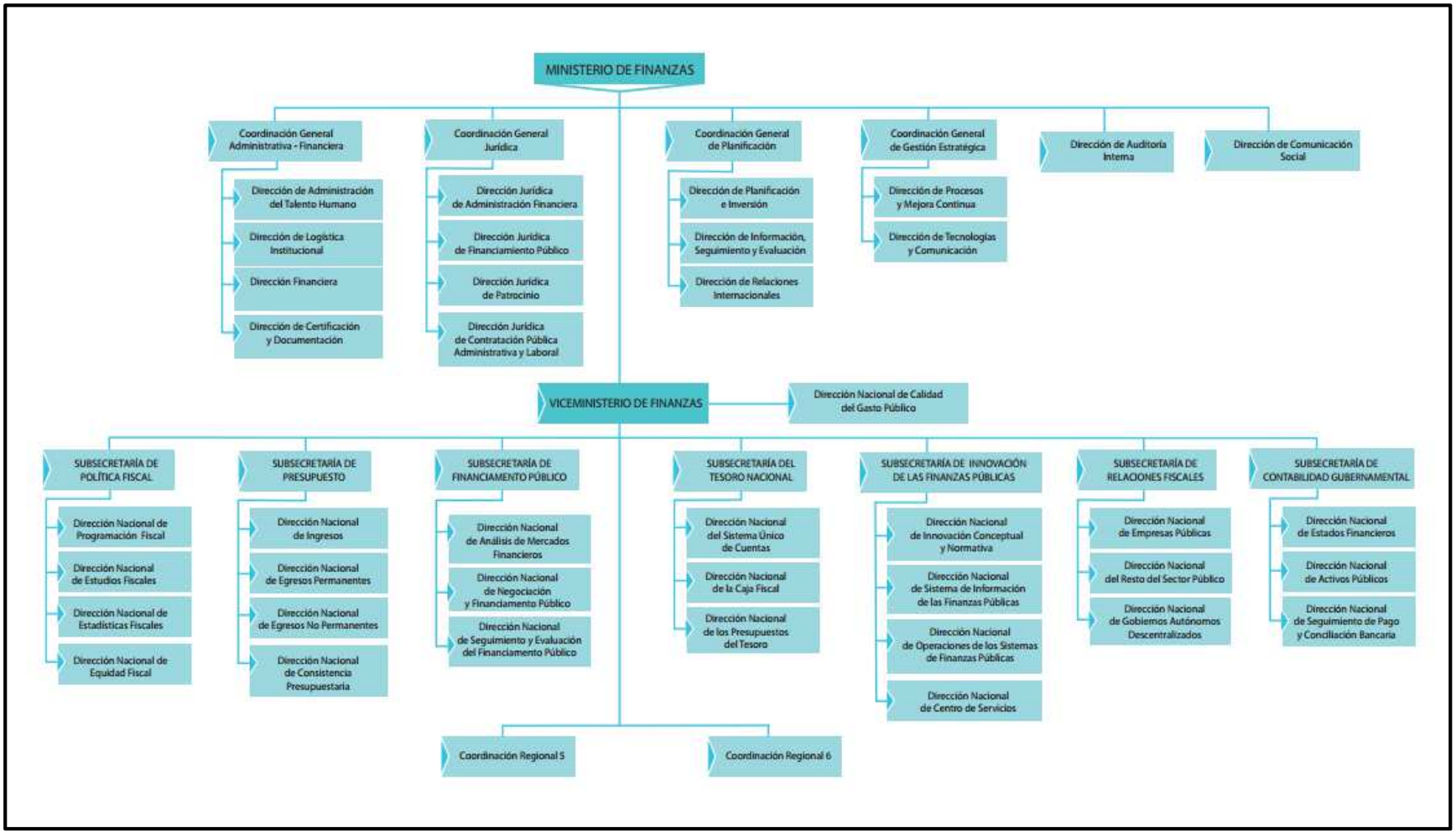


Figura 22 Organigrama del Ministerio de Finanzas

Fuente: **(Ministerio de Finanzas del Ecuador, s.f.)**

Localidad Regional 5

Se encuentra ubicada en la ciudad de Guayaquil, edificio Ex Ministerio del Litoral, avenida Francisco de Orellana, Piso 11, como se indica en la siguiente Figura.

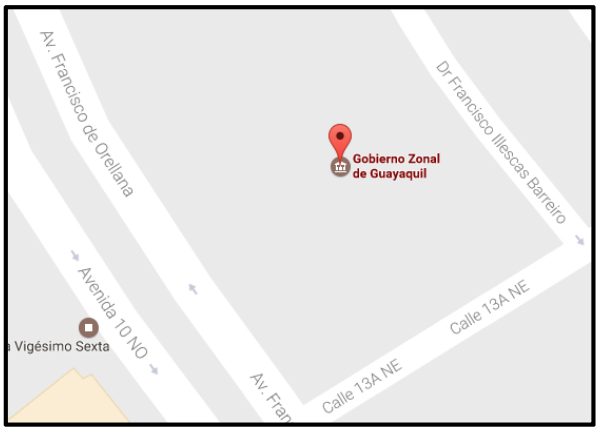


Figura 23 MINFIN Localidad Guayaquil

Fuente: **(Google, s.f.)**

Localidad Regional 6

Se encuentra ubicada en la ciudad de Cuenca, avenida México entre Unidad Nacional y avenida las Américas, edificio Ex-CREA, como se indica en la siguiente Figura.

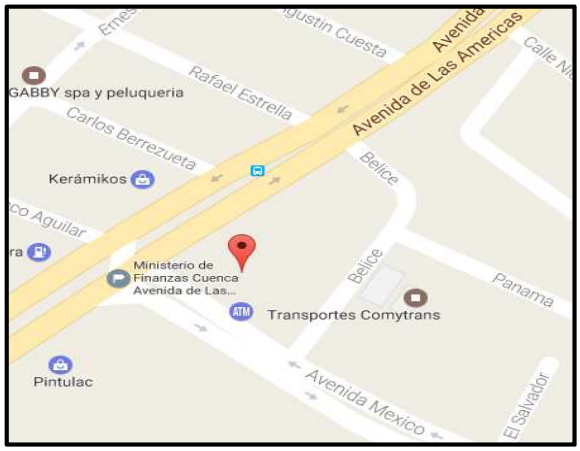


Figura 24 MINFIN Localidad Guayaquil

Fuente: **(Google, s.f.)**

3.2 Análisis de la Situación Actual de la Red de Datos MINFIN

Las autoridades y servidores públicos que laboran en las Coordinaciones Regionales 5 (Guayaquil), 6 (Cuenca) consumen todos los servicios tecnológicos del edificio matriz del Ministerio de Finanzas ubicado en la (avenida 10 de agosto y Bolivia).

Entre los servicios principales que consumen las Regionales 5 (Guayaquil), 6 (Cuenca) son correo electrónico, internet, telefonía IP y aplicativos propios internos (Sistemas de Gestión Financiera, SPRYN, eSIGEF, eByE, GLPI, y Sistemas de permisos de asistencia).

3.2.1 Topología de Red de Datos Global del MINFIN

El Ministerio de Finanzas matriz y sus sucursales de Guayaquil y Cuenca se interconectan a través de enlaces de datos con el edificio matriz (avenida 10 de agosto y Bolivia) para el consumo de servicios tecnológicos.

A continuación, se detalla la Topología de red de datos global del MINFIN, a fin de mantener ideas claras y aterrizadas de los segmentos de red críticos que se mejoraran con el afinamiento de la *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"*.

Es importante mencionar que no se puede mostrar el direccionamiento IP real en la Topología de red de datos global del MINFIN que a continuación se expone. Debido a normas de confidencialidad y seguridad informática de esta Cartera de Estado.

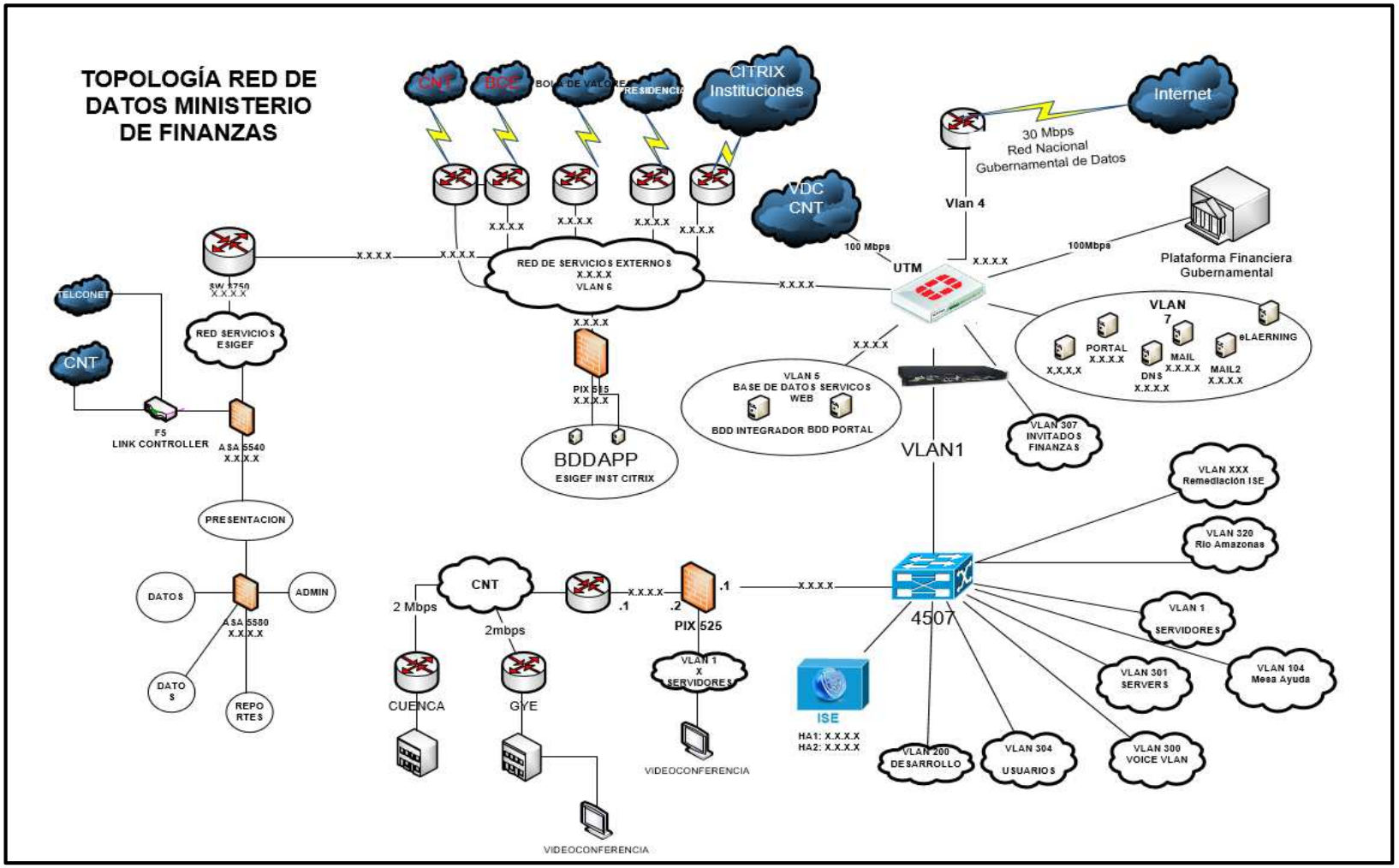


Figura 25 Topología Global de la Red de Datos del MINFIN

3.2.2 Direccionamiento IP de la Red de Datos del MINFIN

El Ministerio de Finanzas cuenta con dos redes compartidas dentro de la misma institución.

La primera red de datos denominada "Red interna MINFIN" es la usada a nivel interno por todos los funcionarios institucionales.

La segunda red de datos denominada "Red de Producción" de igual forma es usada a nivel interno por los funcionarios institucionales y además es usada por todos los funcionarios públicos a nivel nacional del *"Sistema de Gestión Financiera eSIGEF"*

Por motivos de confidencialidad y en cumplimiento del acuerdo No. 166 del *"Esquema Gubernamental de Seguridad de Información (EGSI)"* basado en la norma INEN ISO/IEC 27002, según dominio *"13. Seguridad en las Telecomunicaciones"* y control de dominio *"(…) 13.2 Gestión de la Seguridad en las Redes"* que indica *"(…) 13.2.4 Acuerdos de Confidencialidad y Secreto"*. Se utilizará direccionamiento no oficial para describir la red de datos denominada *"Red interna MINFIN"* con fin de facilitar el entendimiento y comprensión del presente trabajo de tesis.

En la siguiente Tabla se expone la distribución del direccionamiento IP de la *"Red interna MINFIN"* del esta Cartera de Estado.

Tabla 4
Direccionamiento LAN – MINFIN

Nombre Segmento	Id. Vlan	Direccionamiento	Observaciones
Usuarios_finanzas	304	10.10.0.0/16	Usuarios Generales MINFIN
Desarrolladores	200	10.11.11.0/24	Usuarios desarrolladores.
Telefonía_IP	300	10.12.0.0/16	Registro teléfonos IP.
Servidores	301	10.13.0.0/16	Servidores_MINFIN.
Mesa de Ayuda	104	10.14.14.0/24	Mesa de ayuda eSIGEF
Impresoras	1	10.20.0.0/16	Usada para impresoras y dispositivos IP.

Continúa

Remediacion_ISE	309	10.9.0.0/16	Para dispositivos que no cumplen las políticas de la institucionales
Regional 5 (Guayaquil)	220	10.20.20.0/16	Para funcionarios de la sucursal de Guayaquil.
Regional 6 (Cuenca)	221	10.30.30.0/16	Para usuarios sucursal de Cuenca.
PFG_Minfin	100	10.16.0.0/16	Para usuarios de la Plataforma Financiera Gubernamental.
DMZ	7	10.15.15.0/16	Servidores aislados y dispositivos de invitados.

3.2.3 Topología de Interconexión MINFIN Quito – Guayaquil

El Ministerio de Finanzas se interconecta a través de un enlace de datos con disponibilidad de servicio de 99.8% es decir con un enlace primario y alterno.

Esta Cartera de Estado mantiene un contrato para la provisión de este servicio con la Corporación Nacional de Telecomunicaciones CNT – EP.

Mediante estos enlaces de comunicación los administradores de servicios del área de infraestructura ubicados en la *"Red interna MINFIN"* del edificio matriz de la ciudad de Quito, pueden comunicarse con la infraestructura de la ciudad de Guayaquil.

A continuación, se expone la Figura de interconexión de las dos sucursales Quito - Guayaquil del Ministerio de Finanzas.

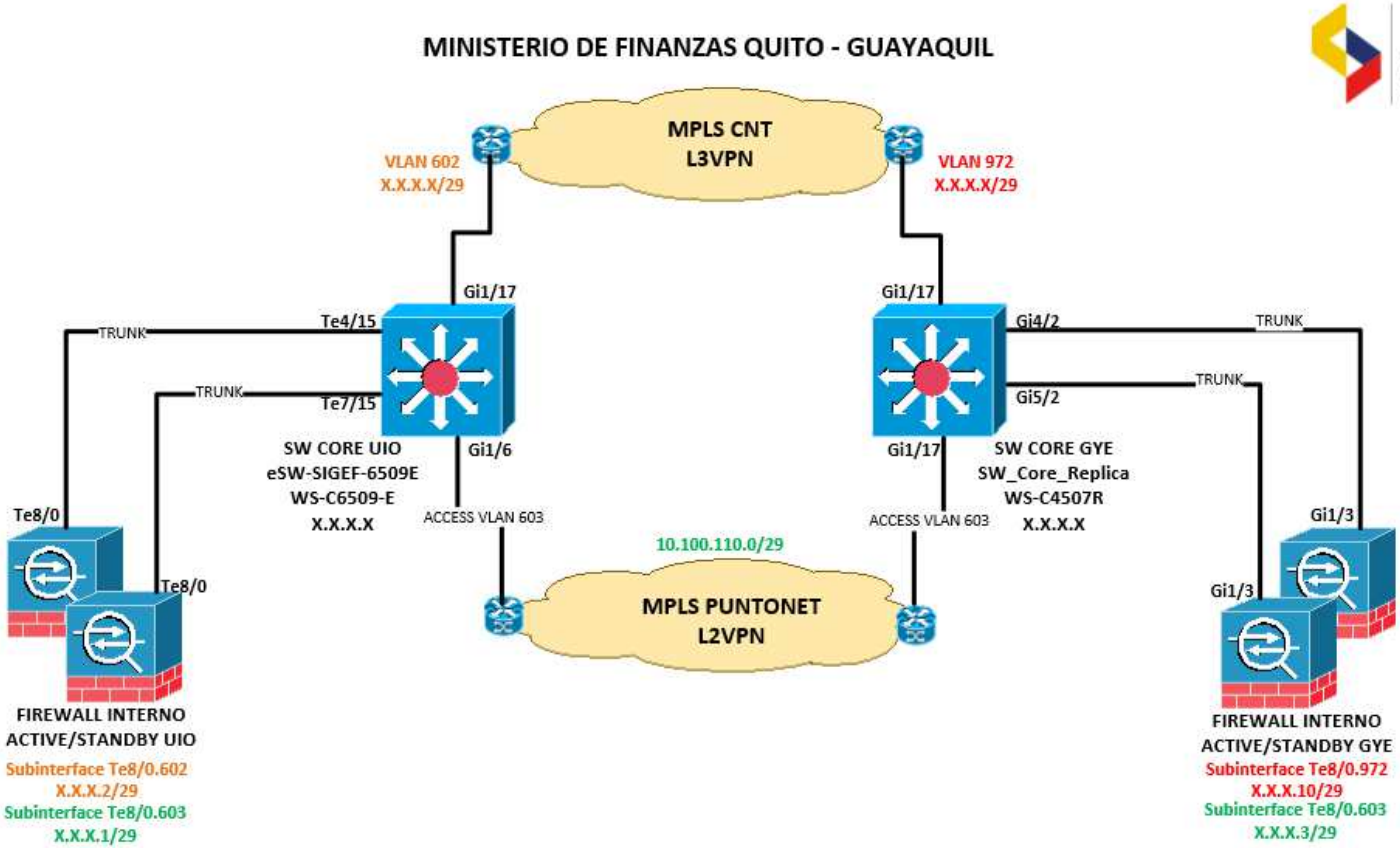


Figura 26 Interconexión MINFIN Quito – Guayaquil

3.2.4 Topología Red de Producción del MINFIN

La segunda red de datos denominada *"Red de Producción"* es la encargada de alojar varios sistemas de fundamentales de negocio del MINFIN.

Estos sistemas son: eSIGEF (Sistema de Gestión Financiera), eSIPREN (Sistema de presupuestos y nóminas), SPRYN (Sistema de presupuestos y nóminas WEB), eSByE (Sistema de bienes y existencias) y eSIGEF Institucional.

En la siguiente Figura se muestra la pantalla inicial de los Sistemas de Gestión Financiera eSIGEF que la *"Red de Producción"* expone a nivel nacional.

Figura 27 Pantalla de inicio eSIGEF

Fuente: **(Ministerio de Finanzas, s.f.)**

En la Figura que se muestra a continuación, se expone la arquitectura de *"Red de Producción"* de esta Cartera de Estado.

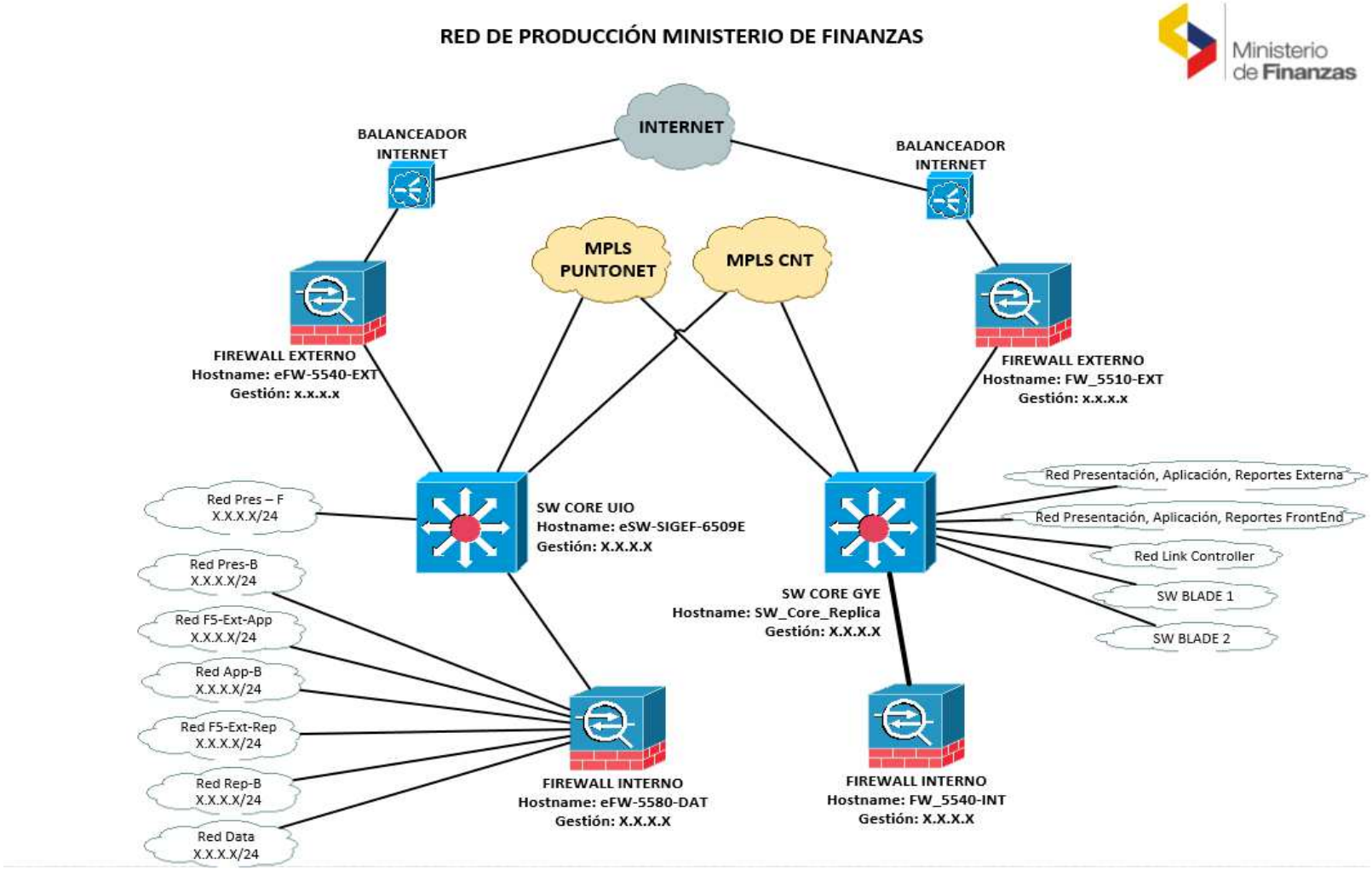


Figura 28 Red de producción Ministerio de Finanzas

3.2.5 Conexiones MINFIN con otras Instituciones Públicas

Esta Cartera de Estado mantiene conexiones punto a punto con otras instituciones a nivel de estado. Con el fin de garantizar la continuidad de servicios entre instituciones públicas y proteger el intercambio de información sensible que manejan entre entidades.

Además, para el cumplimiento del acuerdo No. 166 del *"Esquema Gubernamental de Seguridad de Información (EGSI)"* basado en la norma INEN ISO/IEC 27002, según dominio *"13. Seguridad en las Telecomunicaciones"* y control de dominio *"(…) 13.2 Intercambio de Información con partes externas"* que indica *"(…) 13.2.2 Acuerdos de intercambio."*

Entre los enlaces de interconexión más importantes y sensibles que mantiene el MINFIN con otras entidades es con El Banco Central del Ecuador y el Anillo de Fibra Óptica Interministerial.

3.2.6 Interconexión MINFIN y Banco Central del Ecuador BCE

La Subsecretaria de Tesorería de la Nación del MINFIN, es la encargada de intercambiar información sensible y confidencial con el Banco Central del Ecuador. con fin de efectuar transacciones de sueldos a funcionarios públicos, pagos a proveedores, pagos al exterior, pago de viáticos y una variedad de servicios correspondientes de entidades públicas.

Todas estas transacciones son efectuadas a través de un enlace punto a punto entre el MINFIN y BCE. Este servicio es provisto por la Corporación Nacional de Telecomunicaciones CNT – EP.

En la siguiente Figura se expone la interconexión física - lógica entre el MINFIN y el Banco Central del Ecuador.

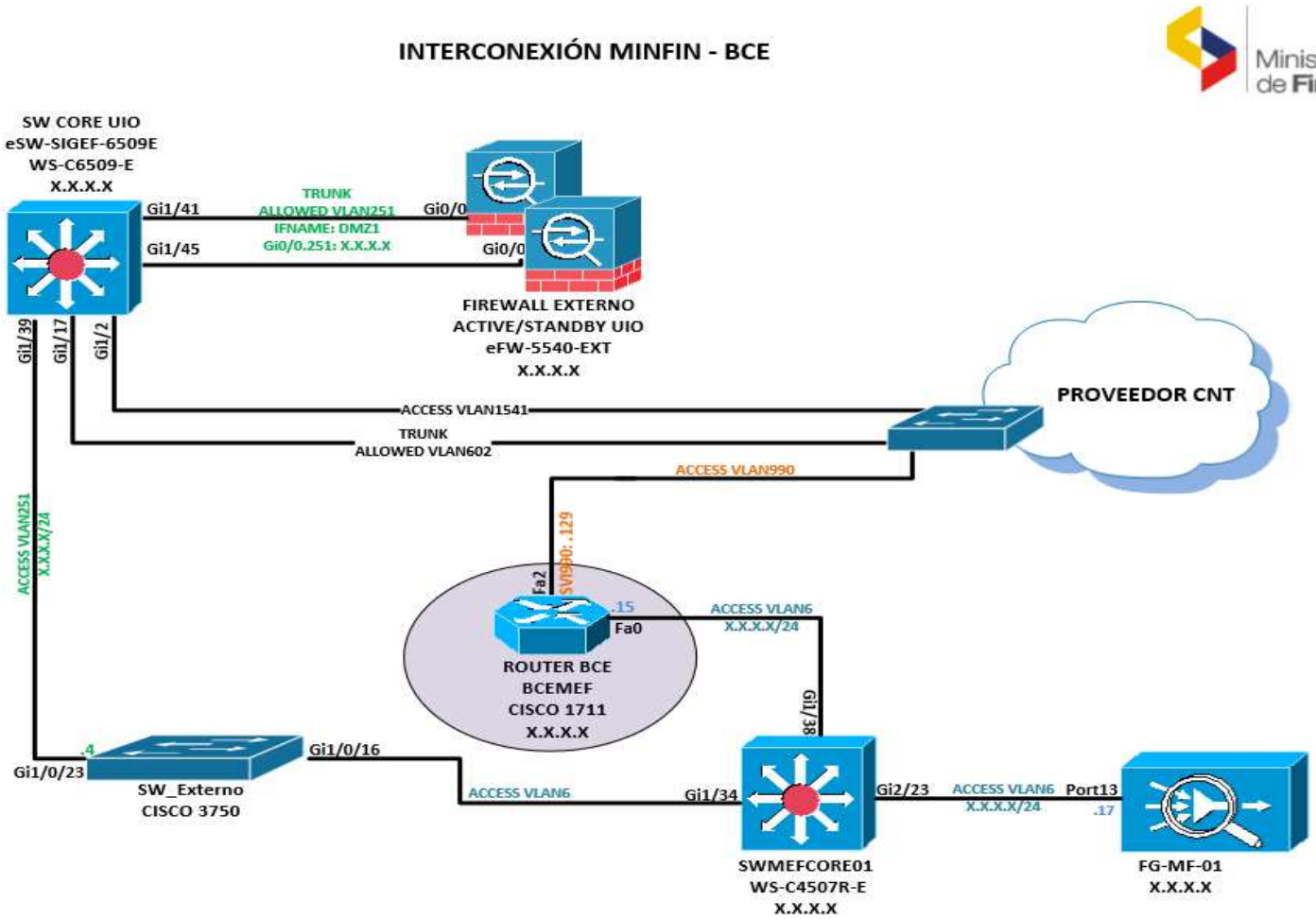


Figura 29 Diagrama de Red Interconexión MINFIN - BCE

3.2.7 Interconexión MINFIN y Anillo de Fibra Óptica Interministerial

Esta Cartera de Estado forma parte de la red de datos segura denominada *"Anillo de Fibra Óptica Interministerial*".

A través de esta red de datos *"Anillo de Fibra Óptica Interministerial*" todas las entidades públicas intercambian información sensible y confidencial. Con el fin de que ninguna amenaza externa pueda interceptar o vulnerar la información que circula por esta red de datos.

A continuación, se indica el direccionamiento IP de las entidades que intercambian información con esta institución.

Tabla 5
Direccionamiento IP "Anillo de Fibra Óptica Interministerial"

Institución	Direccionamiento IP	Servicios
Secretaría Nacional de Administración Pública SNAP	10.80.12.x/24	Gobierno por Resultados GPR y Gestión Documental QUIPUX
Corporación Nacional de Telecomunicaciones CNT	10.80.36.x/24	Facturación electrónica
Registro Civil	10.80.15.x/24	Base de datos ciudadanía
Instituto Ecuatoriano de Seguridad Social IESS	10.80.25.x/24	Servicios Generales
Correos del Ecuador	10.80.17.0/24	Pagos al Exterior
Banco de Desarrollo del Ecuador BDE	10.80.12.x/16	Módulos de Presupuesto
Servicio de Rentas Internas	10.80.42.x/24	Facturación Electrónica y declaraciones tributarias
Servicio Nacional de Aduanas del Ecuador SENAE	10.80.14.x/24	Tributación Aduanera

En la siguiente Figura se expone el diagrama de red del segmento IP 10.80.128.x/16 *"Anillo de Fibra Óptica Interministerial*".

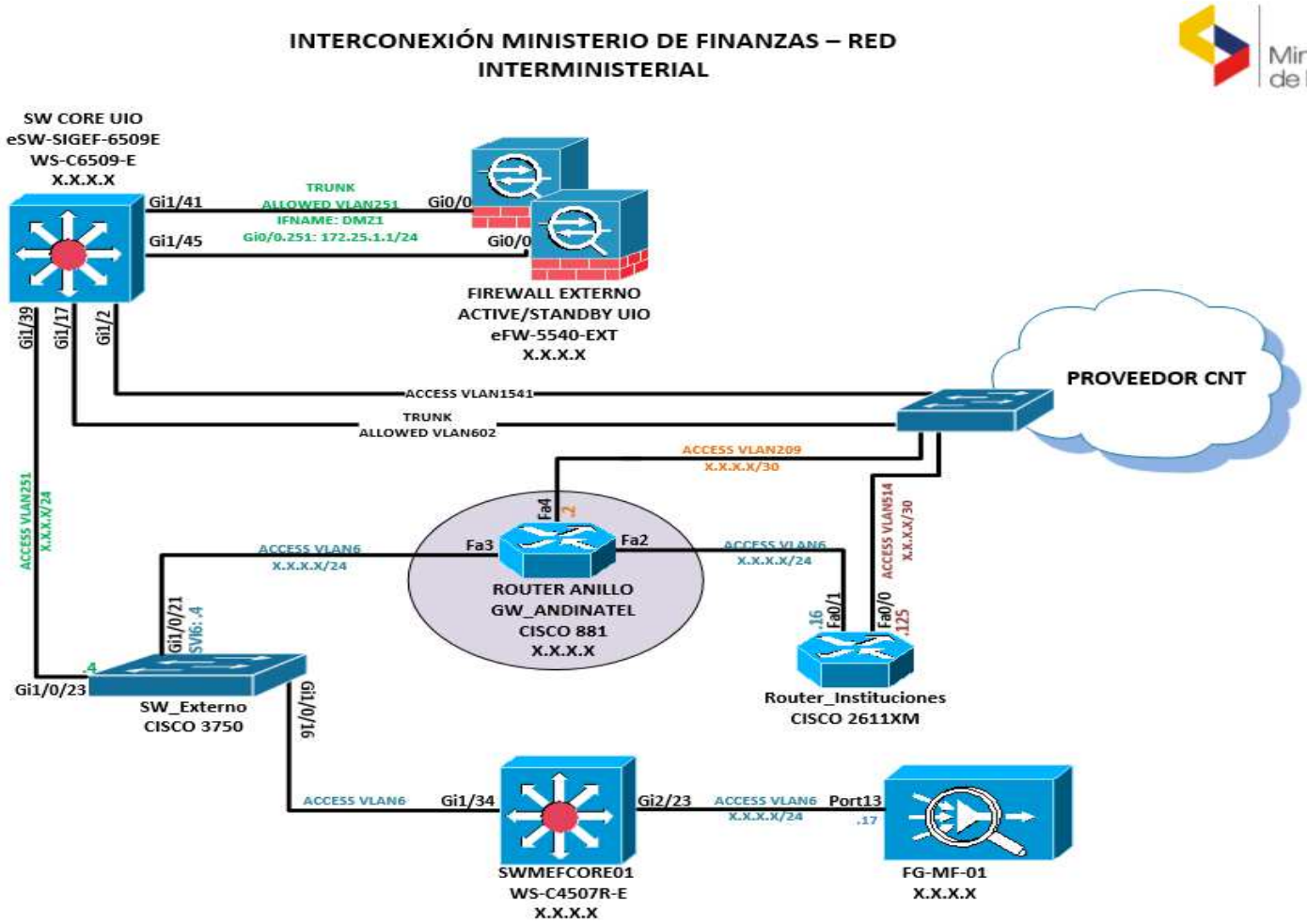


Figura 30 Interconexión MINFIN- Red Interministerial

3.2.8 Levantamiento Información Equipos de Comunicación Red interna

La matriz de esta Cartera de Estado como se indicó anteriormente se encuentra ubicada en la Avenida 10 de agosto y Bolivia “Sector la Mariscal”.

Esta edificación consta de una planta baja, mezzanine y 5 pisos. En el primer piso se encuentra el Data Center[26] principal, donde se encuentra los servidores necesarios para el funcionamiento del *“Sistema de Gestión Financiera eSIGEF”*.

Además en el Data Center principal de esta Cartera de Estado se encuentran servidores, switches[27] core, distribución, controladora inalámbrica WLC[28], central telefónica, routers[29], firewalls[30], UTM[31] y otros equipos.

Los equipos de comunicación de cada piso se interconectan a través de fibra óptica al “switch de distribución” ubicado en el Data Center del primer piso. Estos equipos se interconectan con el equipo central de comunicaciones “switch de core”. Con el fin de obtener una estructura de red de comunicaciones organizada y jerarquita, obedeciendo las mejores prácticas y recomendaciones realizadas por los fabricantes líderes en comunicaciones a nivel mundial.

En la Figura que se expone a continuación se indica la estructura de una red de datos jerárquica. Tomada como ejemplo para especificar la distribución de la red de datos de esta Cartera de Estado.

---

[26] **DATA CENTER:** CUARTO CENTRAL DE PROCESAMIENTO DE INFORMACIÓN.

[27] **SWITCH:** ES UN EQUIPO INTELIGENTE DE DISTRIBUCIÓN DE ENTRADA Y SALIDA DE PAQUETES

[28] **WLC**: WIRELESS LAN CONTROLLER.

[29] **ROUTER:** EQUIPO INTELIGENTE QUE ENCAMINE PAQUETES Y COMUNICA REDES.

[30] **FIREWALL:** SOFTWARE O HARDWARE QUE PERMITE O DENIEGA EL ACCESO A REDES DE DATOS.

[31] **UTM**: GESTIÓN UNIFICADA DE AMENAZAS, INTEGRA VARIOS SERVICIOS EN UNO SOLO POR EJEMPLO FIREWALL, FILTRADO WEB, FILTRADO DE APLICACIONES ETC.

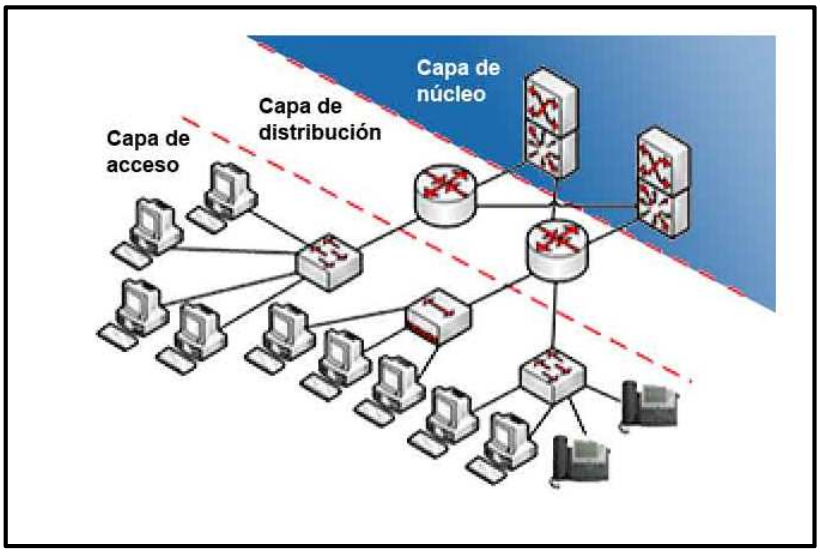


Figura 31 Distribución de una Red de Datos Jerárquica

Fuente: **(Valdés, 2015)**

- **Equipos de Interconexión para la Red de Datos MINFIN**

En la Tabla que se expone a continuación se efectúa un inventario de todos los equipos de comunicaciones de esta Cartera de Estado ubicados en el edificio matriz Avenida 10 de agosto y Bolivia "Sector la Mariscal" y las sucursales Regional 5 (Guayaquil), Regional 6 (Cuenca).

Tabla 6
Inventario Equipos de Comunicaciones MINFIN y Regionales

Piso	Nombre del equipo	Cantidad	Marca	Modelo
Planta Baja	Switch Acceso	2	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Access Points	1	Cisco	AIR-LAP1261N-A-K9
Mezzanine	Switch Acceso	2	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Switch Acceso	2	Cisco	C2960S-UNIVERSALK9-M, Versión 12.2(55)SE2
	Access Points	3	Cisco	AIR-LAP1142N-A-K9
Primer Piso	SwitchCore	1	Cisco	Catalyst 4500 L3

Continúa

	Switch Distribución	1	Cisco	C3750E-UNIVERSALK9-M
	Switch Acceso	1	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Access Points	3	Cisco	AIR-LAP1142N-A-K9
	Controlador Inalámbrica WLC	1	Cisco	Cisco 5500 Series
	Central Telefónica IP	2	Cisco	ST9146803SS
	UTM	2	Fortigate	600C
	Administrador Ancho de Banda	2	Allot	AC-504
	Firewall ASA	2	Cisco	5540
Segundo Piso	Switch Acceso	4	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Switch Acceso	3	Cisco	C2960S-UNIVERSALK9-M, Versión 12.2(55)SE2
	Access Points	3	Cisco	AIR-LAP1142N-A-K9
Tercer Piso	Switch Acceso	3	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Switch Acceso	1	Cisco	C2960-LANBASE-M
	Access Points	3	Cisco	AIR-LAP1142N-A-K9
Cuarto Piso	Switch Acceso	3	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Switch Acceso	1	Cisco	C2960-LANBASE-M
	Access Points	5	Cisco	AIR-LAP1142N-A-K9
Quinto Piso	Switch Acceso	1	Cisco	C2960X-UNIVERSALK9-M, Versión 15.0(2)EX3
	Switch Acceso	3	Cisco	C2960-LANBASE-M
	Access Points	4	Cisco	AIR-LAP1142N-A-K9
Regional 5 (Guayaquil)	Switch Acceso	2	Cisco	C2960-LANBASE-M
	Access Points	1	Cisco	AIR-LAP1142N-A-K9
Regional 6 (Cuenca)	Switch Acceso	1	Cisco	C2960-LANBASE-M
	Access Points	1	Cisco	AIR-LAP1142N-A-K9

En la siguiente Figura se diagrama las conexiones lógicas con los diferentes equipos de comunicación de esta Cartera de Estado.

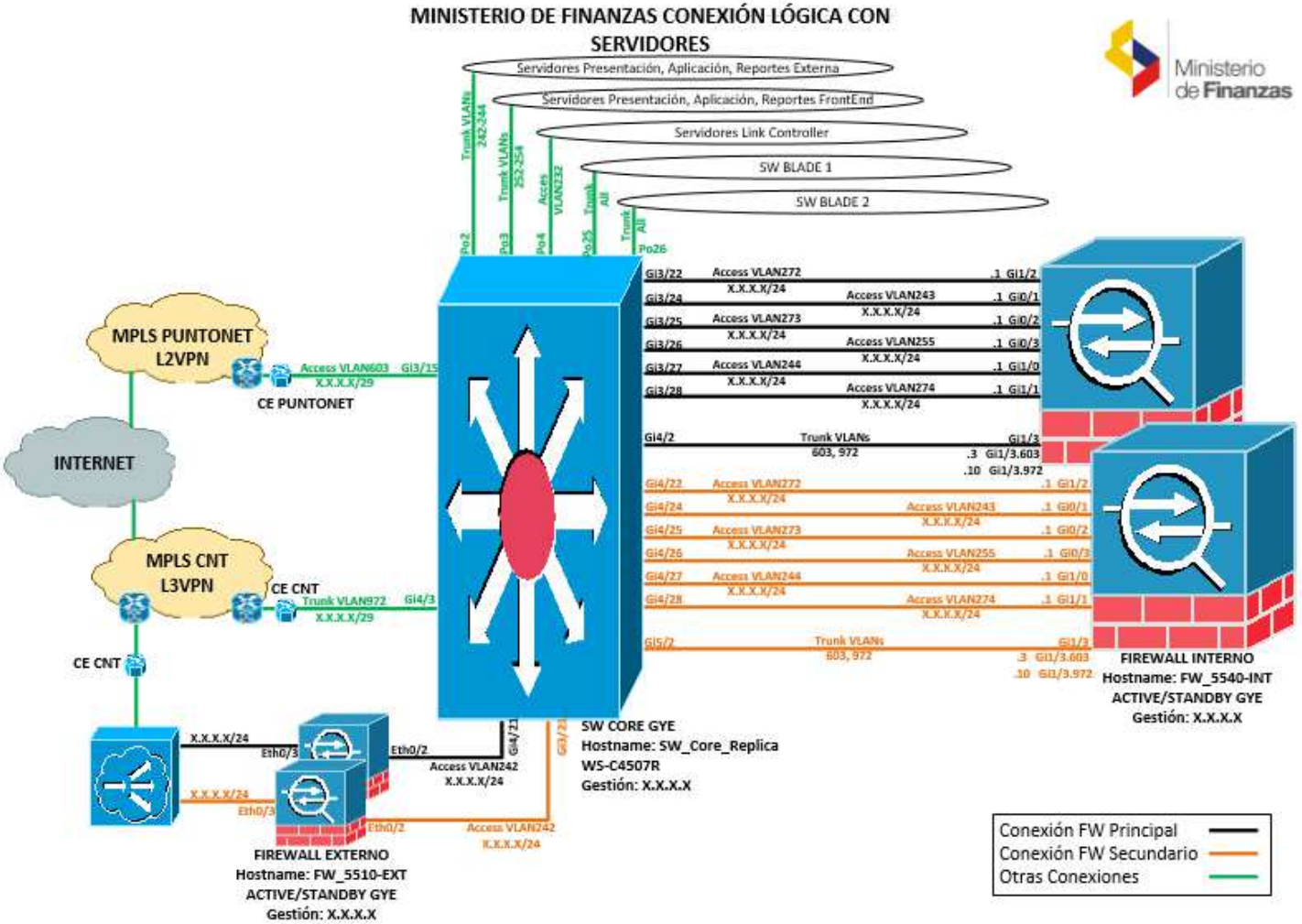


Figura 32 Conexiones de Servidores con equipos de comunicaciones

- **Cantidad de Usuarios en las Dependencias del MINFIN**

Con fecha 22 de junio de 2017, esta Cartera de Estado cuenta con 575 servidores públicos y en crecimiento.

Los servidores públicos de esta Cartera de Estado se encuentran distribuidos en diferentes dependencias como: Despachos, Coordinaciones, Subsecretarias, Direcciones, Regionales y Procesos.

En la siguiente Tabla se expresa la cantidad de servidores públicos incluidos jerárquico superior distribuidos por dependencias.

Tabla 7
Cantidad de Servidores Públicos por Dependencia

Dependencia	**Número de usuarios**
Despacho Ministerial	40
Despacho Viceministro	34
Coordinación General Administrativa Financiera	56
Coordinación de Gestión Estratégica y Planificación	60
Coordinación General Jurídica	54
Coordinación Regional 5	15
Coordinación Regional 6	8
Subsecretaría del Tesoro Nacional	54
Subsecretaría de Presupuesto	75
Subsecretaría de Contabilidad Gubernamental	59
Subsecretaría de Financiamiento Publico	36
Subsecretaria de Relaciones Fiscales	34
Subsecretaria de Innovación de las Finanzas Publicas	50
Total	575

3.2.9 Parque informático del MINFIN

Esta Cartera de Estado, cuenta con un parque informático muy amplio tanto en hardware y software. Necesarios para la ejecución de las actividades diarias de los servidores públicos de esta institución.

Es indispensable para las configuraciones del presente trabajo de tesis el inventario de las versiones de sistemas operativos y services pack que poseen los computadores de escritorio, portátiles y thin clients de esta institución. Debido que el mejoramiento de la *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"* ejecutará la característica de "Postura" y "análisis de requisitos mínimos" para ingreso a la red de datos institucional.

En la Tabla que se muestra a continuación, se expone el inventario de versionamiento de sistemas operativos y services pack instalados en los computadores de escritorio, portátiles y thin clients que usan actualmente los servidores públicos de esta Cartera de Estado.

Tabla 8
Inventario Sistemas Operativos computadores MINFIN

Sistema Operativo/Modelo	Sin SP[32]	SP 1	SP 2	SP 3	Id. SP	Total General
Microsoft Windows 7 Professional	6	259			15	280
HP 6000		6				6
HP 6001	6	8				14
|HP 6002		1				1
All Series		6			2	8
DB85FL		4				4
HP Compaq 6000 Pro MT PC		1				1
HP Compaq 6000 Pro SFF PC		61			2	63

Continúa

[32] **SP.:** ABREVIATURA USADA PARA SERVICE PACK DE MICROSOFT

HP Compaq dc5100 MT(PM213AV)		5				5
HP Compaq dc5750 Microtower		30			1	31
HP Compaq dc5800 Microtower		1				1
HP Compaq dc5800 Small Form Factor		18				18
HP Compaq dc7800p Small Form Factor		1				1
HP Compaq Pro 6300 MT		40			8	48
HP Compaq Pro 6300 SFF		36			1	37
HP dx2000 MT (PP826A)		4				4
HP ProDesk 400 G1 MT		22			1	23
MS-7788		2				2
OptiPlex 740		3				3
OptiPlex 745		7				7
OptiPlex GX620		2				2
OptiPlex GX621		1				1
Microsoft Windows 7 Ultimate		1				1
HP Compaq Pro 6300 MT		1				1
Microsoft Windows 8 Pro	13					13
10A90014LS	11					11
HP Compaq Pro 6300 SFF	1					1
M93p Desktop (ThinkCentre) 10A90014LS	1					1
Microsoft Windows 8.1 Pro	19				2	21
10A90014LS	1					1
HP Compaq Pro 6300	1					1
HP Compaq Pro 6300 MT	1				1	2
HP Compaq Pro 6300 SFF	10				1	11
HP ProDesk 600 G1 TWR	6					6
Microsoft Windows XP Professional		65	2	170	23	260
HP Compaq 6000 Pro SXF PC		65			8	73
HP Compaq 6000 Pro MT PC				3		3
HP Compaq 6000 Pro SFF PC				69		69
HP Compaq dc5100 MT(PM213AV)				4	2	6

Continúa

HP Compaq dc5750 Microtower				34	10	44
HP Compaq dc5750 Small Form Factor				1		1
HP Compaq dc5800 Small Form Factor				15		15
HP Compaq dc7700 Ultra-slim Desktop			1	12		13
HP Compaq dc7800p Small Form Factor				2		2
HP Compaq dx2300 Microtower				2		2
HP dx2000 MT (PP826A)				15	2	17
HP Pro 3130 Microtower PC			1			1
OptiPlex 745				7		7
OptiPlex GX260				2		2
OptiPlex GX280				1		1
OptiPlex GX620				3	1	4
Total general	**38**	**325**	**2**	**170**	**40**	**575**

- **Dispositivos de Voz IP**

El Ministerio de Finanzas posee una gran diversidad de modelos de teléfonos IP marca “Cisco”.

Estos dispositivos se encuentran instalados en cada estación de trabajo de los servidores públicos de esta Cartera de Estado. Para apoyar el correcto cumplimiento y desempeño de las actividades diarias de los funcionarios de esta institución.

En la Tabla que se muestra a continuación, se expone la cantidad y modelos de teléfonos IP que actualmente ocupan los servidores públicos de esta Cartera de Estado. Es importante mencionar que estos dispositivos mediante la característica de *“Perfilamiento”* del equipo *“Identity Service Engine - ISE”* direccionará automáticamente a la VLAN 300 de voz.

Tabla 9
Modelos Teléfonos IP – MINFIN

Modelos	Cantidades
Cisco 6921	455
Cisco 7821	3
Cisco 7925	4
Cisco 7942	62
Cisco 7961G-GE	1
Cisco 7962	28
Cisco E20	11
Cisco IP Communicator	3
Cisco 6922	7
Cisco 7963	1
Total general	575

3.2.10 Limitación Actual de la Solución de ISE en la Red de Datos del MINFIN

Esta Cartera de Estado en la actualidad cuenta con una *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"* basada en la tecnología Identity Service Engine de Cisco Systems.

En la Tabla que se expone a continuación se indica las limitaciones actuales que la "*Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas*" presenta en la red de datos institución.

Tabla 10
Limitantes actuales Cisco ISE – MINFIN

Característica actual	Limitante
Remediación	Parcialmente implementada en la VLAN 104 (Mesa de Ayuda) y VLAN 300 (telefonía_IP)
Profiling (Perfil de Usuario)	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
Postura (Escaneo de políticas)	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda
Servicios AAA Autenticación, Autorización y Contabilización	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
Portal de Invitados alámbrica e inalámbrica	No implementado

Continúa

Control de dispositivos móviles	No implementado
Administración de Dispositivos Móviles MDM	No implementado
Integración con Directorio Activo de Windows	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
TrustSec	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
Reportería	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
Monitoreo	Parcialmente implementada en dispositivos de la VLAN 104 (Mesa de Ayuda)
BYOD Bring your Own Device	No implementado
Integración WLC Wireless LAN Controller	No implementado

3.3 DESARROLLO DE LA METODOLOGÍA PMP PARA EL MEJORAMIENTO Y GESTIÓN DE LA SOLUCIÓN CISCO ISE - MINFIN

Parar el *"Mejoramiento de la Solución Cisco ISE - MINFIN"* vamos a usar y seguir las recomendaciones básicas de la metodología básica PMP[33] para la "Administración de Proyectos de manera Profesional" por las siguientes razones:

Esta metodología permite al líder de proyecto, usar las mejores recomendaciones estandarizadas internacionalmente. A fin de obtener una mayor eficacia y eficiencia en el resultado final del proyecto.

En el trabajo de tesis planteado para el *"Mejoramiento de la Solución Cisco ISE – MINFIN"*, usaremos las actividades básicas de PMP como son: inicio, planificación, ejecución y cierre.

En la Figura que se muestra a continuación se expresa la metodología PMP básica usada para el *"Mejoramiento de la Solución Cisco ISE – MINFIN"*.

[33] **PMP:** ADMINISTRACIÓN PROFESIONAL DE PROYECTOS, FUNDADA EN 1969 POR EMPRESAS USA INTERESADAS.

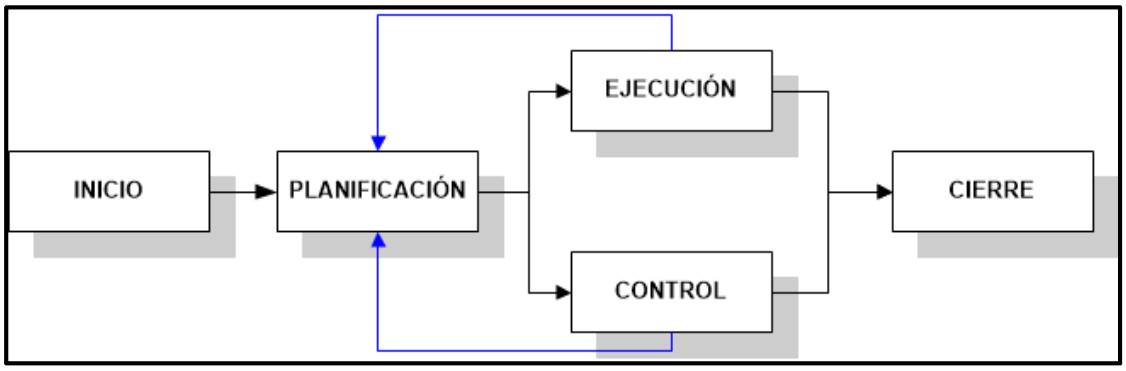


Figura 33 Etapas administración de proyectos básicas PMP

Fuente: **(SAT, 2013)**

3.3.1 ETAPA DE INICIO

3.3.1.1 Levantamiento de Información

La Solución de Cisco ISE actualmente implementada en la red da datos de esta Cartera de Estado, ha contribuido exponencialmente al control de acceso y cumplimiento de políticas de los dispositivos que se conectan únicamente al segmento de red 104 (Mesa de Ayuda).

Dejando a un lado la protección de varios segmentos de red críticos para el MINFIN como son: VLAN 200 (Desarrolladores), VLAN304 (Usuarios Generales), VLAN 1 (Impresoras, cámaras, lectoras) y VLAN 307 (Invitados Finanzas).

El mejoramiento de la *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA"* que plantea el presente trabajo de tesis. Consiste en integrar dentro de la solución de *"Cisco ISE"* los segmentos de red no protegidos de esta Cartera de Estado.

Mediante la actualización de las versiones de *NADs (Network Access Devices)*, reconfiguraciones de características de Control de Acceso, Postura, Remediación, Profiling y Servicios AAA (Autenticación, Autorización y Contabilización).

A fin de controlar, unificar, centralizar y tener mayor visibilidad de todos los dispositivos cableados e inalámbricos que ingresan a la red de datos (producción) de esta Cartera de Estado. Con el fin de aprovechar al máximo las características que brinda esta solución que aún no han sido explotada a su máximo potencial.

- **Requisitos para el Mejoramiento de la Solución de Cisco ISE – MINFIN**

La solución de *"Cisco ISE - MINFIN"*, integra *NADs (Network Access Devices)* equipos de acceso a la red como son: WLC Wireless LAN Controller (acceso inalámbrico) y switches de acceso capa 2 (acceso cableado). Que interactúan para comunicarse con los dispositivos finales de usuarios (thin clients, teléfonos IP, computadores de escritorio, portátiles, smartphones, celulares, impresoras, lectores biométricos) y una gran variedad de dispositivos de red.

- **Compatibilidad NADs (Network Access Devices) con Cisco ISE - MINFIN**

Como antecedente se debe mencionar que esta Cartera de Estado, con el afán de mejorar y estandarizar todos sus equipos internos de comunicaciones NADs (Network Access Devices), firmó el contrato para la "Adquisición de Siete Switches de Acceso para Fortalecer la Red Interna de Datos del Ministerio de Finanzas" el 4 de septiembre de 2015, bajo el proceso SIE-MF-021-2015.

Con esta adquisición se reemplazaron switches obsoletos para brindar mayor flexibilidad de administración, velocidad de transmisión de datos y principalmente seguridad al usuario final. Con el fin de poder integrar estos switches a la *"Solución de Cisco ISE del Ministerio de Finanzas"*.

En la siguiente Tabla se mencionan los modelos y versiones de NADs, compatibles con la *"Solución Cisco ISE"* versión 1.2.1.198, actualmente vigente en esta institución.

Tabla 11
Compatibilidad modelos y IOS switches

Dispositivo Compatible	Versión mínima para integración con Cisco ISE
Catalyst 2960, ISR Ethernet Switch ES2 (Catalyst 2960-S, Catalyst 2960-C LAN Base)	IOS v 12.2(55)-SE3
Catalyst 2960-SF, Catalyst 2960Plus	IOS v 15.0.2-SE (ED) LAN BASE
Catalyst 2960–XR, Catalyst 2960–X	IOS v 15.0.2-EX3 (ED)

Fuente: (Cisco, 2016)

Esta Cartera de Estado cuenta con switches Cisco de los modelos: Catalyst 2960, 2960S, 2960-SF, 2960X. Varios de estos equipos, según levantamiento de información Tabla 6. "*Inventario Equipos de Comunicaciones MINFIN y Regionales*" necesitan actualización de su sistema operativo IOS, para soportar la integración con *"Cisco ISE versión 1.2.1.198"*

En la Tabla que se expone a continuación, se detallan los equipos (switches) que se actualizaron a la versión compatible, para la correcta integración con la solución "*Cisco ISE versión 1.2.1.198*" que actualmente posee esta institución.

Tabla 12
Afinamiento NADs para integración con Cisco ISE

TIPO DE EQUIPO	IP DE ADMIN	SISTEMA OPERATIVO (IOS) ANTIGUO	SISTEMA OPERATIVO (IOS) ACTUALIZADO	MODELO
Switch distribución	10.1.250.2	12.2(50)SE3	12.2(55)SE10	WS-C3750E-48TD
Switch Core	10.1.250.9	12.2(35)SE5	12.2(55)SE10	WS-C2960G-24TC-L
Switch Core	10.1.250.10	12.2(25)SEE2	12.2(55)SE10	WS-C3750G-48TS
Switch Acceso primer piso	10.1.250.11	12.2(55)SE2	15.0(2)SE6	WS-C2960S-48LPS-L
Switch Acceso Mesa de Ayuda 1	10.1.250.12	15.0(2)EX3	15.0(2)EX5	WS-C2960X-48FPD-L
Switch Acceso Mesa de Ayuda 2	10.1.250.13	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso mezzanine	10.1.250.16	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso mezzanine	10.1.250.17	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso mezzanine	10.1.250.18	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L

Continúa

Switch Acceso mezzanine	10.1.250.19	12.2(55)SE5	12.2(55)SE5	WS-C2960S-48FPS-L
Switch Acceso segundo piso	10.1.250.21	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso segundo piso	10.1.250.22	12.2(55)SE5	15.0(2)SE6	WS-C2960S-48FPS-L
Switch Acceso segundo piso	10.1.250.23	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso segundo piso	10.1.250.24	12.2(35)SE5	12.2(55)SE10	WS-C2960G-24TC-L
Switch Acceso segundo piso	10.1.250.25	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso segundo piso	10.1.250.26	12.2(55)SE2	15.0(2)SE6	WS-C2960S-48LPS-L
Switch Acceso segundo piso	10.1.250.27	12.2(35)SE5	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso tercer piso	10.1.250.31	12.2(55)SE2	15.0(2)SE6	WS-C2960S-48LPS-L
Switch Acceso tercer piso	10.1.250.32	12.2(25)SEE3	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso tercer piso	10.1.250.33	12.2(25)SEE3	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso tercer piso	10.1.250.34	15.0(2)EX3	15.0(2)EX5	WS-C2960X-48FPD-L
Switch Acceso cuarto piso	10.1.250.41	12.2(55)SE2	15.0(2)SE6	WS-C2960S-48LPS-L
Switch Acceso cuarto piso	10.1.250.42	15.0(2)EX3	15.0(2)EX5	WS-C2960X-48FPD-L
Switch Acceso cuarto piso	10.1.250.43	12.1(13)EA1	12.1(22)EA14	WS-C2950G-48-EI
Switch Acceso quinto piso	10.1.250.51	12.2(25)SEE3	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso quinto piso	10.1.250.52	12.2(25)SEE3	12.2(55)SE10	WS-C2960G-48TC-L
Switch Acceso quinto piso	10.1.250.53	12.2(25)SEE3	15.0(2)SE6	WS-C2960S-48FPS-L
Switch Acceso quinto piso	10.1.250.54	12.2(25)SEE3	15.0(2)SE6	WS-C2960G-48TC-L
Switch Acceso Centro Medico	10.1.250.61	12.1(9)EA1	12.1(22)EA14	WS-C2950G-12-EI
Switch Acceso Comedor	10.1.250.15	12.2(35)SE5	12.2(55)SE10	WS-C2960G-24TC-L

- **Consideraciones tomadas en la actualización de los Switches MINFIN**

Para la actualización de cada uno de los switches de acceso de la tabla anterior, se realizó el respaldo de configuración del IOS[34] antiguo. A fin de precautelar la

[34] **IOS**: SISTEMA OPERATIVO DE CISCO

integridad de estos equipos si presentan algún tipo problema con la nueva versión del IOS actualizada.

- ✓ Se mantienen almacenadas las versiones anteriores de los switches, para el cambio inmediato de IOS en caso de requerirlo.
- ✓ Todos los switches de acceso fueron actualizados y probados su conectividad, antes de incluir a la "Solución de Cisco ISE".
- ✓ De acuerdo a los avances del presente trabajo de tesis se realizarán afinamientos de estos equipos en caso de existir errores.

- **Compatibilidad Solución de Red Inalámbrica con Cisco ISE – MINFIN**

Esta institución actualmente cuenta con una controladora Inalámbrica "WLC – Wireless LAN Controller" que proporciona la comodidad, flexibilidad y privilegios de conexión, a funcionarios generales y desarrolladores, autoridades, y visitantes en general.

El modelo actual de la controladora inalámbrica "*WLC – Wireless LAN Controller"* del MINFIN es 5508, licenciado con soporte para 25 access points, es totalmente compatible con la solución "*Cisco ISE versión 1.2.1.198*".

Asimismo, sus 25 access points son de los modelos: AIR-LAP1261N-A-K9, AIR-CAP1602I-A-K9 y AIR-LAP1142N-A-K9; según levantamiento de información Tabla 6. "*Inventario Equipos de Comunicaciones MINFIN y Regionales*", integrados a la WLC del MINFIN, son compatibles con la solución "*Cisco ISE versión 1.2.1.198*".

En la siguiente Figura que se muestra continuación se detallan los SSID[35] (Identificador de Conjunto de Servicios) creados actualmente en la institución.

[35] **SSID:** IDENTIFICADOR DE CONJUNTO DE SERVICIOS. ESTE CONCEPTO ES UTILIZADO EN REDES INALÁMBRICAS

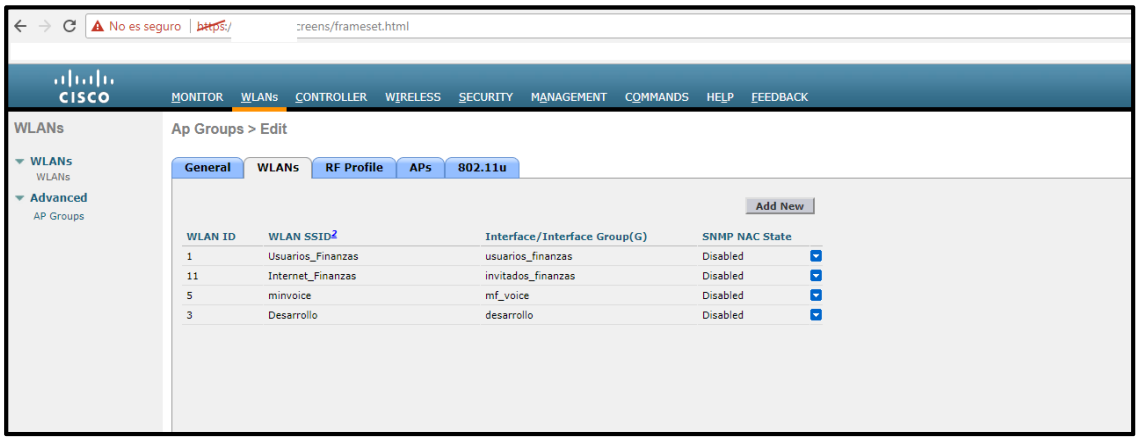


Figura 34 SSID Operativos en el MINFIN

3.3.2 ETAPA DE PLANIFICACIÓN

3.3.2.1 Diseño Plan de Implementación

- **Objetivo de Fase**

Constituir de manera detallada el plan de implementación a seguir para la ejecución de las actividades inherentes en el mejoramiento de la *"Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la red de datos del Ministerio de Finanzas"*

- **Responsabilidades Previas**

La Dirección de Tecnologías y Comunicación del MINFIN, fue la encargada de proveer las facilidades necesarias como: información, equipamiento activo-pasivos y servidores. Con el fin de ejecutar las configuraciones necesarias para el mejoramiento de la solución planteada.

El horario para la ejecución de todas y cada una de las actividades es de lunes a viernes de 8H00 a 16H30. En los casos extremos y estrictamente necesarios que se requiera suspensión del servicio o ejecución de pruebas importantes, el Ministerio de

Finanzas determinará los días y tiempos adecuados; siendo la generalidad de estos los fines de semana, feriados y horarios fuera de oficina.

- **Resumen de entorno**

Mediante la información proporcionada por los administradores de red de la Dirección de Tecnologías y Comunicación del MINFIN, se ejecuta el diseño y el plan de implementación.

Referente a los servidores de directorio activo y CA[36] (Autoridad Certificadora) ubicados en el segmento (10.1.1.x/16) se tiene la siguiente Tabla que se indica a continuación.

Tabla 13
Recursos de Hardware Directorio Activo – Entidad Certificadora

Recursos de Servidores		
Active Directory	Número de dominios	2
	Nombre del dominio	minfin.gov.ec
	versión OS	Windows Server 2008 R2, Estandar
	Service packs	SP1
	Configuración GPO	Si
	Login scripts	Si
LDAP	Fabricante	Microsoft
Entidad Certificadora	CA.minfin.gov.ec	Windows Server 2008 R2 Enterprise

Con el fin que *"Cisco ISE - MINFIN"* pueda ejecutar la funcionalidad de *"Postura"* debemos conocer la versión del antivirus corporativo.

Esta Cartera de Estado mantiene un contrato vigente para protección de dispositivos finales con "Symantec Antivirus" con versión hasta la fecha 12.1.6 cómo se expresa en la Figura que se muestra a continuación.

[36] G AUTORIDAD CERTIFICADORA. SERVIDOR EMISOR DE CERTIFICADOS DIGITALES

Figura 35 Versión antivirus corporativo MINFIN

- **Diseño Propuesto para el "Mejoramiento Solución Cisco ISE - MINFIN"**

Con base al planteamiento que presenta el trabajo de tesis *"Mejoramiento Solución Cisco ISE - MINFIN"* se expone el siguiente esquema de trabajo.

Tabla 14
Medios de Control "Solución Cisco ISE - MINFIN"

Control Cisco ISE – MINFIN		
	Wired	Wireless
SI/NO	SI	SI

Se presenta el resumen de sistemas operativos funcionando actualmente en esta Cartera de Estado, con el fin de elaborar los "Perfiles de acceso" a la red de datos institucional.

Tabla 15
Sistemas Operativos para Perfilamiento Cisco ISE

SISTEMAS OPERATIVOS MINFIN				
Sistemas operativos Estándar	**Total**	**Sp1**	**Sp2**	**Sp3**
Microsoft Windows XP Professional	160	1	9	150
Microsoft Windows 7 Professional	280	0	10	270
Microsoft Windows 8 Pro	14	7	0	0
Microsoft Windows 8.1 Pro	21	5	15	1
Microsoft Windows 10 Enterprise Edition	100	0	0	0
TOTAL	575			

Para el *"Mejoramiento Solución Cisco ISE - MINFIN"* se propone estandarizar:

- ✓ Microsoft Windows XP Professional SP3
- ✓ Microsoft Windows 7 Professional SP1
- ✓ Microsoft Windows 8 Professional SP1
- ✓ Microsoft Windows 10 Enterprise Edition

Además, esta institución cuenta con equipos sin usuario de dominio que deben autenticarse con la *"Solución Cisco ISE"* mediante MAB (MAC Address Bypass) como se indica a continuación.

- ✓ Impresoras: 75 impresoras (28 HP y 47 Xerox)
- ✓ Teléfonos: 575 teléfonos marca Cisco modelos Cisco 6921, 7821, 7925, 7942, 7961G-GE, 7962, E20, IP Communicator, 6922, y 7963

Referente al antivirus institucional queda estandarizado *"Symantec Versión 12.1.6"* y versiones posteriores.

Con respecto a los segmentos de red activos de esta Cartera de Estado tenemos:

Tabla 16
Segmentos de red producción Ministerio de Finanzas

Segmentos Activos - MINFIN				
VLAN	**Nombre**	**DHCP**	**Profile**	**Tipo de uso**
1	Native	NO	Impresoras	Servidores, cámaras, lectoras, impresoras, switches
200	Desarrollo	NO	Desarrollo	Desarrolladores
304	Usuarios_MF	SI	Usuarios_MF	Usuarios en general
300	Voice	SI	Voip_MF	teléfonos
301	Servidores Virtuales	NO	access-points	Access points, servidores virtuales
307	Invitados_Wireless	SI	wifi-invitados	Invitados Finanzas
104	Mesa de Ayuda	NO	mesa_ayuda	Mesa de Ayuda
305	Enlace Litoral	NO	Guayaquil	Mesa de Ayuda GYE
306	Enlace Cuenca	NO	Cuenca	Mesa de Ayuda Cuenca

Para los dispositivos que no cumplan los requisitos de acceso a la red de datos institucional, necesita una *"VLAN DE INICIO o DIAGNOSTICO"*, para el primer control de acceso a la red, previo a otorgar el perfil requerido.

Con base a la información referenciada se realiza el mejoramiento de *"Perfiles de acceso a la red de datos"* con las siguientes características de control de acceso como se expone en la siguiente Tabla.

Tabla 17
Mejoramiento de Perfiles para el Control Acceso - MINFIN

Perfiles para Control Accesos del Ministerio de Finanzas			
Profile 1	**Profile 2**	**Profile 3**	**Profile 4**
Usuarios_MF	Mesa ayuda Quito	Desarrollo	Remediación
VLAN 304	VLAN 104	VLAN 200	VLAN 309
IP FIJA - DHCP[37]	IP FIJA – DHCP	IP FIJA - DHCP	DHCP
Usuarios de Directorio Activo	Usuarios de Directorio Activo	Usuarios de Directorio Activo	Usuarios de Directorio Activo
Autentica AD + CA	Autentica AD + CA	Autentica AD + CA	Autentica AD + CA
Valida SO[38] (W8, W7, WXP, W10) + AV[39]	Valida SO (W8, W7, WXP, W10) + AV	Valida SO (W8, W7, WXP, W10) + AV	Valida SO (W8, W7, WXP, W10) + AV
Profile 5	**Profile 6**	**Profile 7**	**Profile 8**
Guayaquil	Cuenca	Pruebas	Telefonía
VLAN 305	VLAN 306	VLAN 220	VLAN 300
IP FIJA – DHCP	IP FIJA – DHCP	DHCP	DHCP
Usuarios de Directorio Activo	Usuarios de Directorio Activo	Usuarios otros segmentos	Autentica mac address
Autentica AD + CA	Autentica AD + CA	Autentica AD + CA	Base datos mac-address ISE
Valida SO (W8, W7, WXP, W10) + AV	Valida SO (W8, W7, WXP, W10) + AV	Valida SO (W8, W7, WXP, W10) + AV	No valida SO - AV
Profile 9	**Profile 10**	**Profile 11**	**Profile 12**
Impresoras	Access Points	Wifi-invitados	Wifi-BYOD
VLAN 1	VLAN 1	VLAN 307	VLAN 307
FIJA	DHCP-FIJA	DHCP	DHCP

Continúa

[37] **DHCP**: PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST, ASIGNACIÓN AUTOMÁTICA DE IP A UN DISPOSITIVO

[38] **SO:** SISTEMA OPERATIVO

[39] **AV:** ANTIVIRUS CORPORATIVO

Autentica mac-address	Autentica MAC-ADDRESS	SPONSOR	BYOD- Usuarios AD móviles
Base datos mac-address ISE	Base datos mac-address ISE	SPONSOR	Base datos mac-address ISE
No valida SO - AV	No valida SO – AV	No valida SO - AV	No valida SO – AV

Como alcance definido dentro de la *"fase de implementación*" se van a trabajar todos los perfiles propuestos, excepto el *"Perfil 7"*. Debido a que este perfil se utilizara para diferentes pruebas, como por ejemplo la interacción de *"Cisco ISE"* con firewalls Fortinet y Sophos, BYOD entre otras funcionalidades.

Pruebas Post- Implementación "Mejoramiento Solución Cisco ISE - MINFIN"

- **Objetivo de Fase**

Indicar de manera general las etapas y resultados obtenidos en las pruebas, antes de iniciar un despliegue masivo para el mejoramiento de la *"Solución de Control de Acceso, Remediación, Profiling y servicios AAA "Authentication, Authorization and Accounting"* en la red de datos del Ministerio de Finanzas.

- **Detalles de Configuraciones**

A continuación, se exponen los pasos necesarios para ejecutar las pruebas post-implementación para el mejoramiento de la "*Solución de Control de Acceso - MINFIN*"

- En la siguiente Figura que se muestra continuación se detalla la creación de grupos de seguridad en el Directorio Activo de acuerdo a los perfiles propuestos en el diseño.

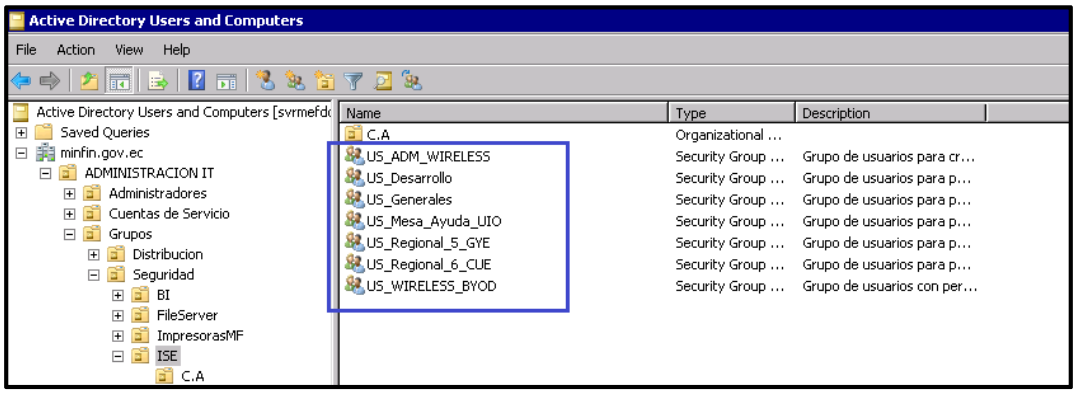


Figura 36 Creación perfiles AD – MINFIN

- ✓ Creación de usuarios de prueba (Prueba1, Prueba2 y Prueba3) que consten en los grupos de seguridad del Directorio Activo con base a los perfiles definidos
- ✓ Pruebas con computadores instalados sistemas operativos definidos (Microsoft Windows XP Professional, 7 Professional, 8 Pro, 8.1 Pro, 10, Mac OS y Linux).
- ✓ Identificación y ejecución de comandos de seguridad en los puertos de cada uno de los switches en las cuales estarán conectadas los dispositivos de red. A fin de interactuar con *"Cisco ISE"*
- ✓ Migración de las máquinas con Sistemas operativos antiguos con el fin de estandarizar todas las versiones.
- ✓ Creación de Scope[40] de DHCP para grupos que actualmente están con direccionamiento estático.

- **Desarrollo Etapa de Pruebas Post- Implementación**

Con base a la información de planificación se realizó las configuraciones en la *"Solución Cisco ISE"* con los grupos de "PERFILES" definidas en la Tabla 17. "*Mejoramiento de Perfiles para el Control Acceso - MINFIN"*, para el control de acceso en los medios WIRED (cableada) y WIRELESS (inalámbrica).

[40] **SCOPE:** GRUPO DE DIRECCIONAMIENTO IP USADO ESPECIALMENTE EN DHCP

En la siguiente Figura se expresa las configuraciones realizadas en los medios WIRED (cableada) y WIRELESS (inalámbrica) para nuestra etapa de *"Pruebas Post-Implementación.*

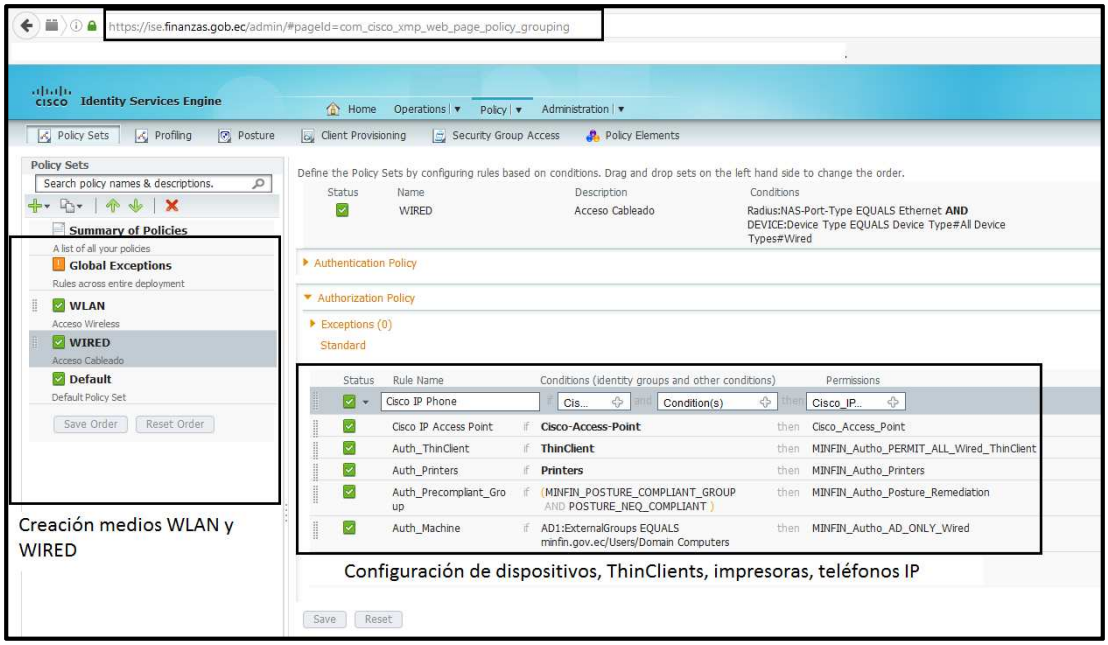


Figura 37 Configuraciones medias WLAN Y WIRED

Con el prototipo de implementación post-producción se buscó hacer una implementación en un ambiente controlado, donde se pueda reunir la mayor parte de conocimiento y elementos de red que se encontrarán en la red de producción institucional.

Para lograr armar el ambiente de pruebas se definió el alcance del mismo, en función del universo de elementos de la red de producción, obteniendo las siguientes tareas:

- **Procedimientos realizados**
- **Básicos**
  - ✓ Instalación y configuración de los servidores en modo "Deployment"[41]
  - ✓ *Actualización de switches. Tabla 12. "Afinamiento NADs … (…)"*

[41] **DEPLOYMENT**: SE REFIERE A DESPLEGAR UN SERVICIO INFORMÁTICO.

- **Integraciones**
  - ✓ Integración de servidores a la red, a nivel de conectividad WLAN y WIRED.

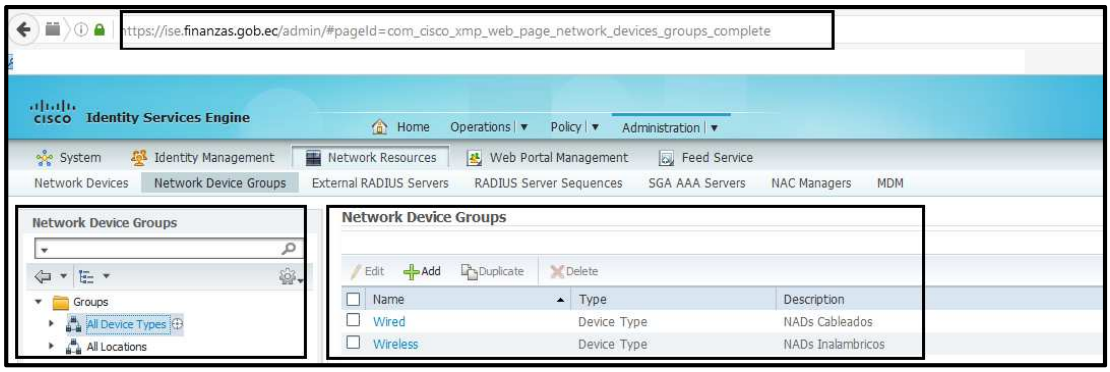


Figura 38 Grupos WLAN Y WIRED Cisco ISE – MINFIN

  - ✓ Verificación de versiones y compatibilidades, a nivel de actualizaciones. Referencia Tabla 15 “Sistemas Operativos para Perfilamiento Cisco ISE”.
  - ✓ Integración con los servidores a de Directorio Activo y Unidad Certificadora.
  - ✓ Integración de elementos de control a servidores “Cisco ISE – MINFIN”, 1 switch de prueba activo y controladora Inalámbrica.

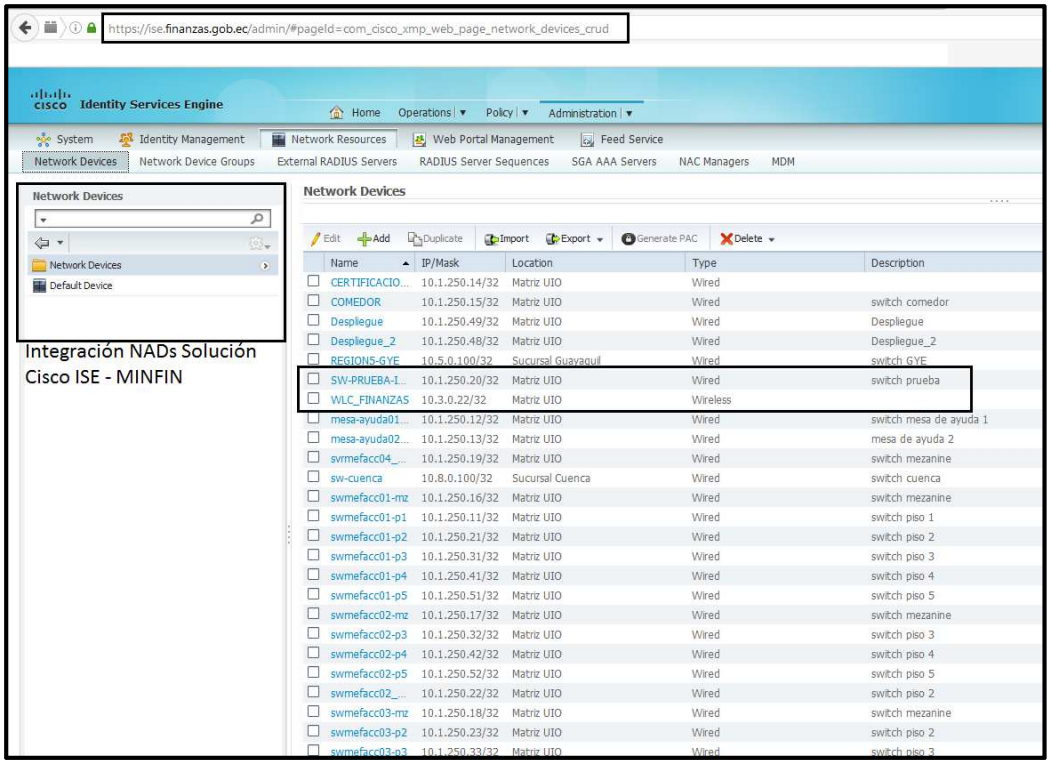


Figura 39 Integración NADs Cisco ISE – MINFIN

- **Perfiles**
  - ✓ Configuración de 8 perfiles de control de accesos indicados en la Tabla 17.
  - ✓ Definición de control de accesos estáticos.
  - ✓ Instalación de agentes en equipos de prueba.
  - ✓ Definición para el uso del agente cisco en sistema Windows.
  - ✓ Validación de equipos de prueba.
  - ✓ Validación de característica MAB en teléfonos, impresoras, access points y otros dispositivos IP. Prueba realizada con 5 dispositivos móviles de diferentes marcas y modelos, Además se realizaron pruebas con 2 impresoras y 8 teléfonos IP de diferentes modelos

- **Pruebas de Control de Acceso**

Para realizar pruebas de control de accesos de una manera organizada y planificada de la *"Solución Cisco ISE -MINFIN"* y con el fin de no encontrarnos con imprevistos al momento de desplegar esta solución en el ambiente de producción se realizaron los siguientes pasos:

- **Validación de control de acceso con los SO estandarizados**
  - ✓ Microsoft Windows XP Professional SP3
  - ✓ Microsoft Windows 7 Professional SP1
  - ✓ Microsoft Windows 8 Professional SP1
- **Validación de control de acceso con el Antivirus definido**
  - ✓ Symantec versión definida
- **Validación de control de acceso de VLAN definida**
  - ✓ Verificación de direccionamiento del dispositivo a VLAN definida.
  - ✓ Definición y verificación de accesos con dACLS.
- **Validación de direccionamiento a la VLAN de remediación**
  - ✓ Dispositivos que no cumplan con los lineamientos de acceso a la red se direccionen a la VLAN de remediación10.9.X.X/16
- **Validación de funcionalidad en Wireless**
  - ✓ Usuarios internos.

- ✓ Usuarios invitados.
- ✓ Bring your Own Device BYOD, para usuarios pertenecientes al dominio MINFIN.

- **Resultados Obtenidos**

Según la información obtenida *"Base de Conocimiento"* y las validaciones ejecutadas en la *"Etapa de Pruebas"* se obtuvieron los siguientes resultados:

- ✓ Revisión de parches de seguridad en el equipo "*Cisco ISE – MINFIN*" primario y secundario, manteniendo la versión 1.2.
- ✓ Revisión de licenciamiento actual a fin de no tener problemas al momento del despliegue masivo. El licenciamiento actual de "*Cisco ISE – MINFIN*" es para 1000 dispositivos finales. Y para los servicios de *"Remediación"* y *"Profiling"* para 700 dispositivos finales verificando su consumo con base a los dispositivos que se van integrando a la solución.
- ✓ Integración con el servidor AD (Directorio Activo) y CA (Entidad Certificadora) de cada grupo de seguridad, según Tabla 18 *"Mejoramiento de Perfiles para el Control Acceso –MINFIN"*
- ✓ Integración con los NADs de prueba "switches" comprobando la autenticación de los usuarios con la *"Solución Cisco ISE – MINFIN"*.
- ✓ Verificación de los NADs de prueba "switches" y la *"Solución Cisco ISE – MINFIN"* con parámetros de RADIUS, AAA y SNMP[42].
- ✓ Configuración de los perfiles definidos en el diseño para usuarios de prueba, según Tabla 19 *"Mejoramiento de Perfiles para el Control Acceso –MINFIN"*.
- ✓ Verificación de funcionalidad de los agentes cisco "AnyConnect" o suplicante nativo de Windows 802.1X para autenticación de los dispositivos.
- ✓ Definición de uso de agente "Cisco AnyConnect" para todos los computadores de escritorio y portátiles que usen sistema operativo de Microsoft.

[42] **SNMP:** PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED

- ✓ Instalación y Verificación de los dispositivos de prueba como: computadores de escritorio y portátiles, access points, teléfonos IP, impresoras y teléfonos móviles.
- ✓ Configuración de políticas para los servicios de *"Authentication, Authorization and Accounting (AAA)"*, con base a la información de usuario, dispositivo, validación de cumplimiento de lineamientos institucionales, protocolos de autenticación, perfiles que se usaran para los usuarios de prueba y producción.
- ✓ Configuración y validación de los perfiles de grupo en dispositivos finales entre los que se encuentran: computadores de escritorio y portátiles, access points, teléfonos IP e impresoras
- ✓ Validación de lineamientos institucionales configurados *"Authentication, Authorization and Accounting (AAA)"* con los usuarios de prueba1 y 2, en los dispositivos finales con sistemas operativos Windows XP Professional SP3, Windows 7 Professional SP1, Windows 8 Professional SP1 y MAC. Con el fin de validar la autenticación de cada usuario en la solución.
- ✓ Ensayos de autenticación y autorización con cada usuario de pruebas. Además, verificamos en la *"Solución Cisco ISE – MINFIN"* la característica de accounting que efectúa cada dispositivo sobre la hora, día y ubicación permitiendo el control del acceso a la red.
- ✓ Configuración y validación de los mecanismos para el control de acceso a la red, incluyendo: VLANs (304, 104, 300, 200,1) definida y dACLS "ACLs descargables".
- ✓ Configuración y validación de políticas de antivirus y sistema operativo en los computadores de usuarios de prueba y cumplimiento de las políticas de acceso a la red de datos institucional.
- ✓ Verificación de la VLAN 309 *"Remediación"* para los usuarios que no cumplan con los requisitos mínimos para acceder a la red de datos de producción.
- ✓ Verificación que desde la VLAN 309 *"Remediación"* permita la descarga y actualización del antivirus en los computadores que lo necesiten.
- ✓ Validación de la característica de *"Postura"* mediante el agente NAC, para ser descargado e instalado automáticamente una vez que se pone la seguridad en el puerto del switch y el dispositivo final ingresa a la *"Solución Cisco ISE – MINFIN"*

- ✓ Configuración y validación con los usuarios de pruebas para acceso WLAN (Wireless) definiendo los siguientes SSID: Usuarios_ISE, Invitados_ISE y BYOD_ISE.
- ✓ Configuración portal cautivo validando el funcionamiento con los usuarios de prueba como el registro de dispositivos móviles.
- ✓ Registro y administración de invitados controlando que el acceso sea por un tiempo limitado a través del portal de administración.

3.3.3 ETAPA DE EJECUCIÓN Y CONTROL

- **Objetivo de Fase**

Establecer de manera detallada el "Plan de Despliegue Masivo" para la ejecución de las actividades inherentes al *"Mejoramiento de la Solución Cisco ISE"* para el Ministerio de Finanzas.

- **Detalles previos**

La Dirección de Tecnologías y Comunicación de esta institución es responsable, de toda la infraestructura necesaria para el correcto funcionamiento de la mejora de la *"Solución Cisco ISE - MINFIN"*. Es decir, todas las facilidades para configurar el equipamiento activo y pasivo.

- **Despliegue**

Una vez finalizada las etapas de inicio, planificación y pruebas en un ambiente controlado se inicia la etapa de "Ejecución" para el despliegue masivo en la red de datos de producción del Ministerio de Finanzas.

El despliegue para el mejoramiento de la *"Solución Cisco ISE - MINFIN"* tiene una duración de 4 meses laborables con umbral de 15 días por contratiempos e imprevistos y se limita a los elementos definidos a continuación:

- **Requisitos por parte de la DTIC:**

a) Se requiere los usuarios de dominio y las credenciales de acceso para la administración de los switches.
b) Se requiere el usuario de administración de *"Cisco ISE"*.
c) Se requiere que los usuarios se encuentren en los grupos de seguridad definidos en la Figura 32*"Creación perfiles AD – MINFIN"*.
d) Se requiere presencia de un técnico de soporte a usuarios durante los 30 días de despliegue esta actividad.
e) Se requiere la presencia de los funcionarios institucionales para el ingreso con sus credenciales a computador de escritorio o portátil.
f) Se requiere el soporte del administrador de Directorio Activo para que pueda colaborar con políticas GPO[43] para la instalación de los agentes Cisco AnyConnect y Cisco NAC.
g) Durante el tiempo de duración del despliegue masivo, amerita horarios de trabajo fuera de oficina se requiere de la presencia de alguna persona de la DTCs, para el ingreso a las áreas de trabajo.
h) En casos de ausencia del funcionario para el ingreso de la contraseña de dominio en su computador se realizará a través de un usuario "administrador local y de red", a fin de validar las características de la solución mejorada.
i) Es necesario el acompañamiento del administrador de red de la institución, para la implementación del mejoramiento de la *"Solución Cisco ISE – MINFIN"* en la red de datos de producción.

- **Planificación de Actividades**

Las actividades que se mencionan a continuación tomaran un tiempo de 50 minutos aproximadamente por cada equipo institucional.

- **Ingreso a los switches mediante telnet, SSH de acuerdo a los pisos**

[43] GPO: POLÍTICAS DE GRUPO ORGANIZACIONALES USADAS EN SERVICIOS DE AD.

- ✓ Conexión segura a los switches de acceso MINFIN, se puede usar cualquier aplicación de conexiones telnet o SSH[44].

  Tiempo Estimado: 5 min.

- **Verificación en la "Solución Cisco ISE - MINFIN" que se encuentren agregados los NADs "switches" correspondientes**

  Tiempo Estimado: 5 min.

- **Instalación de utilitarios en los computadores de los funcionarios públicos**

  - ✓ Instalación del agente Cisco AnyConnect.
  - ✓ Instalación de agente Cisco NAC.
  - ✓ Reinicio del computador. Se requiere nuevamente el ingreso de usuario y contraseña en el computador.
  - ✓ Presencia del usuario durante las configuraciones e instalaciones de los agentes.

Tiempo Estimado: 8 a 15 min.

- **Configuración de seguridad en el puerto del switch**

  - ✓ Desconexión del patch cord[45] UTP[46] del usuario.
  - ✓ Verificación en switch del puerto desconectado.
  - ✓ Reseteo de configuración del puerto.
  - ✓ Reconfiguración del puerto del switch con comandos de autenticación para el mejoramiento de la *"Solución Cisco ISE - MINFIN"*. Los comandos a ser ingresados en la interface del NAD "Switch de acceso".

---

[44] **SSH:** SECURE SHELL, EN ESPAÑOL: INTÉRPRETE DE ÓRDENES SEGURO

[45] **PATCH CORD:** DENOMINADO CABLE DE RED PARA CONEXIONES ENTRE EQUIPO DE COMUNICACIÓN Y ESTACIONES DE TRABAJO

[46] **UTP:** PAR TRENZADO NO APANTALLADO

En la Figura que se expresa el significado de cada comando ingresado en los switches de acceso, para que interactúe y aplique políticas con la gestión de Cisco ISE – MINFIN.

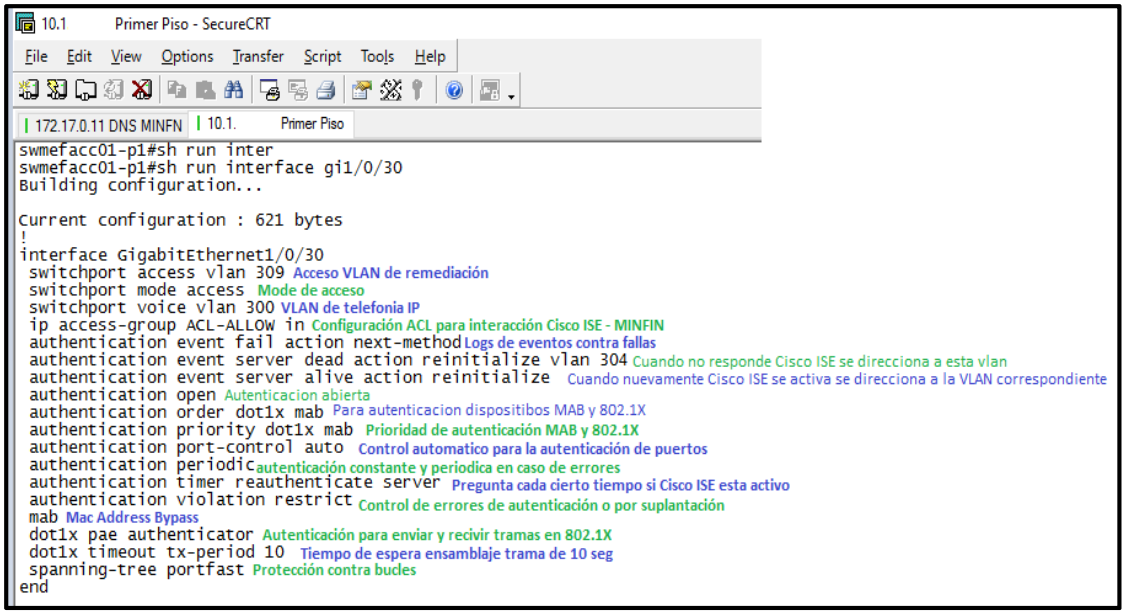


Figura 40 Comandos interface NAD para interacción con Cisco ISE

Tiempo Estimado: 5 min.

- **Verificación de características AAA y Postura de usuario**

  - ✓ Verificación de autenticación con Cisco AnyConnect.
  - ✓ Validación de las 3 funciones AAA *"Autenticación, Autorización y Contabilización"* en el switch de acceso institucional. Mediante el comando *"show authentication sessions interface (número de la interface switch de acceso)"*.

En la siguiente Figura se expone la información detallada al aplicar el comando en mención.

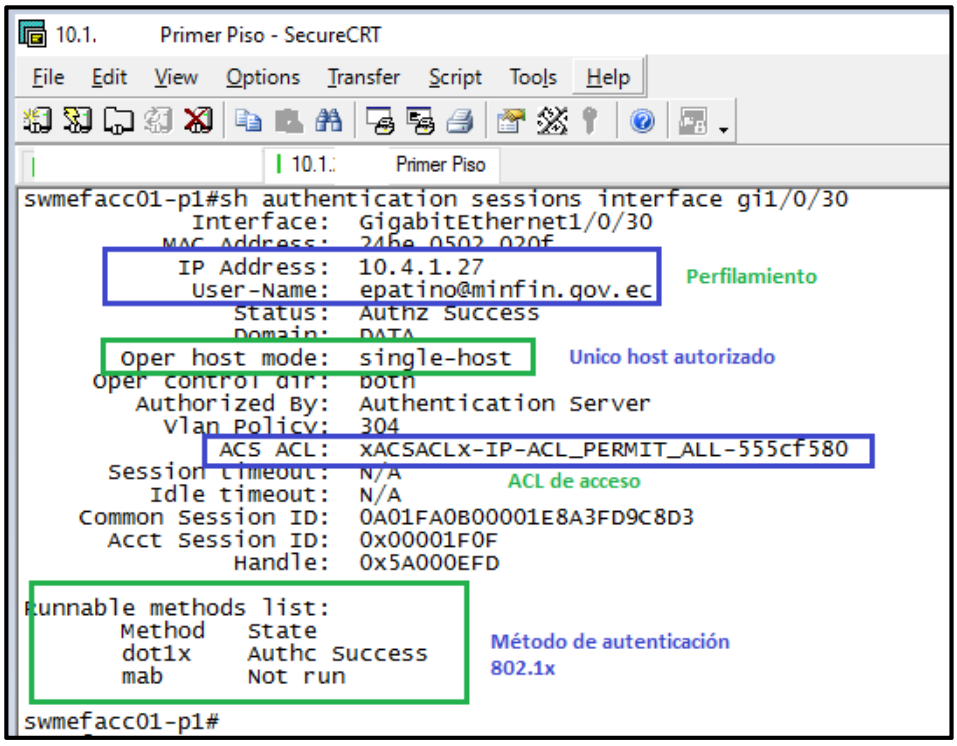


Figura 41 Comando de validación funcionalidades *"Cisco ISE"*

- ✓ Verificación de políticas de *"Postura"* (antivirus y sistema operativo).
- ✓ Validación de servicios en el computador del usuario final.

Tiempo Estimado: 10 min.

- **Procedimiento de restauración**

En el caso de presentarse problemas o dificultades con la integración del computador a la *"Solución Cisco ISE"* se procederá a dejarlo en su estado inicial, es decir sin "seguridad en el puerto del switch".

Tiempo Estimado: 10 min.

3.4.3.1 Plan de Implementación "Mejoramiento Cisco ISE - MINFIN"

- **Procedimiento de Instalación para el Ingreso de Computadores con Sistemas Operativos Windows**

En esta sección se presentan el procedimiento de instalación de certificados, agentes y despliegue de la *"Solución Cisco ISE - MINFIN"*

- **Importante:**

Los procedimientos que se indican a continuación, se pueden realizar desde cualquier computador que este dentro del dominio MINFIN. Adicionalmente para la descarga de certificados, agentes, antivirus y actualizaciones se pueden también realizar desde el segmento de remediación 10.9.X.X/16.

- **Verificación e instalación de certificados**

Digitamos el comando mmc[47] dentro de la casilla de la ventana ejecutar. Esta ventana podemos obtenerla con la combinación de teclas + R, tal como lo muestra la imagen.

Realizar este proceso para validar que los certificados de computador y usuario sean los correctos; estos certificados son necesarios para que el computador/usuario puedan ingresar a la red de datos del MINFIN.

En la Figura que se muestra a continuación indica el registro de los usuarios en la entidad certificadora del MINFIN.

[47] **MMC:** MICROSOFT MANAGEMENT CONSOLE

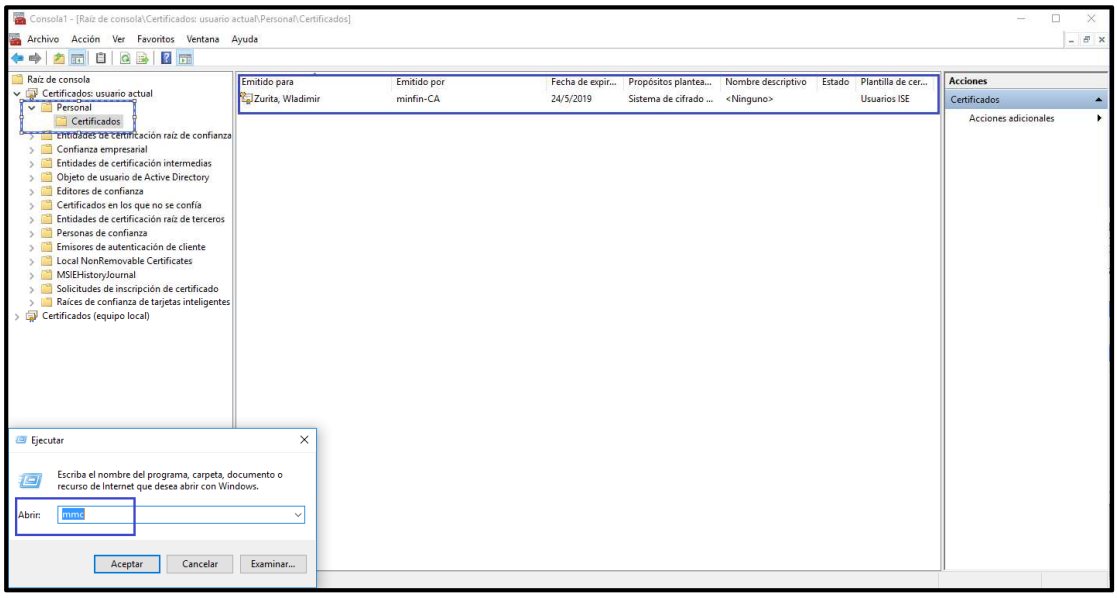


Figura 42 Verificación de Certificados

- **Instalación de Agentes Cisco NAC y AnyConnect**

Con los siguientes procedimientos demostraremos paso a paso como instalar los agentes AnyConnect y NAC. Estos agentes son instalados en cada computador con sistema operativo Windows.

- **Importante:**

Los instaladores de Cisco AnyConnect y NAC se encuentran en un repositorio protegido administrado por la DTCs, para facilidad de acceso por el personal técnico de esta Dirección.

A continuación, realizamos una breve descripción de los agentes "Cisco AnyConnect y Cisco NAC" para mayor entendimiento del potencial de la *"Solución Cisco ISE"* mejorada en la red de datos del MINFIN.

Cisco AnyConnect Secure Mobility

Permite a sus empleados trabajar desde cualquier lugar, con sus computadores portátiles o de escritorio, así como en los dispositivos móviles personales,

independientemente de su ubicación física. Proporcionando la seguridad necesaria para ayudar a mantener los datos de su organización segura y protegida.

Figura 43 Instalador Cisco AnyConnect

Cisco NAC Agente

Proporciona una evaluación de postura basada en agentes locales de máquina y la remediación que no cumplen con los lineamientos organizacionales. El agente NAC de Cisco está diseñado para proporcionar capacidad de conexión del usuario en una amplia gama de equipos.

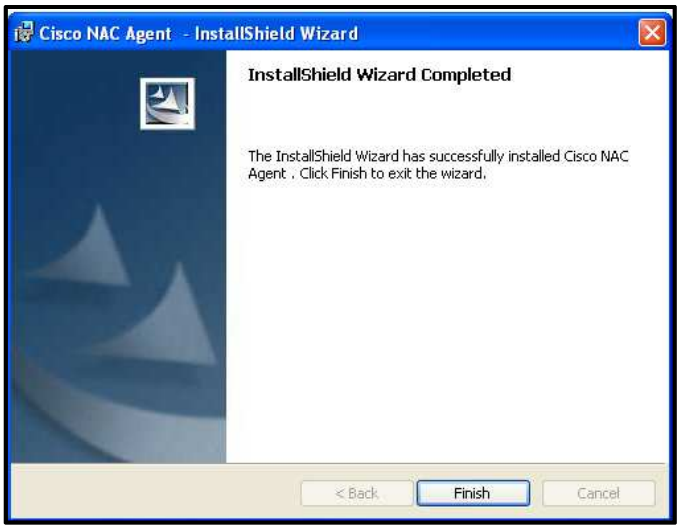


Figura 44 Instalador Cisco NAC

Los agentes *"Cisco AnyConnect y Cisco NAC"* pueden ser instalados mediante política de directorio activo. Con el fin de que cuando el usuario inicie la sesión en su computador automáticamente se instale cada uno de ellos, sin necesidad de la intervención de un técnico de soporte técnico del MINFIN.

Para los casos de no despliegue de los agentes por política de directorio activo, se debe realizar la instalación manualmente.

- **Importante:**

Para finalizar estos procedimientos se debe realizar un reinicio del computador con el fin de hacer efecto los cambios ejecutados.

Una vez adoptadas las configuraciones de los agentes en el computador, se debe ejecutar los comandos de seguridad en el puerto del switch expuestos en la Figura 42 *"Comandos interface NAD para interacción con Cisco ISE"*.

- **Verificación de instalación de Agentes Cisco NAC y AnyConnect**

Una vez configurado la seguridad en el puerto del switch del usuario para ingreso a la *"Solución Cisco ISE - MINFIN"*, se debe verificar la asignación de IP *"Remediación 10.9.X.X/16"* en la pantalla del agente AnyConnect, como se indica en la siguiente Figura.

Figura 45 AnyConnect VLAN 309

Transcurrido de 1 a 2 minutos el *"Agente Cisco NAC"* empieza la revisión, de cumplimiento de requisitos definidas para el ingreso del computador o dispositivo en la red de producción institucional. Seguido realizará la revisión de postura como se expone en las siguientes Figuras.

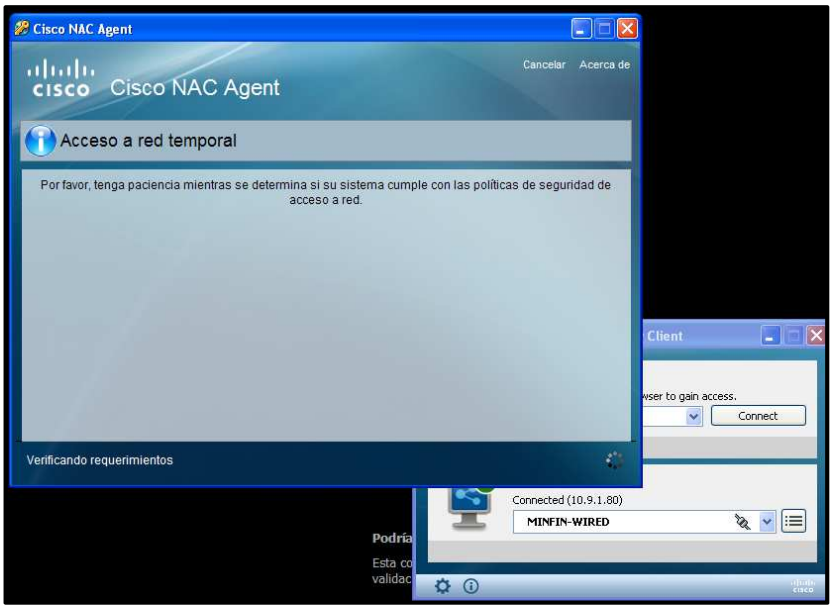


Figura 46 Análisis cumplimiento de requisitos

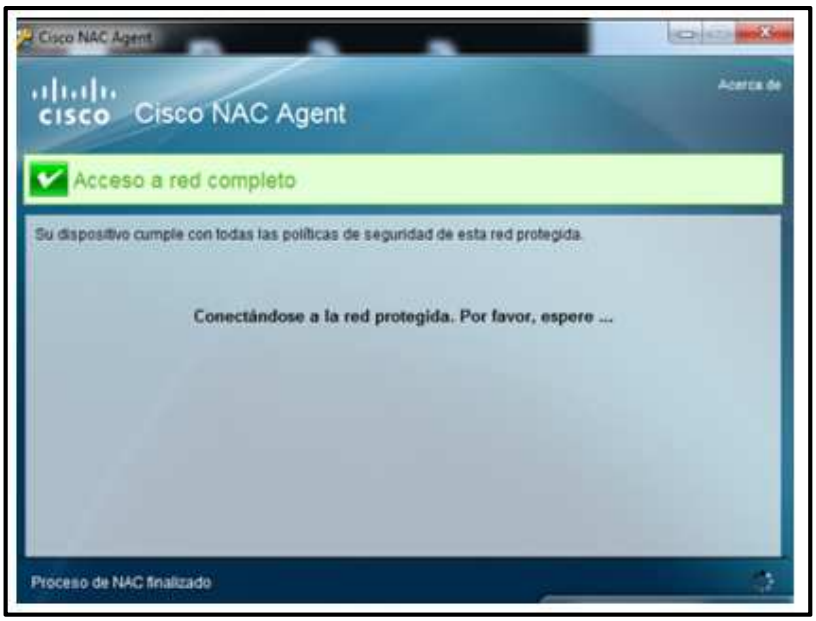


Figura 47 Acceso al computador a la red con el Agente NAC

Si el computador cumple con los requisitos mínimos como es antivirus "Symantec" y parches actualizados de sistema operativo. Inmediatamente se direcciona a la VLAN que pertenece según definición de perfile Tabla 20 **"***Mejoramiento de Perfiles para el Control Acceso – MINFIN"*.

Figura 48 Asignación a la VLAN definida en AD – MINFIN

Para los computadores portátiles que utilizan acceso mediante red inalámbrica. Para esto se debe conectar a los SSID que terminan en "ISE".

Estos SSID fueron creados con el fin que la *"Solución Cisco ISE - MINFIN"* interactúe con estos dispositivos. Seguido se debe esperar para que la tarjeta asocie una dirección IP de acuerdo al direccionamiento definido.

- **Importante**

El SSID *"Usuarios Finanzas ISE"*, realiza el mismo análisis con el agente NAC, de igual forma como se realiza en un usuario cableado. En las siguientes Figuras se expone esta característica.

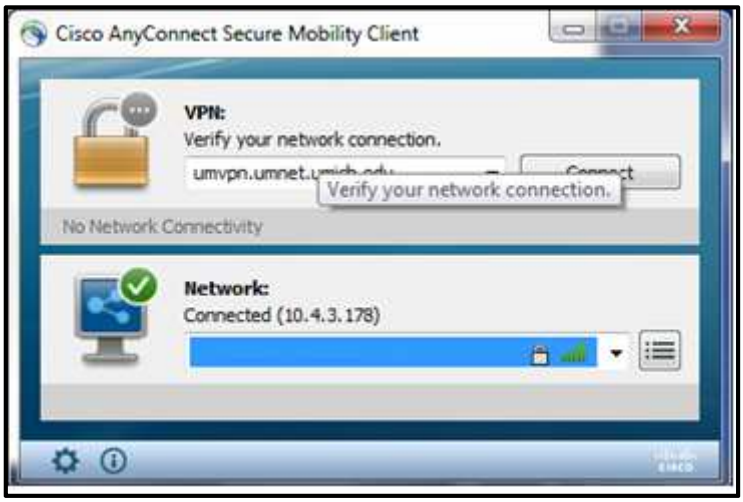


Figura 49 Conexión SSID con seguridad "Cisco ISE - MINFIN"

Figura 50 Identificación SSID
"Usuarios Finanzas ISE"

- **Procedimiento de Instalación para el Ingreso de computadores con Sistemas Operativos OS X y Linux en la Solución Cisco ISE - MINFIN**

Los equipos con sistemas operativos OS X (Apple Mac) y Linux no requiere la instalación de ningún agente. Este tipo de sistemas operativos tienen activo por defecto

el suplicante nativo 802.1X para realizar la autenticación. Como se indica en la siguiente Figura.

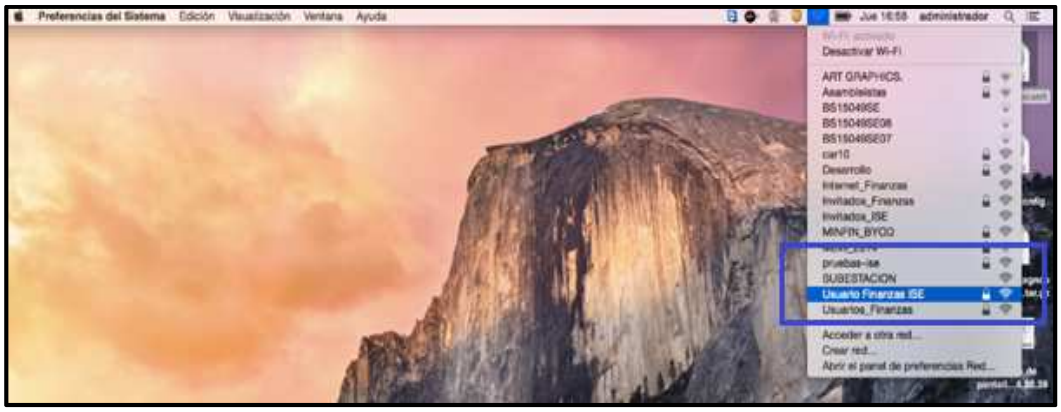


Figura 51 Ingreso SO, Mac y Linux

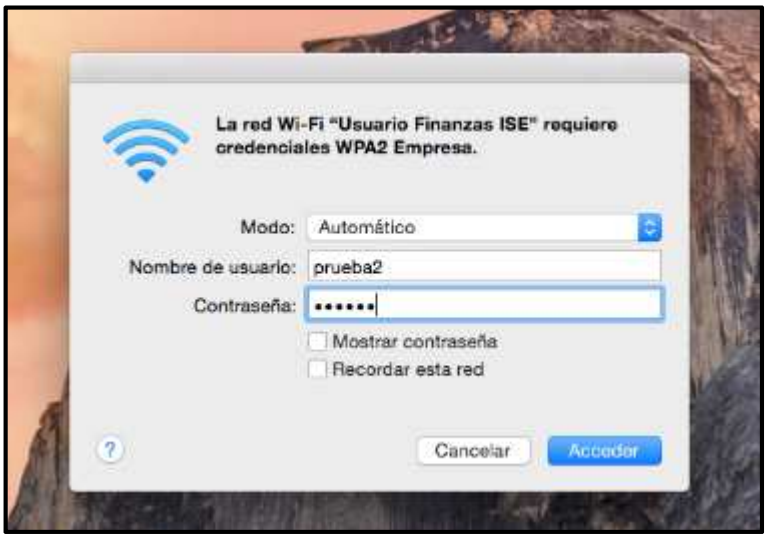


Figura 52 Credenciales para "Usuarios Finanzas ISE"

Al conectar un computador OS X (Apple Mac) en la red cableada institucional, automáticamente aparece la opción de conexión 802.1X. Adicionalmente debemos ingresar el usuario y contraseña del dominio *"minfin"* como se expone en la siguiente Figura.

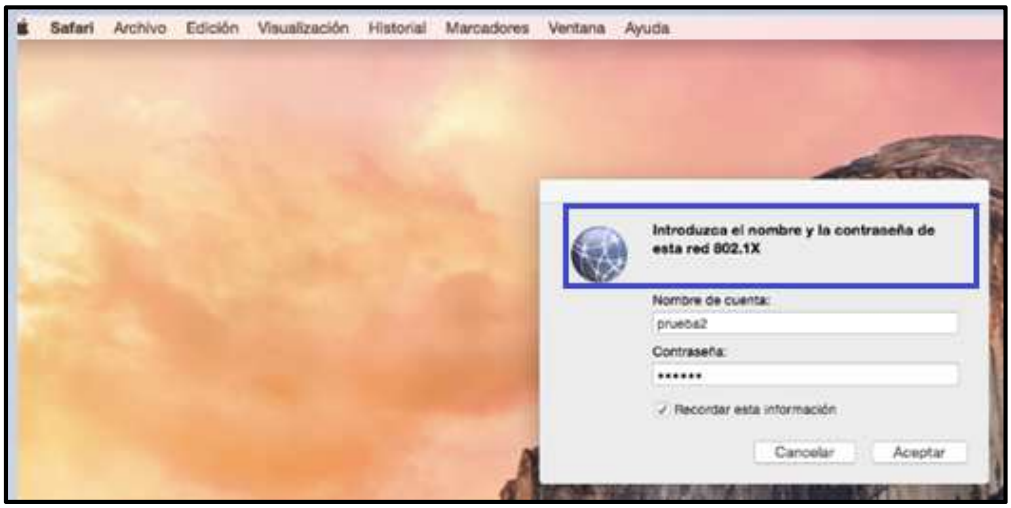


Figura 53 Autenticación 802.1X sistema operativo Mac

- **Procedimiento de Ingreso para Dispositivos mediante MAB**

Para el ingreso de dispositivos mediante MAB, se debe escalar al administrador de la "*Solución Cisco ISE – MINFIN"*. Para el ingreso de la dirección mac address del dispositivo para el acceso a la red de producción del MINFIN.

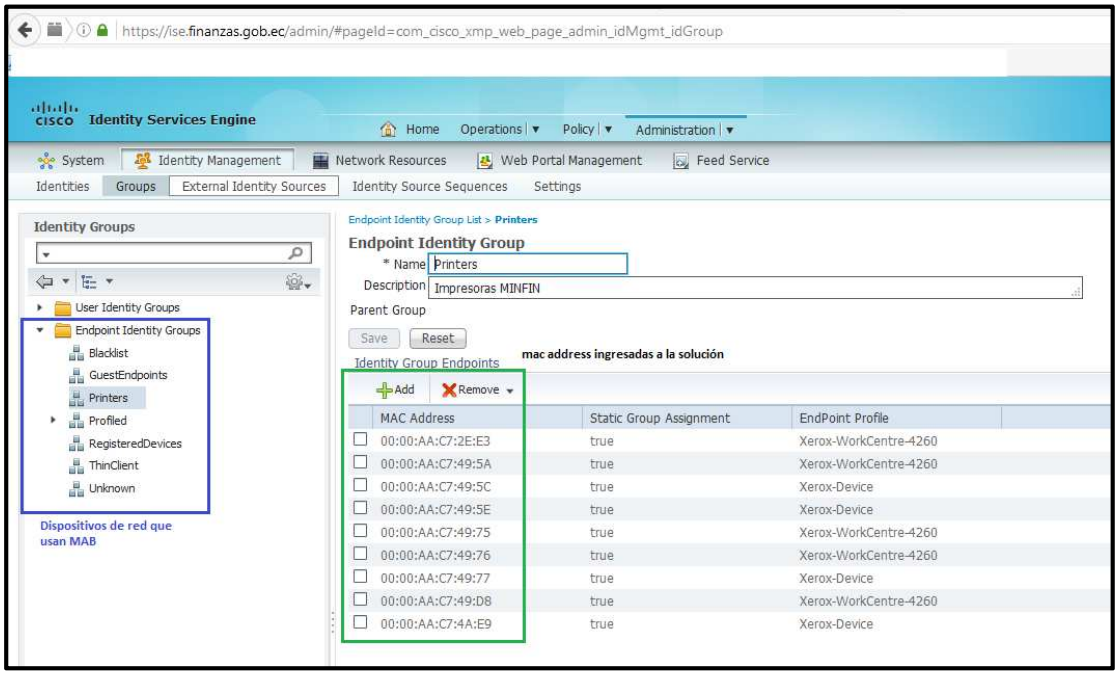


Figura 54 Ingresos de dispositivos mediante MAB

Una vez ingresado el dispositivo a la *"Solución Cisco ISE – MINFIN"*, el administrador de la herramienta, debe verificar la conectividad realizando ping a la dirección IP (dispositivo que usa MAB).

Además, el administrador de la solución debe ejecutar los comandos que se exponen en la siguiente Figura, para validar que el dispositivo que usa MAB, se haya integrado correctamente a *"Cisco ISE - MINFIN"*

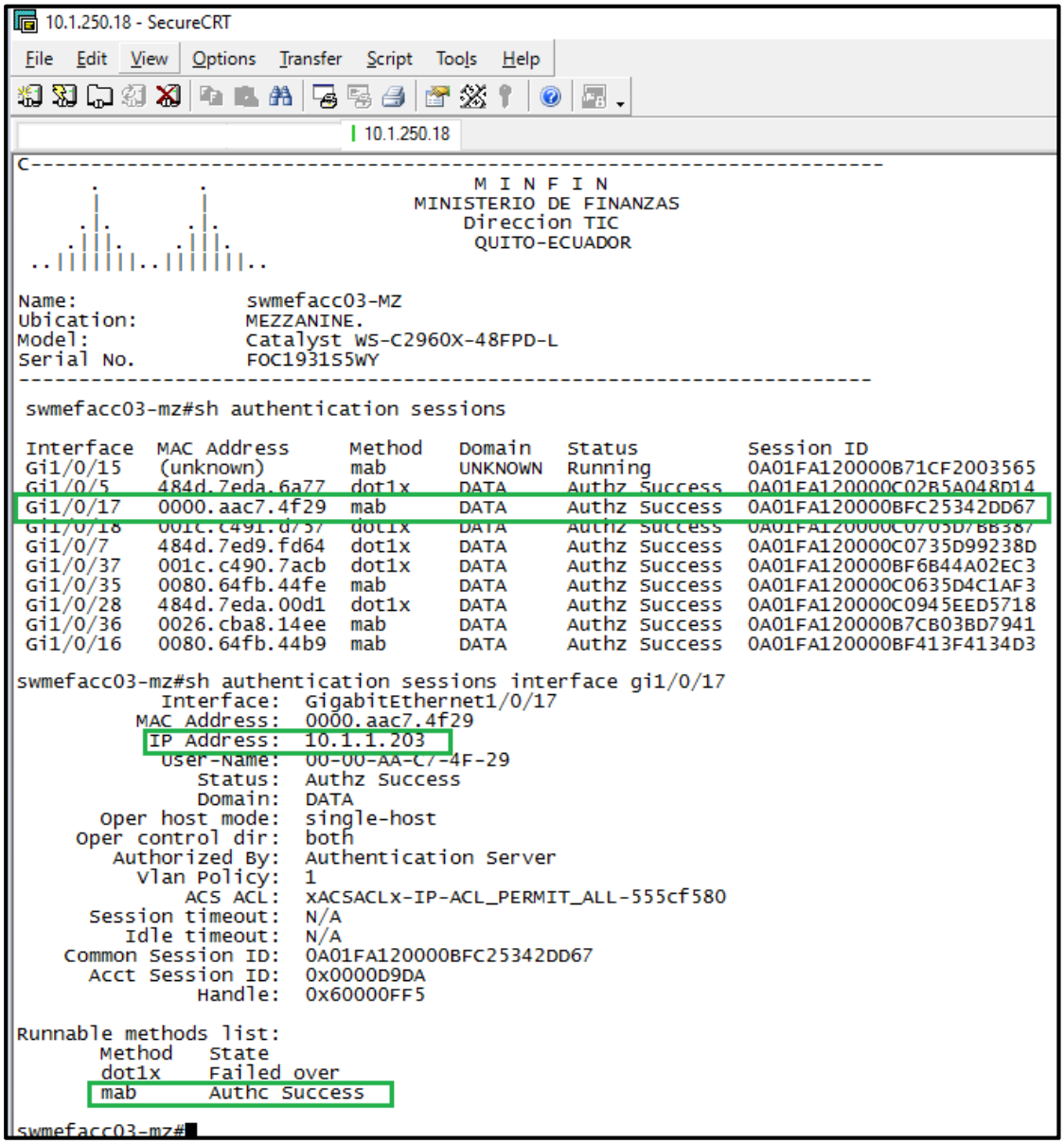


Figura 55 Comandos validación integración dispositivos MAB

- **Procedimiento para el Ingreso de Usuarios Invitados**

Una de las opciones configuradas en la "*Solución Cisco ISE – MINFIN*, es permitir la administración del portal de invitados en el caso que se requiera acceso al internet.

Se reconoce como invitado a un dispositivo que no está en el dominio "*minfin*". El requerimiento debe ser realizado por un funcionario a través de un correo electrónico solicitando el acceso a internet.

Una vez recibido la notificación mediante correo electrónico el administrador del portal de invitados procede con el siguiente procedimiento:

a) Creación del usuario invitado ingresando a la dirección web: **https://sponsor-ise.finanzas.gob.ec:8443/sponsorportal**
b) Ingreso de datos obligatorios (nombre, apellidos y dirección de correo electrónico) seguido enviar. En la siguiente Figura se expone el evento de notificación al correo electrónico del funcionario o invitado que realizó el requerimiento con las credenciales de acceso.

Figura 56 Notificación de creación de credenciales

En el caso que un usuario "*invitado*" necesite acceder a la red de datos por medio de tarjeta inalámbrica debe abrir redes inalámbricas y escoger Invitados_ISE, como se expone en la siguiente Figura.

Figura 57 Conexión SSID
"Invitados_ISE"

Para el caso que la conexión se realice por medio cableado no se requiere escoger ninguna opción, la conexión es automática. Debemos abrir un navegador e ingresar cualquier dirección, en ese momento aparece el portal de invitados , seguido ingrear nombre de usuario y contraseña y por último iniciar sesión.

Es decir unicamente debemos ingresar el usuario y la clave asignada al usuario invitado para el ingreso a la red, como se expone en la siguiente Figura.

Figura 58 Pantalla de portal de invitados

- **Procedimiento de registro dispositivos móviles (BYOD)**

BYOD es una política que permite únicamente a los funcionarios institucionales integrar sus dispositivos personales como computadores portátiles, celulares, tablets entre otros a la red de datos de esta Cartera de Estado.

Además, al utilizar estos dispositivos para acceder a la información restringida de la institución de forma segura y controlada.

Entre los dispositivos móviles que se pueden ingresar a la *"solución ISE - MINFIN"* son únicamente los que trabajen con sistemas operativos Windows, Android e IOS.

A continuación, se explica el procedimiento que se debe seguir para el ingreso de dispositivos externos a la red de datos del MINFIN.

a) Previamente en los dispositivos móviles con sistemas operativos Windows, Android se debe descargar e instalar el agente "Network Setup Assistant", el que permite realizar la descarga de los certificados desde la entidad certificadora del MINFIN.
b) En la siguiente Figura se expone el procedimiento a seguir para la conexión e instalación del agente Cisco.

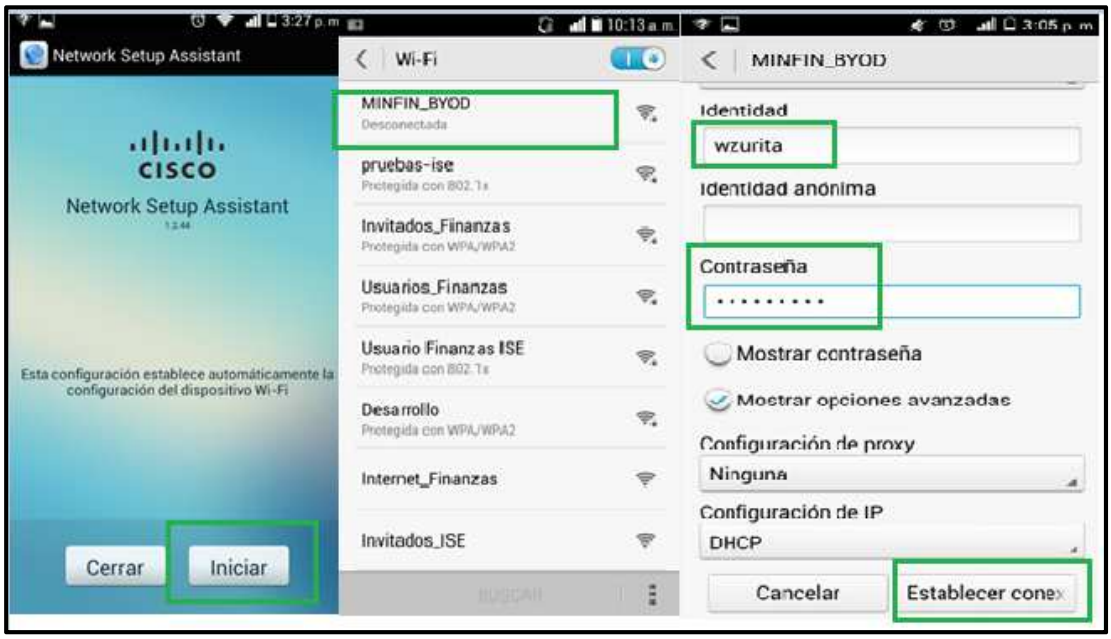


Figura 59 Conexión dispositivos móviles BYOD

c) Seguido abrir un navegador, recomendable que sea del propio sistema operativo, e ingresar cualquier dirección web por ejemplo: http://www.finanzas.gob.ec/.

d) Por último registrar el dispositivo móvil, poniendo cualquier descripción por ejemplo “wzurita” y por ultimo registrar. A continuacion se exponen la Figura de procedimiento para el registro de dispositivos móviles.

Figura 60 Registro dispositivo en la red de datos MINFIN

3.3.4 ETAPA DE CIERRE

- **Monitoreo de la Administración Solución Cisco ISE – MINFIN**

Para realizar un Troubleshooting[48] resolución de problemas más detalladamente, se creó una cuenta para el área de "Soporte Técnico" de la Dirección de Tecnología y Comunicación para el monitoreo periódico. A continuación, se detalla el modo de acceso:

a) Ingreso al ambiente de administración de la *"Solución Cisco ISE - MINFIN"*, ingresando en un navegador web la siguiente dirección: https://isemf-1.minfin.gov.ec, y con las credenciales de acceso respectivas. En la siguiente Figura se expone el acceso con credenciales de monitoreo. A fin que el personal de soporte técnico DTIC, pueda realizar análisis y solución de problemas como se indica en la siguiente Figura.

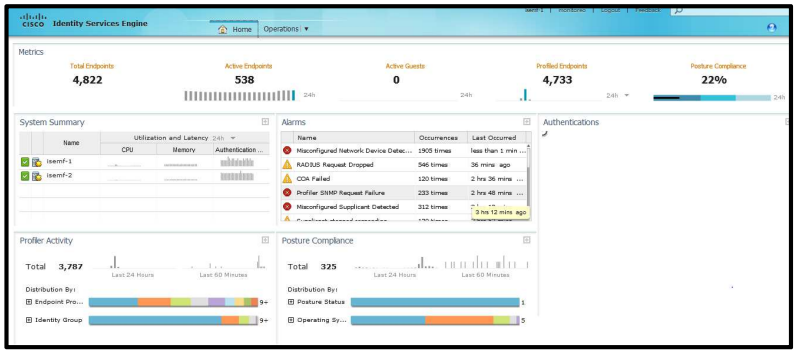


Figura 61 Monitoreo y Análisis dispositivos

- **Diagrama de Flujo y Troubleshooting Básico**

En la siguiente Figura se expone el flujograma para la instalación de los agentes de *"Cisco ISE"* y troubleshooting básico en caso de requerirlo. Esto es con fin que el área de soporte técnico tenga una base de conocimiento para resolución de problemas antes de escalar al administrador de la solución.

[48] **TROUBLESHOOTING**: ANÁLISIS Y RESOLUCIÓN DE PROBLEMAS

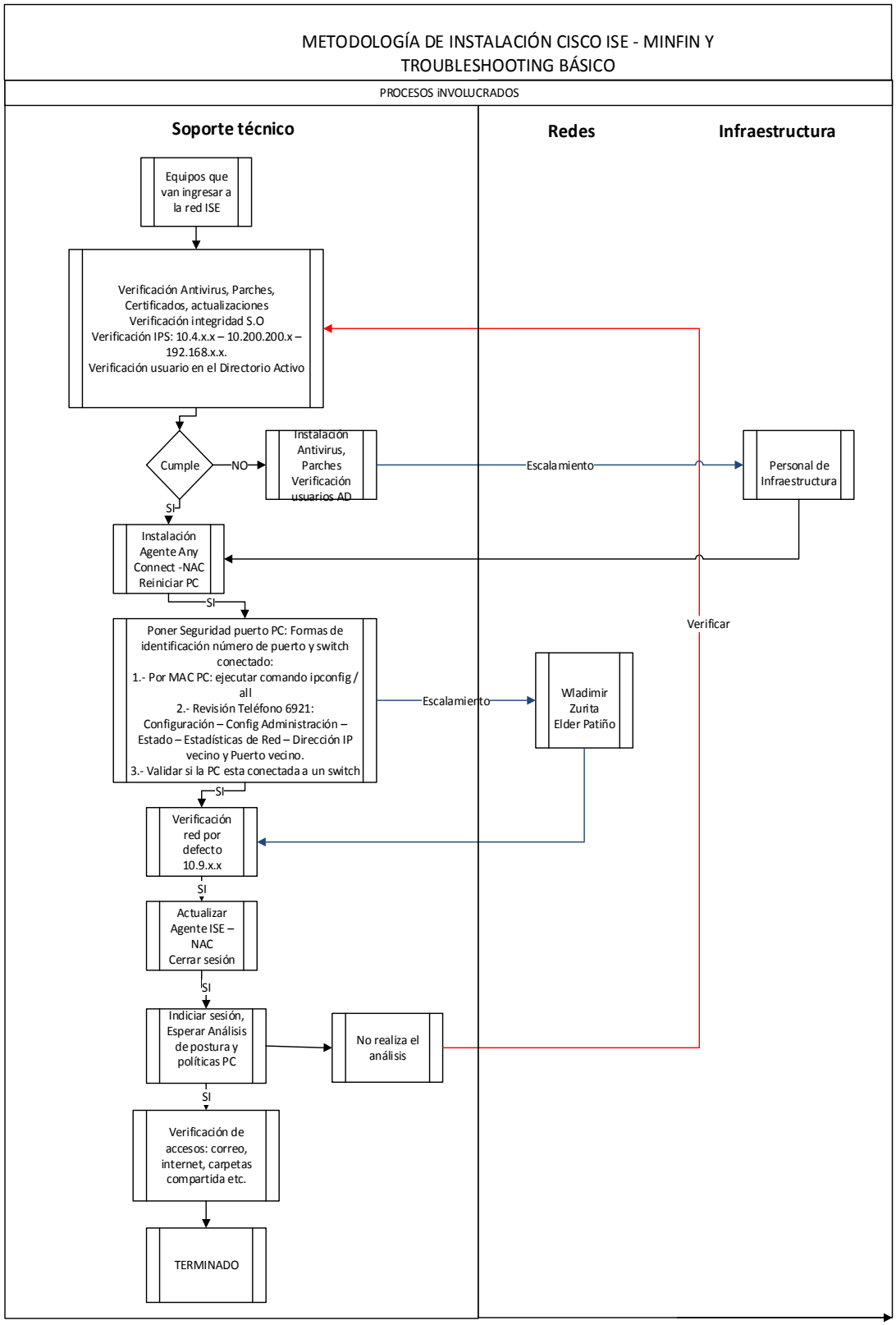


Figura 62 Flujograma de instalación y Troubleshooting Básico

- **Acompañamiento y Soporte Técnico para la Resolución de Problemas**

Durante el tiempo de acompañamiento post implementación existieron varios problemas técnicos referentes al despliegue de la *"Solución Cisco ISE"* en la red de producción del Ministerio de Finanzas.

A continuación, se indican algunos inconvenientes y soluciones a los problemas presentados:

- **Dispositivos sin certificados**

Un error común al configurar el puerto con seguridad es no tener los certificados de computador o de usuario.

Para solucionar este problema se debe realizar la solicitud de manera manual de los certificados como se expresa en la siguiente Figura.

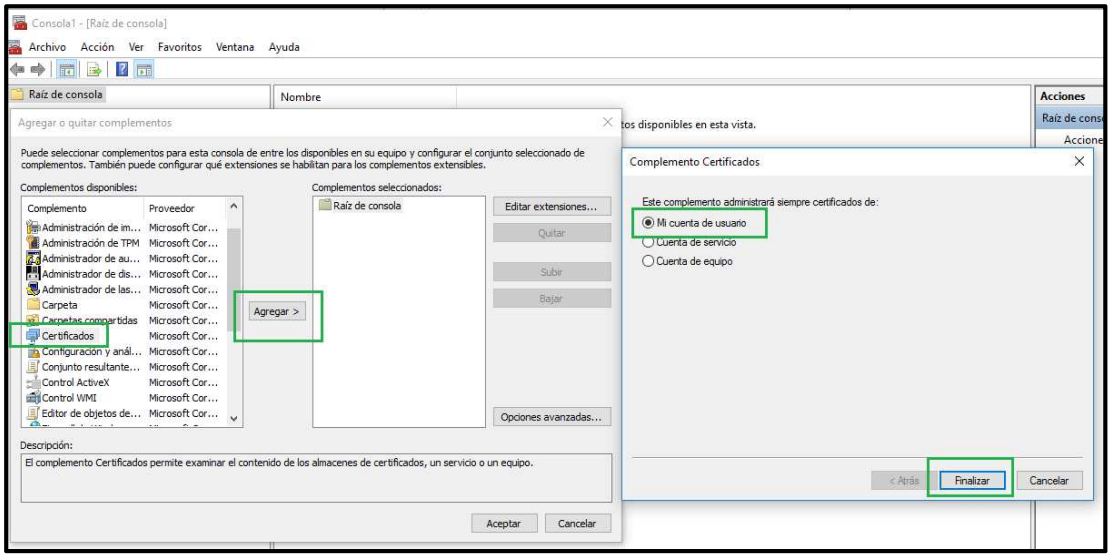


Figura 63 Invocación manual de certificados

- **Usuarios internos redireccionan al portal de Invitados**

Uno los errores comunes es cuando un usuario no está agregado a los grupos del directorio activo, para el *"Perfilamiento"* como resultado se direcciona a la VLAN de *"Remediación"* apareciendo en el navegador el portal de "invitados" para la autenticación.

Como solución a este punto debemos escalar a los administradores del *"Directorio Activo"* para el ingreso del usuario al grupo de seguridad que pertenezca en el AD.

Al ejecutar el ingreso del usuario con problemas al grupo de AD correspondiente, el usuario es asignado a la VLAN institucional que pertenece, como se expone en la siguiente Figura.

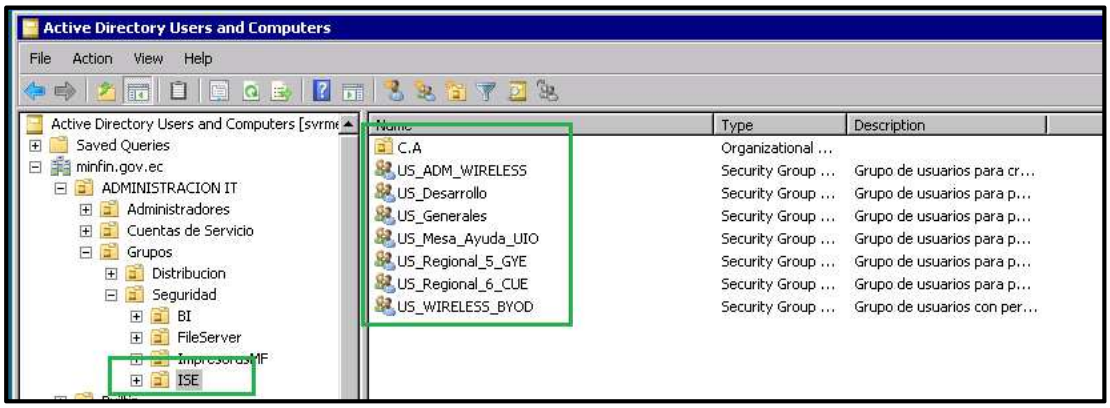


Figura 64 Usuarios AD integrados "Cisco ISE - MINFIN"

- **Servicios de Antivirus Detenidos**

Dentro de los problemas frecuentes son los servicios de antivirus detenidos. Por tal motivo el Agente NAC al validar los requerimientos de acceso a la red, detecta que no tiene antivirus, enviando al equipo o dispositivo a la red de *"Remediación"* 10.9.X.X/16.

Para solucionar este inconveniente se debe escalar a los administradores de antivirus para determinar la razón del problema.

- **Discusión de Resultados**

Una vez realizado el acompañamiento al personal de soporte técnico de la DTIC, durante el tiempo post implementación se ha validado que la mejora de la "Solución Cisco ISE – MINFIN" está al 100% probada.

En casos de presentar errores de conexión con el usuario y la red, se recomienda realizar validaciones de toda la infraestructura para establecer la causa real del problema, y no centrase únicamente en la *"Solución de Cisco ISE"*. Debido a que puede estar el problema en servidores como: DNS, DHCP, antivirus, central telefónica, directorio activo, o puntos finales como: computadores, teléfonos IP e impresoras.

Para conocimiento general el trabajo de la *"Solución Cisco ISE - MINFIN"*, es efectuar AAA y hacer cumplir requerimientos definidos.

La *"Solución Cisco ISE - MINFIN"*, no hace el trabajo de DHCP para direccionamiento o registros de teléfonos.

3.4 Evidencias Obtenidas con el Mejoramiento de la "Solución de Cisco ISE"

El Ministerio de Finanzas, por tratarse de una entidad estatal que maneja el sistema financiero más grande a nivel nacional "eSIGEF", debe proteger y asegurar los datos que transita a nivel de su red interna institucional.

Al mejorar la *"Solución Cisco ISE - MINFIN"*, uno de los logros más importantes obtenidos en cuanto a protección y seguridad informática, fue el de frenar

la propagación del ataque “Ransomware”[49] virus denominado como “WannaCry”[50] en la red interna institucional.

Este troyano se ejecutó a nivel global en el Ecuador el viernes 12 de mayo de 2017, Intentando afectar a varias empresas e instituciones estatales como el Ministerio de Finanzas.

Según José Vinicio Freire Rumazo, Oficial de Seguridad de la Información del Ministerio de Finanzas, menciona que el virus puede entrar de diferentes formas. Como por ejemplo: dispositivos externos infectados, ataque directo al dominio, y en el caso particular de esta Cartera de Estado por “Phishing”[51] como se expone evidencia de la siguiente Figura.

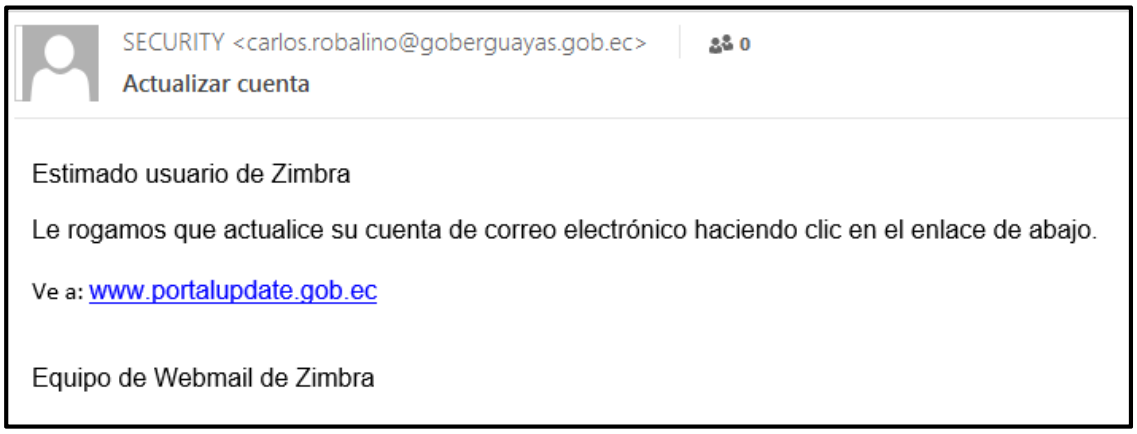


Figura 65 Correo electrónico que ingreso a los buzones – MINFIN

Este tipo de correos electrónicos mal intencionados, ingresaron a varios buzones de funcionarios del MINFIN. El link “www.portalupdate.gob.ec” direccionaba a una página que contenía el virus Ransomware *“WannaCry”*.

Al momento que el virus Ransomware *“WannaCry”*, establece la conexión con el sitio maliciosa e ingresa al computador del funcionario víctima, elimina 3 ficheros

[49] **RANSOMWARE:** SUS SIGLAS PROVIENEN DE RANSOM 'RESCATE', Y WARE, “POR SOFTWARE’ PROGRAMA INFORMÁTICO QUE CIFRA LA INFORMACIÓN Y PIDE DINERO COMO RESCATE.

[50] **WANNACRY**: ES LA EVOLUCIÓN DE UN RANSOMWARE, ES UN VIRUS TROYANO QUE ENCRIPTA FICHEROS ES LA EVOLUCIÓN MÁS SOFISTICADA DEL CRYPTOLOCKER.

[51] **PHISHING:** SUPLANTACIÓN DE IDENTIDADES

importantes para el correcto funcionamiento del antivirus “Symantec”, como se expone en la siguiente Figura.

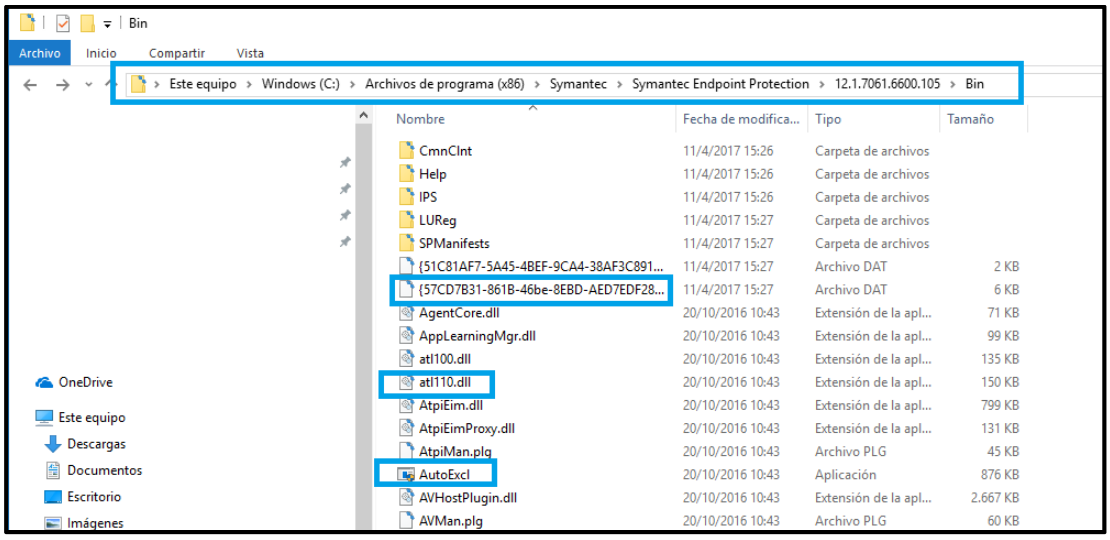


Figura 66 Eliminación archivos de instalación Symantec

Además, se identificó como evidencia que esta evolución de virus Ransomware “WannaCry” detiene los servicios de protección en tiempo real del antivirus “Symantec”, como se expone en la siguiente Figura.

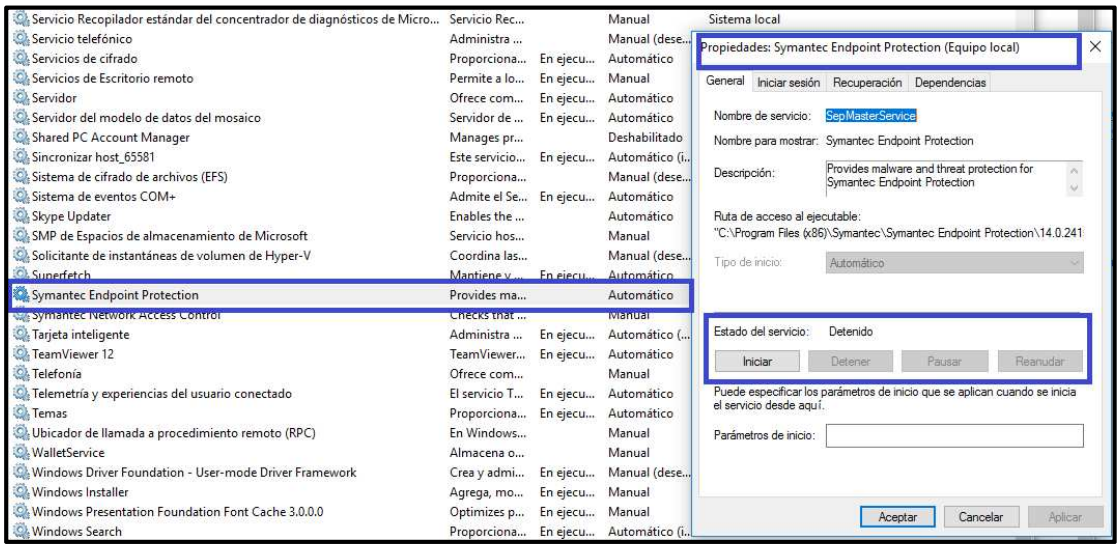


Figura 67 Evidencia “Detiene servicios antivirus”

En la siguiente Tabla, se describe los incidentes que han sido detectados por personal de la Dirección de Tecnologías y Comunicación con la ayuda de la

"Herramienta antispan de Symantec - MINFIN" o reportados por los servidores/as públicos de esta Cartera de Estado. Relacionados a correos no deseados recibidos, los mismos que después de ser analizados se ejecutaron acciones dependiendo del caso.

Tabla 18
Reporte de incidentes y acciones realizadas: mayo 2017

Fecha	Tipo	Remitente	Dirección IP	Acciones realizadas
01/05/2017	Publicidad	ringcentral@mindspring.com	175.139.242.50	Remitente bloqueado. Total de correos: 1
19/05/2017	Publicidad	servicios@genialecuador.com	192.185.148.194	Remitente bloqueado. Total de correos: 19
12/05/2017	Phishing	carlos.robalino@gobierguayas.gob.ec	89.26.123.25	Remitente bloqueado. Total de correos: 352

3.5 Discusión de resultados

El Mejoramiento de la *"Solución Cisco ISE - MINFIN"* mediante la característica de *"Postura"*, permitió que cuando el virus Ransomware *"WannaCry"*, detenga los servicios de *"Symantec Antivirus"* en los computadores institucionales, envié inmediatamente a la red aislada de "Remediación 10.9.X.X/16". Con el fin de frenar la propagación de este virus mal intencionado en la red de datos institucional. Afectando la integridad de la información que transita en esta institución.

3.6 Orientación y Cumplimiento del Acuerdo 166 EGSI

Una vez realizado el *"Mejoramiento de la Solución Cisco ISE - MINFIN"*, ayudará a esta Cartera de Estado al cumplimiento de manera eficiente los dominios, controles y controles de dominio que el EGSI *"Esquema Gubernamental de Seguridad de Información "* que dispone se implementen en las entidades de la Administración

Pública Central que dependen de la Función Ejecutiva emitida mediante el Acuerdo No. 166 del 19 de septiembre de 2013.

Es importante recalcar que el *"Esquema de Seguridad de la Información EGSI"* está basado en la familia *"ISO/IEC 27002*" como se indica en los capítulos anteriores. Esta norma es el código para el cumplimiento de las buenas prácticas y la gestión de seguridad de la información.

Su estructura radica en la descripción de objetivos de control y controles recomendables en implementaciones de seguridad de la información. Consta de 14 dominios con 35 objetivos de control y 114 controles en su última versión.

Existe una pregunta muy importante ¿Con el Mejoramiento de la Solución Cisco ISE – MINFIN, cumpliremos todo el acuerdo 166? la respuesta es simple y sencilla, el mejoramiento de la *"Solución Cisco ISE – MINFIN"* ayuda enormemente al cumplimiento únicamente de ciertos controles y objetivos de control según su afinidad.

Con base a esta pregunta, en la siguiente Tabla se efectúa el análisis de los de 14 dominios, 35 objetivos de control y 114 controles del *"Acuerdo 166 basado en la norma ISO 27002*" que cumple esta Cartera de Estado con el *"Mejoramiento de la solución Cisco ISE - MINFIN"*.

Tabla 19
Cumplimiento controles EGSI - Solución Cisco ISE

DOMINIO	**CONTROLES**	**CONTROLES DE DOMINIO**
Políticas de Seguridad de la Información.	Orientación de la dirección para la Gestión de la Seguridad de la información	Políticas de la seguridad de la información.
Organización de la seguridad de la Información	Dispositivos Móviles y Teletrabajo.	Política de Dispositivos Móviles Teletrabajo.

Gestión de Activos	Responsabilidad por los activos.	Inventario de Activos.
Control de Acceso	Requisitos del negocio para el control de acceso.	Acceso a redes y servicio de red. Políticas de control de acceso
	Gestión de acceso de usuarios.	Revisión de los derechos de acceso.
Seguridad de Operaciones.	Gestión de Vulnerabilidad Técnica.	Restricción sobre la instalación de Software.
Seguridad de la Comunicaciones.	Gestión de Seguridad de las redes.	Controles de Redes. Seguridad de los servicios de Red. Separación en las Redes.
Gestión de incidentes de la seguridad de la información.	Gestión de incidentes y mejoras en la seguridad de información.	Reporte de eventos de seguridad de la información. Recolección de evidencia.
Cumplimiento	Cumplimiento de requisitos legales y contractuales.	Privacidad y protección de la información y datos personales.
	Revisión de Seguridad de la información.	Cumplimiento con políticas y normas de seguridad.

3.7 Decisión para adquirir Soluciones Cisco en el Ministerio de Finanzas

Como se explicó en capítulos anteriores el Ministerio de Finanzas, es una de las entidades estatales más importantes a nivel de estado. Debido a la complejidad en el manejo de las finanzas públicas a nivel nacional.

Las Direcciones Tecnológicas internas de esta Cartera de Estado, apoyan tecnológicamente a los funcionarios institucionales y administran el *"Sistema de Gestión Financiera eSIGEF"*, medio fundamental para el manejo y gestión financiera de todas la entidades públicas y municipales a nivel nacional.

La alta Gerencia Tecnológica del Ministerio de Finanzas con el apoyo de sus Analistas Técnicos, observaron a *"Cisco Systems"* un aleado tecnológico por ser un

líder mundial de redes y comunicaciones. Además, por su diversidad en soluciones tecnológicas de redes y comunicaciones “networking”, seguridad informática, soporte técnico, canales de garantía en el país y su constante evolución e innovación en soluciones informáticas.

Desde los inicios tecnológicos del MINFIN, expertos de *“Cisco Systems”* han apoyado técnica y conceptualmente con los diseños e implementación de soluciones de redes y seguridades informáticas que satisfagan las necesidades de esta organización.

En el caso puntual de la adquisición *“Solución de Control de Acceso, Remediación, Profiling y servicios AAA para la red de datos del Ministerio de Finanzas”*, implementada desde 27 junio de 2015, bajo la administración de la Dirección de Tecnología y Comunicación del MINFIN.

Tanto la parte Directiva en conjunto con los Analistas de Tecnologías y Comunicación de esta institución, antes iniciar el proceso de adquisición de la *“Solución Cisco ISE - MINFIN”* analizaron estos dos aspectos fundamentales que se referencian a continuación:

3.7.1 Unificación y Centralización de los equipos Cisco existentes en el MINFIN

Esta Cartera de Estado cuenta con equipos como: switches, routers, teléfonos IP, controladora inalámbrica, central telefónica IP, access points, Firewalls y demás equipos de comunicaciones con tecnología Cisco.

Mediante la adquisición de la *“Solución Cisco ISE - MINFIN”* se unificará todos los equipos de tecnología Cisco. A fin de facilitar la administración, monitoreo y convertir desde un punto de vista técnico una red de datos inteligente por las características de Cisco ISE.

3.7.2 Soporte y Garantía Técnica en Ecuador

Cisco Systems, cuenta con oficinas en Ecuador ubicados en Eurocenter Diursa Building, Piso 6. Avenida Amazonas 37-29 Quito, Pichincha. Además, con una serie de canales aleados distribuidores directos calificados por en tres categorías Oro, Plata y Bronce.

Cisco Systems, califica a sus canales de distribución con estas tres categorías dependiendo de varios factores, por ejemplo: su personal técnico altamente capacitado y calificado, experiencia en el mercado, enfoque de cliente y otros aspectos. Con el fin de brindar a los clientes como el Ministerio de Finanzas, el total respaldo técnico y garantía de los equipos ante fallos y problemas.

3.8 Análisis de retorno de Inversión "Solución Cisco ISE-MINFIN"

- **Antecedentes**

Esta Cartera de Estado suscribió el contrato SIE-MF-038-2014 de fecha 28 de enero de 2015, por un valor de USD 100.000 dólares americanos, para la *"Implementación de una Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la Red de Datos Institucional"*.

- **Análisis Valor Actual Neto (VAN) y Tasa Interna de Retorno (TIR)**

Con el valor de inversión de USD 100.000 dólares americanos, señalado en el párrafo anterior, procederemos a realizar los cálculos del VAN y TIR.

Estos cálculos permitirán determinar si la *"Implementación de una Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la Red de Datos Institucional"*, es rentable en el tiempo.

- **Análisis del Valor Actual Neto (VAN)**

Todo proyecto tecnológico debe analizarse de acuerdo a su viabilidad y la rentabilidad que genera. Cuando se plantea la necesidad de un proyecto hay que invertir un capital, y esperar la rentabilidad a través de los años.

El VAN tiene tres componentes básicos que son:

- ✓ Inversión Inicial $\boldsymbol{I_0}$
- ✓ Flujos Futuros $\boldsymbol{F_t}$
- ✓ Tasa de Retorno o descuento $\boldsymbol{r}$

Para que un proyecto sea rentable, se espera que el VAN sea positivo. El VAN debe ser positivo porque se obtiene mayores flujos futuros posibles y tasa de retorno pequeña.

Además, significa que la rentabilidad a obtener del proyecto supera la tasa de retorno. esperada.

Determinemos que la rentabilidad del proyecto *"Implementación de una Solución de Control de Acceso, Remediación, Profiling y Servicios AAA para la Red de Datos Institucional",* se invirtió USD 100.000 dólares americanos y que nos ofrece el siguiente flujo dentro de los próximos 5 años, a una tasa de retorno de 14%.

Donde el:

Valor Total del Proyecto: **USD 100.00**

Tabla 20
Flujos Futuros dentro de los primeros 5 años

	Año 1	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Flujo Neto	USD 27.680	USD 28.970	USD 31.200	USD 42.100	USD 45.000

Beneficio Neto Nominal: USD 174.950

Ganancia Nominal: USD 174.950 + USD 100.00 = USD 74.950

Nota: Para el resultado anterior la ganancia no es real, debido a que no se considera la "Rentabilidad mínima" ni el valor del dinero en el tiempo. Aquí comienza a desempeñar el papel de VAN.

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{[1+r]} t$$

$$\frac{F_1}{(1+0{,}14)}\mathbf{1} + \frac{F_1}{(1+0{,}14)}\mathbf{2} + \frac{F_1}{(1+0{,}14)}\mathbf{3} + \frac{F_1}{(1+0{,}14)}\mathbf{4} + \frac{F_1}{(1+0{,}14)}\mathbf{5} \text{ - } \mathbf{100.000}$$

$$\frac{\mathbf{27.680}}{(\mathbf{1,14})}\mathbf{1} + \frac{\mathbf{28.970}}{(\mathbf{1,14})}\mathbf{2} + \frac{\mathbf{31.200}}{(\mathbf{1,14})}\mathbf{3} + \frac{\mathbf{42.100}}{(\mathbf{1,14})}\mathbf{4} + \frac{\mathbf{45.000}}{(\mathbf{1,14})}\mathbf{5} - \mathbf{100.000} = \mathbf{15.929,46}$$

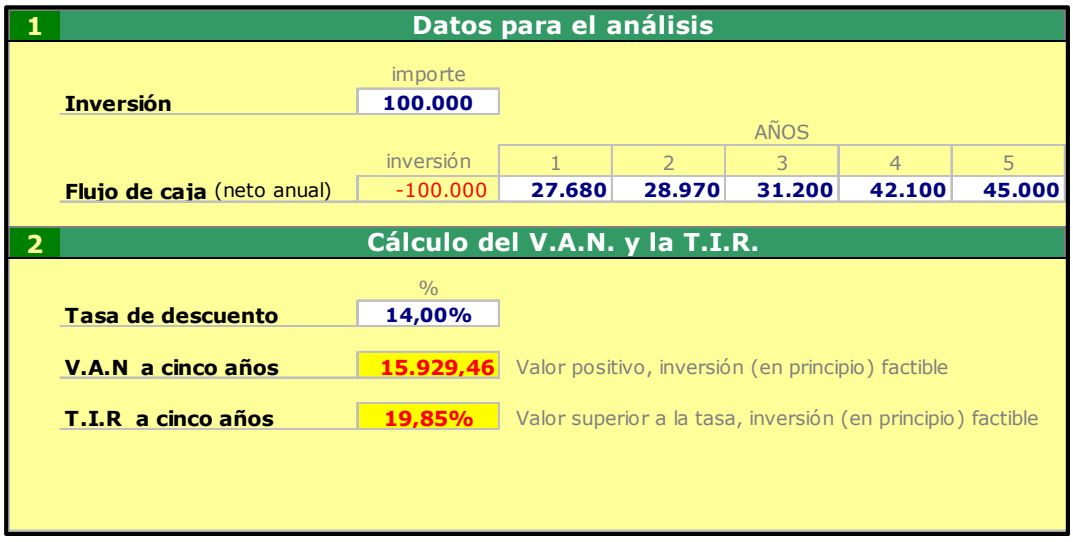
- **Análisis Tasa Interna de Retorno (TIR)**

Buscar el TIR, implica que necesariamente que el VAN es cero

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{[1+r]} t = 0$$

$$\frac{\mathbf{27.680}}{(\mathbf{1}+\boldsymbol{r})}\mathbf{1} + \frac{\mathbf{28.970}}{(\mathbf{1}+\boldsymbol{r})}\mathbf{2} + \frac{\mathbf{31.200}}{(\mathbf{1}+\boldsymbol{r})}\mathbf{3} + \frac{\mathbf{42.100}}{(\mathbf{1}+\boldsymbol{r})}\mathbf{4} + \frac{\mathbf{45.000}}{(\mathbf{1}+\boldsymbol{r})}\mathbf{5} - \mathbf{100.000} = \mathbf{0,198}$$

En la siguiente Figura se expresa los cálculos del Valor Actual Neto (VAN) Y Tasa Interna de Retorno (TIR) usando ecuaciones predefinidas en la hoja de cálculo De Microsoft Excel.



1	Datos para el análisis						
		importe					
	Inversión	**100.000**					
			AÑOS				
		inversión	1	2	3	4	5
	Flujo de caja (neto anual)	-100.000	**27.680**	**28.970**	**31.200**	**42.100**	**45.000**

2	Cálculo del V.A.N. y la T.I.R.		
		%	
	Tasa de descuento	**14,00%**	
	V.A.N a cinco años	**15.929,46**	Valor positivo, inversión (en principio) factible
	T.I.R a cinco años	**19,85%**	Valor superior a la tasa, inversión (en principio) factible

Figura 68 Cálculo VAN y TIR mediante EXCEL

Fuente: **(LPS, 2015)**

- **Discusión del Análisis Financiero**
  - ✓ Los valores futuros fueron considerados de acuerdo a los beneficios obtenidos con el mejoramiento de la *"Solución Cisco ISE - MINFIN"* dentro de los primeros 5 años de implementación.
  - ✓ Además, en los valores futuros se considera el ahorro que el MINFIN tendrá al no contratar consultoras externas para afinamiento de la solución, capacitación al personal técnico y herramientas de terceros por el desconocimiento del potencial de la solución *"Mejorada Cisco ISE - MINFIN"*

CAPÍTULO IV

CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURO

CONCLUSIONES

- En esta tesis se fortaleció con éxito la seguridad informática del Ministerio de Finanzas, por medio del mejoramiento de la "*Solución actual de Control de Acceso, Remediación, Profiling y Servicio AAA del Ministerio de Finanzas*". Mediante la cual se mejoró los servicios tecnológicos institucionales, proporcionando altos niveles de seguridad, disponibilidad y cumplimiento de políticas internas institucionales.
- Con el afinamiento de las características de Remediación, Profiling y servicios AAA, de la solución *"Cisco ISE - MINFIN"* en la red cableada e inalámbrica, se obtuvo mayor control y visibilidad de los dispositivos que ingresan a la red de datos institucional, tanto de usuarios institucionales como invitados.
- Mediante la inducción impartida al personal técnico de la Dirección de Tecnologías y Comunicaciones del MINFIN, se explicó como monitorear y visualizar los reportes de la solución *"Cisco ISE - MINFIN"* que permitan mostrar información en tiempo real de los procesos de autenticación, accounting, cumplimiento de políticas, Profiling, acceso de invitados y sesiones de autenticación de todos los eventos que suceden a nivel de red.
- Con el mejoramiento de la solución *"Cisco ISE - MINFIN"* esta institución logró cumplir de manera eficiente algunos dominios, controles y controles de dominio que el "*Esquema Gubernamental de Seguridad de Información"* basado en la norma técnica INEN ISO/IEC 27002, que dispone se implementen en las entidades de la Administración Pública Central.

LÍNEAS DE TRABAJO FUTURO

- Indicar a las autoridades y funcionarios de las diferentes subsecretarias, coordinaciones y direcciones de esta Cartera de Estado, referente a las ventajas de seguridad informática y pontenciabilidad de la solución "*Cisco ISE"* que se encuentran desplegada en la red de datos institucional.
- Fomentar la comunicación adecuada entre personal de soporte técnico a usuarios y los responsables de la administración de la solución "*Cisco ISE"* de la Dirección de Tecnologías de la Información y Comunicación. A fin de brindar alternativas proactivas a los incidentes que reportan los funcionarios y usuarios externos referente al ingreso a la red de datos institucional.
- Analizar futuras mejoras en cuanto a implementar una solución de reportería, detección de amenazas, visualización de ataques, correlación de eventos entre otras, mediante la integración de equipos ya sea con fabricantes de la misma marca o de otras. A fin de fortalecer la seguridad de red interna y estar un paso adelante ante nuevas amenazas que atenten con la integridad de la información del Ministerio de Finanzas.

REFERENCIAS BIBLIOGRÁFICAS

Heary, Jamey., Wolland, Aron. (2013). *Cisco ISE for BYOD and Secure Unified Access*. Indiana-EEUU: Cisco Press Editorial.

Wolland, Aron. (2015). *CCNP Security SISAS 300-208 Official Cert Guide.* Indiana-EEUU: Cisco Press Editorial.

Wolland, Aron. (2016). *Security Solutions: All-in-one Cisco ASA FirePOWER Services NGIPS, and AMP*. California-EEUU: Cisco Press Editorial.

Ritcher, Andy., Wood, Jeremy. (2015). *Practical Deployment of Cisco Identity Services Engine (ISE)*. California -EEUU: Cisco Press Editorial.

Redouane, Meddane. (2016). *Cisco ISE and ACS Configuration: Labs WorkBook (English Edition)*. Indiana-EEUU: Cisco Press Editorial.

Rifkin, Jeremy. (2011). *La Tercera revolución Industrial*. Colorado-EEUU: Editorial: Paidos Ibérica.

Calder, Alan. (2009). *Information Security Based on ISO 27001/ISO 27002 A Management Guide.* Virginia-EEUU: Van Haren Editorial.

Columba, Edgar. (2016). *Fundamentos de Seguridad de la Información basados en ISO 27001/27002.*

Hintzbergen, Jule. (2015). *Foundations of Information Security: Based on ISO 27001 and ISO 27002.* Virginia-EEUU: Van Haren Editorial.

Calder, Alan., Watkins, Steve. (2008). *IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002*. Virginia-EEUU: London and Philadelphia Editorial.

Miller, Agnes., Vandome, John. (2010). *ISO/IEC 27002.* California-EEUU: McBrewster Editorial.

Hogan, Christina., Limoncelli, Thomas., Strata, Chalup. (2016). *The Practice of System and Network Administration*.

Wang, Ping., Zhuang, Weihua. (2013). *Distributed Medium Access Control in Wireless Networks.* California-EEUU: SpringerBiefs Editorial.

Diaz, M. (2013). *Matemáticas Financieras.* Guadalajara-México: Mcgraw-Hill Editorial.

Chen, Hsinchun. (2006). *Intelligence And Security Informatics.* Virginia-EEUU: London and Philadelphia Editorial.

Mulcahy, Rita. (2013). *Preparación para el Examen PMP*, Octava Edición. California-EEUU: RMC Publication Editorial.

Cepeda, Andrés. (2013). *Expertos enseñando a Expertos*. *Netec*. Recuperado el 24 de octubre de 2013, de https://www.netec.com.mx/implementing-and-configuring-cisco-identity-services-engine

Wymerszberg, Gustavo. (2013). *La problemática de la gestión en las soluciones de BYOD. Logicalis.* Recuperado el 15 de marzo de 2013, de

http://www.la.logicalis.com/globalassets/latin-america/logicalisnow/revista-20/lnow20-nota-36-37.pdf

Madrial, Sergio. (2014). *Seguridad en Redes: Arquitectura AAA – Authentication, Authorization and Accounting. SergioMadrigal*. Recuperado el 3 de julio de 2014, de http://www.sergiomadrigal.com/2014/01/13/seguridad-en-redes-arquitectura-aaa/

McNamara, Katherine. (2017). Cisco ISE: Device Profiling. Dark Reading. Recuperado el 5 de noviembre de 2017, de https://www.networkcomputing.com/network-security/cisco-ise-device-profiling/1803763843