UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

TÍTULO:
DISEÑO DE ESTRATEGIAS PARA LA SEGURIDAD DE LAS COMUNICACIONES EN EL DEPARTAMENTO DE GESTIÓN DE ARCHIVO AUDIOVISUAL DEL CANAL TRO SEDE FLORIDABLANCA

Autor:
ELMER YESID MOLINA GELVEZ

Director:
ING. JOHRMAN DE JESÚS VIDES NIÑO

PAMPLONA-COLOMBIA

JULIO DE 2019

UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO EN TELECOMUNICACIONES

TÍTULO:
DISEÑO DE ESTRATEGIAS PARA LA SEGURIDAD DE LAS COMUNICACIONES EN EL DEPARTAMENTO DE GESTIÓN DE ARCHIVO AUDIOVISUAL DEL CANAL TRO SEDE FLORIDABLANCA

Autor:
ELMER YESID MOLINA GELVEZ

Director:
ING. JOHRMAN DE JESÚS VIDES NIÑO

JURADO CALIFICADOR:
Ing. JOHRMAN DE JESÚS VIDES NIÑO
M.Sc (c). EDWIN MAURICIO SEQUEDA ARENAS
M.Sc. NYDIA SUSANA SANDOVAL CARRERO

PAMPLONA-COLOMBIA

JULIO DE 2019

UNIVERSIDAD DE PAMPLONA
FACULTAD DE INGENIERÍAS Y ARQUITECTURA
DEPARTAMENTO DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, SISTEMAS Y TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES

TRABAJO PRESENTADO PARA OPTAR POR ÉL TITULO DE INGENIERO EN TELECOMUNICACIONES

TEMA:

DISEÑO DE ESTRATEGIAS PARA LA SEGURIDAD DE LAS COMUNICACIONES EN EL DEPARTAMENTO DE GESTIÓN DE ARCHIVO AUDIOVISUAL DEL CANAL TRO SEDE FLORIDABLANCA

FECHA DE INICIO DEL TRABAJO: FEBRERO 2019

FECHA DE TERMINACIÓN DEL TRABAJO: JULIO 2019

NOMBRES Y FIRMAS DE AUTORIZACIÓN PARA LA SUSTENTACIÓN:

_____
ELMER YESID MOLINA GELVEZ
AUTOR

_____ _____
ING. JOHRMAN VIDES NIÑO **M.Sc. HERNANDO VELANDIA V.**
DIRECTOR **DIRECTOR DEL PROGRAMA**

JURADO CALIFICADOR:

_____ _____
ING. JOHRMAN VIDES NIÑO **M.Sc (c). EDWIN SEQUEDA ARENAS**

_____
M.Sc . NYDIA S. SANDOVAL C.

PAMPLONA N. S. COLOMBIA
JULIO DE 2019

“A Dios por brindarme la sabiduría,
a mis padres, mis hermanos y
amigos, por toda la confianza y
acompañamiento”.

“A mi madre María Eugenia, que nunca perdió la fe en mi”.

AGRADECIMIENTOS

A Dios, a mis padres María y Carlos por ser ese puntal que todos necesitamos en la vida por quererme sin condiciones y saber perdonar mis errores.

A mis Hermanos, Deicy y Said que sin su ayuda y paciencia no podría alcanzar este momento que estuvieron siempre pendientes de mí persona y que culmine con éxito esta etapa de mi vida no me queda más que agradecerles que me ayudaron a tomar decisiones correctas a lo largo de este camino.

Al Profesor Javier Mogollón, por su apoyo incondicional durante años, que permitieron tener un gran amigo y un gran guía.

Agradezco a todos mis profesores por todos los detalles que aportaron a mi formación profesional, por todo el conocimiento impartido y los buenos consejos que me brindaron.

Por último, quisiera agradecer al canal TRO que me abrió las puertas para realizar las practicas, de la misma forma quiero agradecer a los ingenieros del área Técnica.

A todos y cada una de las personas que hicieron parte de lo que hoy es para mí alcanzar este logro, decirles, ¡Gracias!

RESUMEN

El presente trabajo se enmarca en el diseño de estrategias de un sistema de gestión de la seguridad de las comunicaciones A.13 basado en la norma ISO/IEC 27001:2013 para la red del Canal TRO sede Bucaramanga. Se parte por conocer la norma ISO/IEC 27001:2013 anexo A.13. que permite mantener su objetivo de negocio controlando los riesgos de la perdida de información que puedan afectar desde su imagen pública hasta sus finanzas. Para aplicar las recomendaciones del anexo A.13, se realizó el reconocimiento de los activos de la empresa siguiendo la metodología MAGERIT V3, para determinar los recursos importantes, identificando las amenazas o ataques de los que pueden ser víctimas estos activos, así como también se realiza un análisis de los riesgos para definir el criterio de mitigación de los mismos.

El desarrollo de análisis y gestión de los riesgos, se realizó mediante la metodología antes mencionada, la cual permite a definir un espectro de amenazas determinando su importancia, para luego aplicar de acuerdo a la política y las necesidades del Canal TRO, una serie de Salvaguardas que permiten mitigar, controlar o transferir el riesgo de los activos a proteger y cumplir las recomendaciones de la norma ISO, teniendo en cuenta como se mencionó anteriormente que las decisiones y recomendaciones de los criterios de selección de dichos salvaguardas, obedece enteramente a las de la empresa para tratar el riesgo. En ese sentido, se propone el empleo de un servidor de dominio, para la autenticación de los usuarios de gestión de archivo, y el monitoreo de la red a través de *SNMP*, como una de las recomendaciones para el cumplimento de la sección A13 de ISO/IEC 27001:2013. Se recomendó luego del análisis de vulnerabilidades, la aplicación de las salvaguardas como un servidor de dominio AD, servidor RADIUS para la autenticación WLAN y el monitoreo SNMP empleando dude server de mikrotik.

ABSTRACT

The present work is framed in the design of strategies for an A.13 communications security management system based on the ISO/IEC 27001:2013 standard for the Canal TRO network in Bucaramanga. We start by knowing the ISO/IEC 27001:2013 Annex A.13. which allows to take into account the new control objectives and different controls to be implemented, is of vital importance for a company that wants to maintain its business objective by controlling the risks of information loss that can affect from its public image to its finances. To apply the recommendations of Annex A.13, the company's assets were recognized following the MAGERIT V3 methodology, to determine the important resources, identifying the threats or attacks of which these assets may be victims, as well as an analysis of the risks to define the criteria for mitigating them.

The development of risk analysis and management was carried out using the above mentioned methodology, which allows to define a spectrum of threats determining their importance, and then apply, according to the policy and the needs of the TRO Channel, a series of Safeguards that allow to mitigate, control or transfer the risk of the assets to be protected and comply with the recommendations of the ISO standard, taking into account as mentioned above that the decisions and recommendations of the selection criteria of such safeguards, obey entirely to those of the company to treat the risk. In this sense, it is proposed to use a domain server, for authentication of file management users, and network monitoring through SNMP, as one of the recommendations for compliance with section A13 of ISO/IEC 27001:2013. It was recommended after the vulnerability analysis, the application of safeguards such as an AD domain server, RADIUS server for WLAN authentication and SNMP monitoring using mikrotik's dude server.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Capítulo 1

Introducción

Canal TRO (Televisión Regional del Oriente) es un canal de televisión abierta colombiano, creado en 1995. El canal cubre los departamentos de Santander y Norte de Santander. Su programación es de índole educativa y cultural. Su sede central y principales estudios de transmisión se encuentran en Floridablanca, pero también realiza transmisiones desde los estudios de grabación que tienen en Cúcuta.

Actualmente no existe un control adecuado que asegure la confidencialidad, proteja la integridad de la información en su totalidad y que garantice la disponibilidad, así como la acción rápida durante el tratamiento de la información, razón por la cual no se cuenta con la correcta respuesta frente a algún error en la red del canal.

El trabajo se enfoca en estrategias para realizar los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información, a través del establecimiento de un sistema de seguridad de las comunicaciones basado en la norma ISO 27001:2013, de forma que se garantice un adecuado tratamiento de los problemas según el anexo A.13. teniendo en cuenta las mejores prácticas, valorando los riesgos y las necesidades del canal.

Para ello se evaluará el estado actual del canal frente al control A.13 seguridad en la comunicación, para el departamento de gestión de archivo audiovisual, donde se mostrará los diferentes activos con los que cuenta el canal, y así mismo tener una metodología para el cumplimiento de los controles con sus respectivas salvaguardas, que den soluciones acertadas sobre las falencias en el cumplimiento de la norma.

1.1 Planteamiento del Problema y justificación

El Canal TRO es uno de los más importantes canales de televisión abierta del Oriente Colombiano, que según su Plan Estratégico actualmente es financiado en gran parte por la ANTV y planea ser auto sostenible para el año en curso (TRO C. , Plan Estrategico situacional 202 - 2015, s.f.). Además con base en su visión institucional “en el 2019, Canal TRO será el medio de comunicación público predilecto del Oriente Colombiano, por la calidad de nuestros contenidos y servicios, aportando al progreso de la Región” (CanalTRO, s.f.) el canal plantea mejorar la oferta y calidad de sus servicios que a largo plazo permitan cumplir las meta de su Plan Estratégico. Así mismo, el balance general del canal a 31 de diciembre de 2017 (TRO C. , ESTADO DE SITUACION FINANCIERA , 2017) se observa que los mayores ingresos se encuentran en las pautas publicitarias, cesión de espacios a productoras televisión, producción de contenido propio y planes de medios, en base a ello, parte de las decisiones para aumentar los ingresos del canal, se propuso en el Plan Estratégico de 2016 – 2019 (Canal TRO, 2016) mejorar la seguridad de la información del archivo audiovisual, pues actualmente no se cuenta con un plan de acción que mejore la confidencialidad, integridad y disponibilidad de la información de esta parte importante del canal. -

Un buen indicador que Canal TRO esté a la vanguardia de la seguridad de las comunicaciones, es una certificación de índole internacional y que cada país adopta a sus necesidades, en este caso, se refiere a la norma NTC-ISO/IEC 27001 versión 2013, por ello, es conveniente que las directivas del Canal hayan optado por empezar el proceso para lograr la certificación en NTC-ISO/IEC 27001:2013 que permitan; una ventaja competitiva, para demostrar que se regirán bajo estrictos estándares internacionales y que todos o parte de sus procesos funcionan de acuerdo a las mejores prácticas; un cumplimiento legal, pues cumpliendo la NTC-ISO/IEC 27001:2013 se hallará un camino más adecuado y sencillo para cumplir leyes nacionales como la 1273 de 2009 o también conocida como la Ley de Delitos

Informáticos, que entre otros delitos tipifica la omisión de responsabilidades como causal de penalidades; una confianza y credibilidad, que demuestra a sus cliente y proveedores aseguramiento de la información cedida al canal como avances de producciones, publicidad de un nuevo producto o primicias noticias o cualquier otro tipo de información que divulgada de forma no esperara pueda tener impacto económico negativo.

Al momento de realizar un análisis de la forma en cómo se maneja la red LAN del canal, se evidencia la falencia en los procesos para garantizar la protección de los datos y la seguridad física de los recursos, esto conlleva que en momentos no se tenga una respuesta adecuada a los posibles errores, que se puedan producir en la red pues al realizar un test básico, se evidencia que la red no se encuentra segmentada y se alcanzan diferentes secciones que no deberían visualizarse.

Adicionalmente se observa que los ataques a los dispositivos de red o de usuarios crean baja disponibilidad de la información, por ejemplo, el ataque a un servidor de contenidos, donde la gestión de contenidos de la parrilla televisa es primordial para un canal de televisión. La negligencia por parte de empleados en el olvido de claves genera retrasos y evidencia la falta de control de la organización en la gestión de claves. La necesidad de segregar los roles y responsabilidades de los empleados para evitar que estos eludan un problema en caso de ataques a la seguridad de la información. La alta rotación del personal afecta el sentido de pertenecía a la empresa y su falta de concientización sobre la seguridad de la información son problemas que canal se enfrenta con frecuencia y la implementación de un Sistema de Gestión de la Seguridad de la Información en base a NTC-ISO/IEC 27001:2013 contribuiría en la disminución de los costos e impactos negativos. Estas problemáticas afectan el cumplimiento de los planes estratégicos del Canal pues la desconfianza de sus clientes, proveedores y televidentes bajaría por una mal disponibilidad de los servicios y equipos, uno de esos impactos sería perdida de audiencia (rating), no renovación de contratos de

pautas publicitarias o cesión de espacios a productoras por no garantizar la custodia, conservación y accesibilidad de la información.

La norma ISO 27001:2013 propone varios controles que permiten garantizar que cada aspecto de confidencialidad, integridad y disponibilidad de la información sea cumplido, para ello, el estándar especifica en su ANEXO A el listado completo de cada uno de ellos y quedan agrupado en 18 secciones. Es de gran interés para la presente propuesta el control A.13.1.1 controles de red, perteneciente a los controles de seguridad de las comunicaciones, gestión de la seguridad de las redes, ya que las acciones para cumplir este control permitirán mitigar gran parte de los problemas expuestos anteriormente y presentado soluciones al canal TRO en su camino a la certificación NTC-ISO/IEC 27001:2013. Las acciones necesarias para cumplir el control A.13.1.1 serán: verificar la existencia de políticas de redes físicas e inalámbricas; los mecanismos de registro y monitoreo de la red LAN; y los sistemas de autenticación para los accesos a la red física y LAN.

Al momento de solucionar esta necesidad es conveniente ahondar en la interrogante, **¿cómo se puede implementar el control A.13.1.1 de la norma NTC-ISO/IEC 27001:2013 en departamento de Gestión de Archivos Audiovisual del canal TRO sede Floridablanca – Santander?**

1.2 Delimitación

1.2.1 Objetivo General

Diseño de estrategias para la seguridad de las comunicaciones de la Norma NTC-ISO/IEC 27001:2013 sección A13, en el departamento de gestión de archivo audiovisual del canal TRO sede Floridablanca – Santander.

1.2.2 Objetivos Específicos

- Evaluar el estado actual de la red LAN y WLAN del canal TRO en el departamento de gestión de archivo audiovisual según el control A13, seguridad de las comunicaciones.
- Establecer una metodología basada en la norma NTC-ISO/IEC 27001:2013, para el cumplimiento de los controles de seguridad de la información, aplicado a la seguridad de las comunicaciones.
- Implementar mecanismos para el cumplimiento de los controles de red, de la norma NTC-ISO/IEC 27001:2013 anexo A.13.1.1, en la red física y LAN del departamento de Gestión de Archivos Audiovisual.
- Validar la aplicación de las acciones a través de los requerimientos formales de un SGSI al departamento de Gestión de Archivos Audiovisual.

1.2.3 Acotaciones

- Al finalizar el proyecto se espera que el canal TRO cumpla con el control A.13.1.1.(Controles de red) y se generen estrategias a futuro, para que se cumplan los demás ítems de la sección A.13, y tener un control sobre la seguridad de las comunicaciones.
- Políticas propuestas al Canal TRO en redes físicas e inalámbricas.
- Mecanismos de registro y Monitoreo de la red LAN del canal bajo protocolo SNMP y accesos físicos del personal a las instalaciones del Canal TRO.
- Sistemas de autenticación para todos los accesos a la red WLAN y LAN bajo protocolo AAA, WPA2-Enterprise y Active Directory sobre Windows.

Capítulo 2

Marco Teórico y referencial

2.1 Bases Teóricas

El Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2013 describe cómo gestionar la Seguridad de la Información en una organización, donde se enfrentan diariamente a un gran número de peligros de inseguridad que puede venir de un gran número de fuentes diferentes, esta norma ayuda a identificar las fuentes y en base a un análisis de riesgos se podrán controlar en cierta medida. Según los diferentes objetivos que tenga fijada una organización, se deben aplicar una serie de herramientas con la mayor concientización para garantizar en alta medida la confidencialidad, integridad y disponibilidad de unos de los activos más importantes de las empresas en hoy en día, la información. Por ello, la norma ISO27001:2013, es la solución de mejora continua más apropiada para poder evaluar los diferentes riesgos y establecer una serie de estrategias y controles oportunos para asegurar la protección y defender la información. (pmg-ssi, 2015)

2.1.1 Seguridad informática

Con los beneficios que proporcionan las nuevas posibilidades de conectividad, emergen también una serie de nuevos riesgos. Muchas empresas son blanco de amenazas de ataques informáticos, buscando perjudicar sus activos, y más aún cuando el activo más importante es la información. El deterioro de ésta puede representar millones de dólares en pérdidas en el mundo de los negocios. Las vulnerabilidades en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso,

hackers y crackers que penetran los sistemas de seguridad. Los elementos que la seguridad Figura 1 de la información busca proteger son (Clavijo, 2006):

• La información

• Los equipos que la soportan

• Las personas que la utilizan

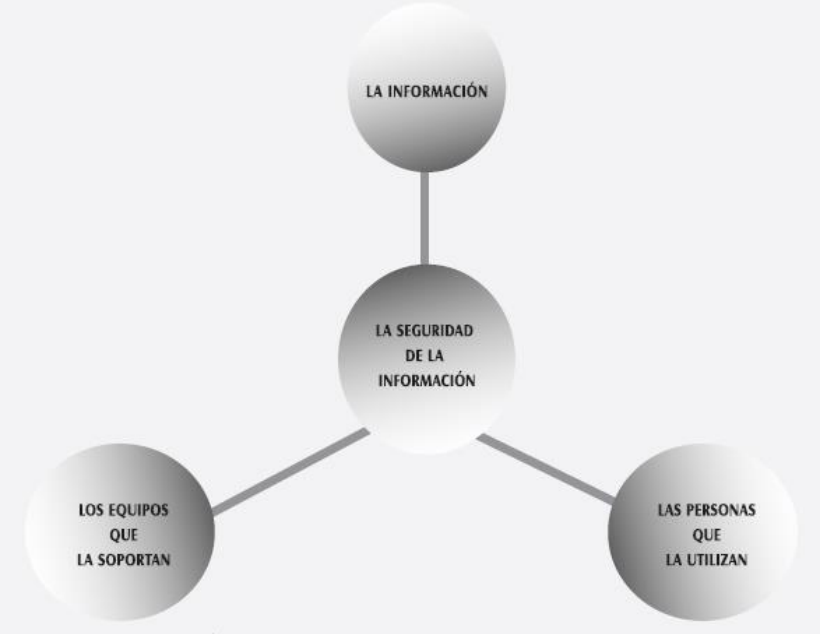


Figura 1 Elementos de la seguridad.
Fuente: (Clavijo, 2006)**.**

Se debe asegurar que el proceso de acceso y modificación a cierta información sólo sea posible mediante personas que estén autorizadas; un sistema se considera seguro cuando tiene integridad, confidencialidad y disponibilidad en la información, lo anterior corresponde a los tres pilares fundamentales de la seguridad de la información.

- ✓ **Integridad:** A través de esta se garantiza que los datos no han sido alterados, y/o destruidos de modo no autorizado, es decir se garantiza la autenticidad de la información sin importar el momento.
- ✓ **Confidencialidad**: Éste hace referencia al atributo que deben tener los datos y/o información, al encontrarse únicamente al alcance de las personas y/o entidades autorizadas, en el momento autorizado.
- ✓ **Disponibilidad:** Se debe garantizar que la información se encuentra disponible para los usuarios siempre que la necesiten. en caso contrario se provocan interrupciones de servicio y con ello problemas de calidad.

Se hace necesario entonces definir que:

- Una **Amenaza** es una persona, entidad, evento o idea que plantea algún daño a un activo.
- Un **Ataque** es la realización de una amenaza.
- Una **protección** son los controles físicos, mecanismos, políticas y procedimientos que protegen los activos o recursos de las amenazas.
- Una **Vulnerabilidad** es el debilitamiento o ausencia de una protección en un recurso o activo.
- Un **Riesgo** es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque.

En ese orden de ideas, se puede decir que las amenazas son clasificadas en intencionales y accidentales, siendo las primeras las más peligrosas, las amenazas intencionales se convierten en un ataque, que puede clasificarse a su vez como activo o pasivo.

2.1.2 Amenazas

Para analizar el contexto de seguridad en las redes, es necesario definir antes un sistema informático como un conjunto completo de elementos de hardware, software, datos/información y personal; que hace posible el almacenamiento, proceso y transmisión de la información con el objetivo de realizar una determinada tarea.

Todos los elementos del conjunto son susceptibles a recibir ataques, basados en una serie de posibles amenazas. El recurso más preciado en una organización es la INFORMACIÓN, recurso sobre cual se aúnan los esfuerzos para sostener un nivel de seguridad adecuado, es por eso que, los tres pilares básicos de confidencialidad, integridad y disponibilidad se definieron con antelación.

Las posibles amenazas que podrían presentarse en la organización, en su estado actual, se clasifican en amenazas fundamentales que afectan directamente cuatro objetivos básicos de seguridad como son: la fuga de información, violación a la integridad y negación de servicios de uso legítimo, estas amenazas serian:

Suplantación: Una persona o entidad que pretende ser otra diferente la cual es la forma más común de penetración al perímetro de seguridad.

Sobrepasar los controles: Un atacante explota las fallas de un sistema o debilidad de seguridad para adquirir acceso no autorizado a os recursos u obtener privilegios.

Violación con autorización: Una persona autorizada para usar un sistema o recurso, lo utiliza para lograr un propósito no autorizado.

Caballo de troya: Un software que tiene una parte invisible de código la cual cuando se ejecuta compromete la seguridad del sistema.

Puerta trasera: Es una característica incorporada en un software que ante un evento o entrada ejecuta acciones que pueden comprometer la seguridad del sistema.

Bombas lógicas: Son códigos adicionados a los programas que antes ciertas fechas o tiempo de ejecución efectúan acciones perjudiciales al sistema.

Virus: Son programas que se auto replican y afectan principalmente a los archivos ejecutables, a veces llegan afectar miles de computadoras.

2.1.3 Protocolo RADIUS

El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso de daemon[1] que se ejecuta en UNIX o una máquina del Windows. El cliente pasa la información del usuario a los servidores RADIUS designados y a los actos en la respuesta se vuelve que los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación.

En la Figura 2 se muestra la interacción entre un usuario de marcación de entrada con el servidor y cliente RADIUS.

[1] Daemon (nomenclatura usada en sistemas POSIX), servicio (nomenclatura usada en Windows) o programa residente (nomenclatura usada en MS-DOS) es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario.

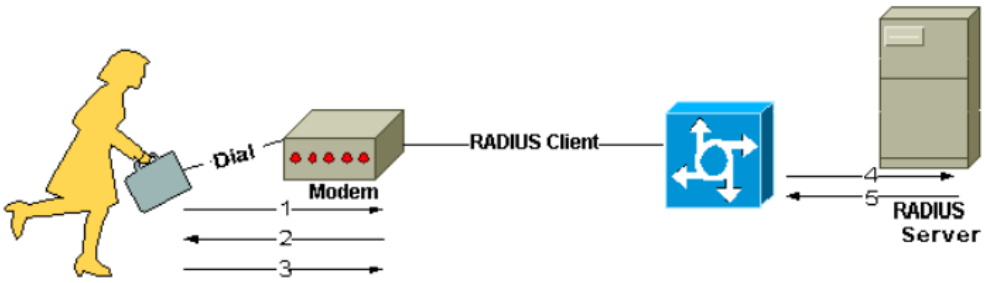


Figura 2. Interacción servidor RADIUS.

El usuario inicia la autenticación PPP al NAS, NAS le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña). Contestaciones del usuario. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar. (cisco, 2017).

2.1.4 Controlador de Dominio de Active Directory

Active Directory (AD) O Directorio Activo es el término utilizado por Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, kerberos, etc). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Estructura de A.D

Active Directory está basado en una serie de estándares llamados (X.500), aquí se encuentra una definición lógica a modo jerárquico. Estos dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Funcionamiento

Su funcionamiento es similar a otras estructuras de LDAP (*Lightweight Directory Access Protocol*), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. La ventaja que presenta esto es la sincronización presente entre los distintos servidores de autenticación de todo el dominio. Debido a esta centralización, se pueden crear varios objetos que afectarán los recursos y los usuarios que acceden a la red.

2.1.5 Segmentación.

Segmentar una red consiste en dividirla en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento, tomando en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo (winex, 2017).

Un segmento es un bus lineal al cual están conectadas varias estaciones. Las características son:

– Cuando se tiene una red grande se divide en trozos llamados segmentos.

– Para interconectar varios segmentos se utilizan bridges o routers.

– Al dividir una red en segmentos, aumenta su rendimiento.

– A cada segmento y a las estaciones conectadas a él se le llama subred.

Cuando se segmenta una red, se están creando subredes que se auto gestionan, de forma que la comunicación entre segmentos solo se realiza cuando es necesario, mientras tanto, la subred está trabajando de forma independiente.

La segmentación de una red se hace necesaria cuando:

– Se va a sobrepasar el número de nodos que la topología permite.

– Mejorar el tráfico de una red.

2.1.6 MAGERIT

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, permite:

- ✓ Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- ✓ Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

2.1.7 ISO 27000:2013

La familia ISO 27000:2013, como se puede ver en la Figura 3, cuenta con un conjunto de estándares desarrollados por la organización internacional (ISO), que

proporcionan un manual de buenas prácticas para llevar un control adecuado de los recursos dentro de una organización que desee implementar esta norma,

Figura 3.Familia ISO 27000
Fuente: Norma Técnica NTC-ISO/IEC Colombiana 27000 (Icontec, 2017)

Dentro de esta norma, la ISO27001 se proporcionan los requisitos del SGSI, la misma, cuenta con 18 controles en su Anexo A como se describe en la Tabla 1, en su sección 13 **Seguridad de las Comunicaciones,** dicha sección, lista todos los procesos necesarios para garantizar la gestión de la seguridad en las redes, y en su control A.13.1.1 detalla la aplicabilidad en una organización los controles de red.

Tabla 1.Anexo A, ISO 27001:2013

ISO 27001-2013
A5. Políticas de seguridad de la información
A6. Organización de la seguridad de la información
A7. Seguridad relativa a los recursos humanos
A8. Gestión de activos
A9. Control de acceso
A10. Criptografía
A11. Seguridad física y del entorno

A12. Seguridad de las operaciones
A13. Seguridad de las comunicaciones
A14. Adquisición, desarrollo y mantenimiento de los sistemas de información
A15. Relación con proveedores
A16. Gestión de incidentes de seguridad de la información
A17. Aspectos de seguridad de la información para la gestión de la continuidad de negocio
A18. Cumplimiento

Fuente: Anexos de ISO/IEC 27001-2013 (Amaya, welivesecurity, 2013)

2.1.8 Controles Físicos

El control físico es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Ejemplos de los controles físicos son (Enterprise, 2018):

- **Cámaras de circuito cerrado:** Diseñada para supervisar una variedad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados.
- **Sistemas de alarmas térmicos o de movimiento:** Herramientas básicas y fundamentales en todo sistema de alarmas, ya que gracias a ellos es posible detectar una intrusión en el interior de un inmueble. Tienen la capacidad de detectar cualquier movimiento o actividad no autorizada en cualquier condición de iluminación.
- **Guardias de seguridad:** Es un profesional de carácter privado que vela por la seguridad, primordialmente en relación a las personas, edificios y bienes materiales.

Puertas de acero con seguros especiales Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para

reconocer individuos).

2.1.2. Controles Técnicos

Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como (Enterprise, 2018):

- **Cifrado:** Es un conjunto de técnicas que tratan sobre la protección de la información frente a observadores no autorizados, también resuelve problemas de seguridad como certificar la autenticidad e integridad de la información.
- **Tarjetas inteligentes:** Es cualquier tarjeta del tamaño del bolsillo con circuitos integrados, que permite la ejecución de cierta lógica programada, usada para autenticar personas ante servicios de red o entes físicos.
- **Autenticación a nivel de la red:** La autenticación a nivel de red completa la autenticación del usuario, antes de que se establezca una conexión a Escritorio remoto y de que aparezca la pantalla de inicio de sesión. Se trata de un método de autenticación, más seguro que puede ayudar a proteger el equipo remoto de usuarios y software malintencionados (forsenergy, 2016).
- **Listas de control de acceso (Acles):** Permiten controlar el flujo del tráfico en equipos de redes, tales como *routers* y *switches*. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.
- **Software de auditoría de integridad de archivos:** Verifica la calidad e integridad de la información de bases de datos y archivos de un equipo, analiza y clasifica los datos aplicando criterios de acuerdo con las reglas y automatiza técnicas de auditoría asistidas con el computador, genera

reportes y exporta archivos.

2.1.9 Sistemas de monitoreo bajo SNMP

Para garantizar las disponibilidades de la información se debe mantener un control constante de la red, la misma se puede gestionar con un protocolo simple de administración de red o SNMP (del inglés *Simple Network Management Protocolo*), finalmente no es más que un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

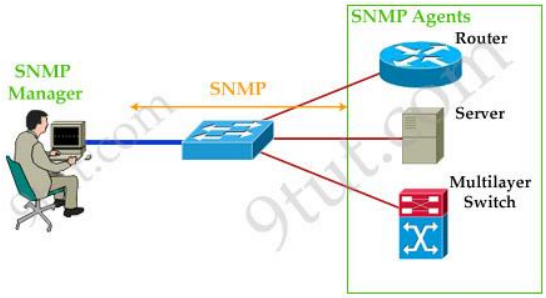


Figura 4. Protocolo SNMP
Autor: Simple Network Management Protocolo SNMP Tutorial (9tut.com, 2014)

Los dispositivos que normalmente soportan SNMP incluyen *routers*, *switches*, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más, lo que permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. (9tut.com, 2014)

El agente SNMP se emplea en todos los dispositivos anteriormente mencionados luego, en un PC, se instala un software SNMP Manager para poder recibir la información de monitoreo así que SNMP es el protocolo que se ejecuta entre el Administrador y el Agente. La comunicación SNMP entre el administrador y el agente se realiza en forma de mensajes ver Figura 4.

2.1.9.1 NMS (Sistema de gestión de red)

Un sistema de gestión de red o NMS (*Network Management System*), es una aplicación o conjunto de aplicaciones que permite a los administradores de red gestionar los recursos independientes de una red dentro de un marco de administración de red más grande. Un NMS se puede usar para monitorizar componentes de software y hardware en una red. Por lo general, registra los datos de los puntos remotos de una red para llevar a cabo informes centrales a un administrador del sistema. (Armando, 2016)

2.1.9.2 Beneficios que aporta el empleo de un NMS

El beneficio clave de usar un NMS es que permite a los usuarios monitorizar o administrar todas sus operaciones en la red usando un único sistema. Un sistema de gestión de red NMS es útil para:

- Descubrimiento de los dispositivos de red
- Supervisión de los dispositivos de red
- Análisis de rendimiento de la red
- Gestión de dispositivos de la red
- Notificaciones inteligentes o alertas personalizables

2.1.10 Controles Administrativos

Los controles administrativos definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como (Enterprise, 2018):

- **Entrenamiento y conocimiento:** Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

- **Estrategias de selección de personal y separación:** Estos funcionarios deben tener un buen nivel de preparación a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del Entidad de manera apropiada.

2.2 Marco Referencial

A continuación, se presentan algunos proyectos referentes a los diferentes temas del proyecto.

2.2.1 Nacional

Título: Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013 (NIEVES, 2017)
Autor: Arlenys Carolina Nieves**.**
Descripción: El contenido de este trabajo es una guía, que permitirá evaluar la integridad, confidencialidad y disponibilidad de los activos (Hardware - Software) de información a las oficinas de Ingreso de Centros de Educación Técnica y Tecnológica del Cesar.
Para el desarrollo de lo anterior, se dividió en tres fases: Planeación, incluyó un análisis de situación y descripción de los procesos, en la fase de Preparación incluyó GAP análisis, activos de información (análisis y evaluación de riesgos), y la última fase Capacitación y sensibilización, en donde se involucra la concientización de seguridad de sistemas y activos de información.

Título: Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001 (SUÁREZ, 2015)
Autor: Alba Elisa Córdoba Suárez.

Descripción: Para la primera fase se aplica la metodología MAGERIT con la cual se realiza el análisis de riesgos que es uno de los procesos más importantes que se debe realizar dentro de la empresa ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales esta expuestos cada uno de ellos. Además, permite identificar amenazas y vulnerabilidades.
Para el análisis de riesgos se realiza un inventario de activos, valoración cualitativa de dichos activos, identificación de amenazas, definición de salvaguardas. Una vez realizado estos procesos y analizado las pruebas realizadas a la red de la Curaduría con herramientas de análisis de trafico de red se procede a realizar una evaluación de los riesgos el cual permite determinar que activos se encuentran en peligro.

Una vez identificado claramente los activos que se encuentran en riesgo y que generarían mayor impacto en caso de sufrir un ataque, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles y el plan de gestión del riesgo, para cada uno de estos activos teniendo en cuenta lo expuesto por la Norma ISO/IEC 27002. Dichas políticas y controles deben ser implementadas en la organización por parte de la gerencia, en este caso por Curador urbano junto al comité de seguridad para cumplir el objetivo fundamental del SGSI que es proteger la información y disminuir los riesgos, garantizando la continuidad del negocio.

Título: Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa interfaces y soluciones (ORJUELA, 2017)
Autores: Luz Adriana Moyano Orjuela – Yasmín Elena Suarez Cárdenas.
Descripciones: Durante el desarrollo se especifican cinco capítulos, que se detallan de la siguiente manera: La planeación, en el cual se identifica el planteamiento del problema, los objetivos del proyecto, así como el alcance y limitaciones, además de la factibilidad técnica, operativa, legal y económica del proyecto.

En el contexto organizacional, se realiza el reconocimiento y se detalla la estructura organizacional, mostrando el estado actual de la organización con respecto a la ISO/IEC 27001, en lo que respecta a los diferentes dominios, como lo son políticas de seguridad, organización de la seguridad de la información, seguridad de los RRHH, gestión de activos, control de accesos, criptografía, seguridad física y ambiental, seguridad en las operaciones, seguridad en las comunicaciones, entre otros.

En la gestión de riesgos, se realiza el inventario de activos y su valoración, el análisis de amenazas y la valoración de riesgos.

En la selección de salvaguardas se define las estrategias, técnicas y el plan de tratamiento del riesgo, especificando las políticas del SGSI, los controles recomendados, las opciones de monitoreo y la asignación de responsabilidades de acuerdo al compromiso con la norma 27001:2013.

2.2.2 Internacional

Titulo: Diseño De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Basado En La Norma ISO 27001:2013 Para La Red Corporativa De La Empresa Ecuatronix.

Autores: Miguel Leopoldo Villacís Espinosa

Descripción: En la actualidad el alto índice de crecimiento de las Tics, se ha convertido en un factor delimitante a ser tomado en cuenta por las empresas o compañías ya que la información, y comunicaciones son hoy en día un activo de mucho valor. Por lo tanto, deben ser manejadas de tal manera que garanticen un alto índice de confiabilidad, integridad, y disponibilidad, para un correcto funcionamiento de las mismas.

El Internet es uno de los medios de comunicación más utilizados a nivel mundial; por lo que es la vía principal, por la cual una red estará expuesta a posibles riesgos o ataques en su integridad. En la actualidad, los virus, amenazas y ataques son muy

comunes dentro de las redes; esto implica que se debe adoptar medidas que protegerán la información contenida en las mismas. (Flores Estévez & Jiménez Nuñez, 2010). Estas políticas o normas de seguridad de la información que han sido mencionadas son un conjunto de guías o procedimientos de referencia para su implementación, y no son más que uno de los tantos métodos que existen para salvaguardar la información de una entidad.

2.3 Marco legal

Hoy en día la seguridad en las comunicaciones es una herramienta importante e indispensable para el desarrollo de una empresa. Es por esto que el crecimiento significativo y avance de la tecnología, llevaron a la necesidad de brindar un servicio con calidad, esto implica establecer un marco jurídico que promueva el desarrollo de calidad.

Las decisiones del Estado se materializan a través de la implementación de políticas públicas como instrumentos jurídicos que racionalizan y simplifican del ordenamiento legal, las herramientas que aseguran la eficiencia económica y social para afianzar la seguridad jurídica, siendo la televisión un servicio público en Colombia, no ha sido ajeno a la necesidad de legislar normas que garanticen su prestación conforme a unos principios, fines y normas que regulen el uso de contenidos.

A continuación, se presentan las diferentes Leyes, Decretos mediante los cuales, se rige el canal TRO.

2.3.1 LEY 1273 DE 2009

Se adiciona al Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", el cual es parte importante para el presente proyecto ya que, especifica los delitos recurrentes que se presentan en el acceso abusivo a un sistema informático.

1. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
2. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
3. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.
4. Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
5. Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
6. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos

personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

7. Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

2.3.2 Ley 23 enero 28 de 1982, Sobre derechos de autor.

Como se expresa en los artículos 1° y 2° de la “LEY N° 23 DE 1982”, los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. Así mismo en su artículo 3° expresa las disposiciones a las que se hacen partícipes los autores, como disponer su obra de forma gratuita o de manera onerosa según lo contemple el titular, dicho titular puede ser el autor de la misma, el intérprete o cantante en caso de que sea una obra artística o en su defecto aquella persona natural o jurídica que, en virtud de contrato obtenga por su cuenta y riesgo, la producción de una obra científica, literaria o artística realizada por uno o varios autores en las condiciones previstas en el artículo 20 de la presente ley.

De igual manera expone que tanto las ideas como los conceptos de obras que apliquen como destacamento científico, literario o artístico, no constituyen un objeto de apropiación, la ley 23 de 1982 expresa enteramente que sólo se protege el modelo literario de como el autor plasma las ideas dentro de las categorías antes

mencionadas. Del mismo modo, dicta las disposiciones legales y limitaciones en cuanto a reproducción y cita de cualquier modelo literario, propendiendo por proteger siempre a la figura de autor comprendida en los literales antes mencionados.

2.3.3 Ley Estatutaria 1581 De 2012

Esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. En concordancia con lo anterior, solo serán tenidos en cuenta para la protección aquellos datos que reposen en cualquier base de datos entablada para el tratamiento de la información en entidades constituidas de manera pública o privada, más no para sistemas que capten información o que la contengan de manera local en domicilios personales y domésticos, igualmente aplica esta restricción de protección a las bases de datos que contengan información militar o de seguridad nacional. Del mismo modo, dispone las legalidades en el ámbito del tratamiento de la información rigiéndose por los siguientes principios de legalidad: fidelidad, libertad, veracidad, transparencia, confidencialidad y seguridad de la información; teniendo en cuenta la disposición de lo que se conoce como datos sensibles, los derechos de niños y adolescentes, así como los derechos de autor y los derechos de los titulares de la información susceptible. Lo anterior corresponde a los lineamientos de tratamiento de los datos sensibles, como el derecho de conocer quiénes serán los responsables de procesar los datos y bajo que finalidad, así como también respetar los lineamientos nombrados anteriormente.

Capítulo 3

Reconocimiento de la Organización

Canal TRO (Televisión Regional del Oriente) es un canal de televisión abierta colombiano, creado en 1995. El canal cubre los departamentos de Santander y Norte de Santander. Su programación es de índole educativa y cultural. Su sede central y principales estudios de transmisión se encuentran en Floridablanca, pero también realiza transmisiones desde los estudios de grabación que tienen en Cúcuta.

Gran parte del canal es financiado por la ANTV y planea ser auto sostenible para 2019.1

3.1 Estructura organizacional.

La estructura interna del Canal y la planta de personal será determinada por la Junta Administradora consultando el objeto social de la entidad y la necesidad de servicio, todo de acuerdo con las disposiciones legales vigentes, en la figura 5 se observa el organigrama jerárquico del Canal TRO.

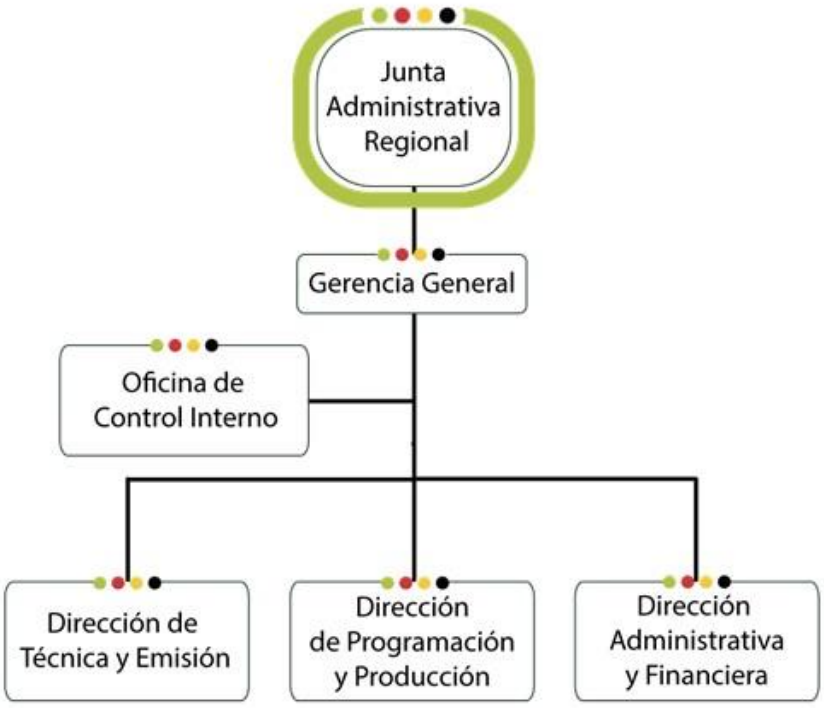


Figura 5. Organigrama Canal TRO
Fuente: Pagina Web Canal TRO. (TRO, 2019)

Área Administrativa Y Planeación:

Lidera, orienta, asesora y concierta con las distintas dependencias, la formulación de los planes de mediano y largo plazo, y los planes anuales en concordancia con el Plan Estratégico Situacional y presentarlos a las instancias correspondientes.

Programación:

Planea, coordina, organiza, dirige y controla todas las producciones del Canal y del servicio de producción que se les preste a terceros. Programa, diseña y supervisa

tanto la calidad de la programación como el cumplimiento de la reglamentación vigente en materia de televisión y comercialización de la misma.

Producción:

Planea, dirige y evalúa el desarrollo, fortalecimiento, la operación, el mantenimiento y control de la calidad de los recursos técnicos de emisión, producción, pos producción, transmisión y retransmisión necesarios para la prestación de un óptimo servicio de televisión.

Área jurídica:

Asesora y conceptúa sobre los asuntos jurídicos de la organización y vela porque las actividades se desarrollen con sujeción a las disposiciones constitucionales y legales.

Área Financiera:

Planea, dirige y controla las actividades relacionadas con la administración de los servicio, bienes y suministros, así como las derivadas de la contabilización de las operaciones, inversiones, financiación, presupuesto y disponibilidad de efectivo para el adecuado funcionamiento de la entidad.

Área comercial:

Encargada de la comercialización del producto empresarial. Esta actividad puede desarrollarse directamente por la empresa o a través de organizaciones privadas especializadas en la materia.

Área Técnica:

Encargada de desarrollar procesos de producción específicos, sugerir e implementar la asimilación de nuevas tecnologías, coordinar y dirigir el sistema operativo de la Empresa. (TRO, 2019)

3.2 Infraestructura.

El Canal Cuenta con una planta de dos pisos, de ésta disposición se puede describir lo siguiente: en el primero se encuentra el estudio de televisión, junto con las secciones de producción y emisión, dependencias en las que se encuentran los *Switches* y servidores como se muestra en la Figura 106, que permiten la comunicación con las diferentes dependencias y equipos del segundo piso.

3.2.1 Arquitectura de datos

Cuando se habla de arquitectura de datos, se establece inicialmente que el contexto se relaciona estrictamente, para este caso, acerca de qué manera están distribuidos los activos de la red, de acuerdo a las disposiciones de la planta física de TRO, tipificando la ubicación de los equipos.

Tipo de red interna

La red interna del canal TRO cuenta con una segmentación por VLAN, la misma se divide en los diferentes departamentos del canal. Cuenta con Switch principal CORE ubicado en la oficina llamada dirección técnica resaltada en la siguiente figura, desde donde se administra la red de internet del canal, en la Figura **6**, se muestra a planta física

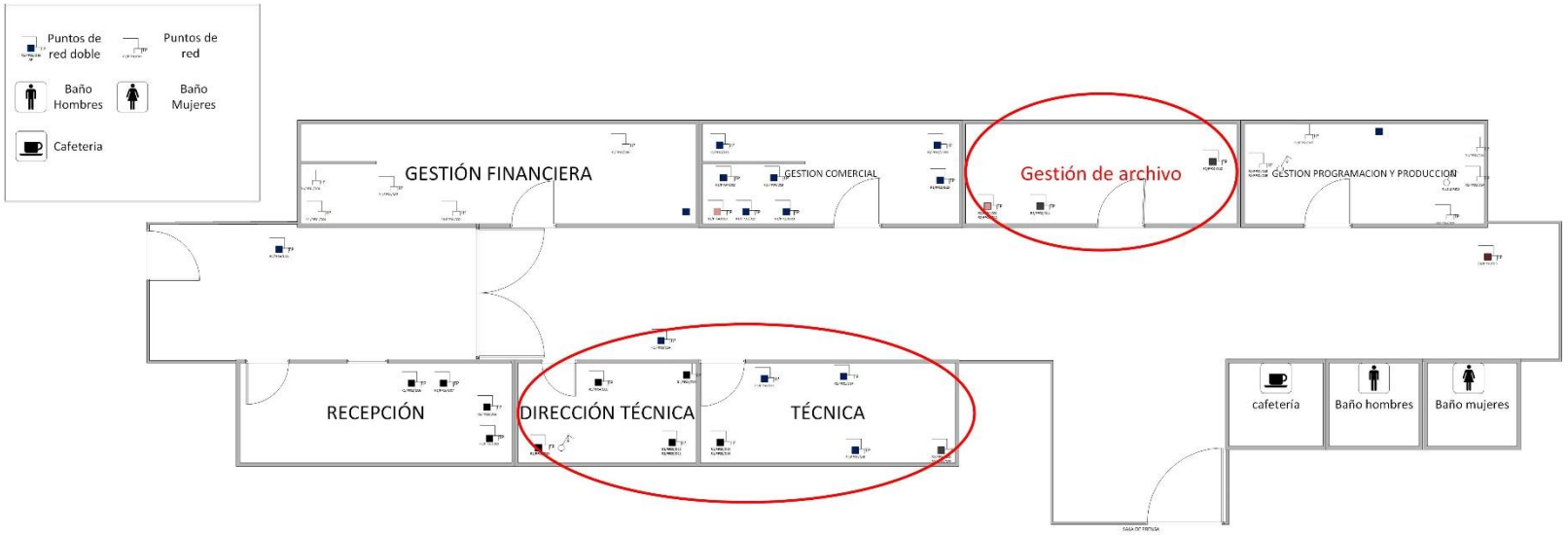


Figura 6. Puntos de red segundo piso

correspondiente al segundo piso del Canal, así como la distribución de los puntos de la red para usuarios finales, del mismo modo en Figura 7 con la salvedad de que ésta detalla la primera planta.

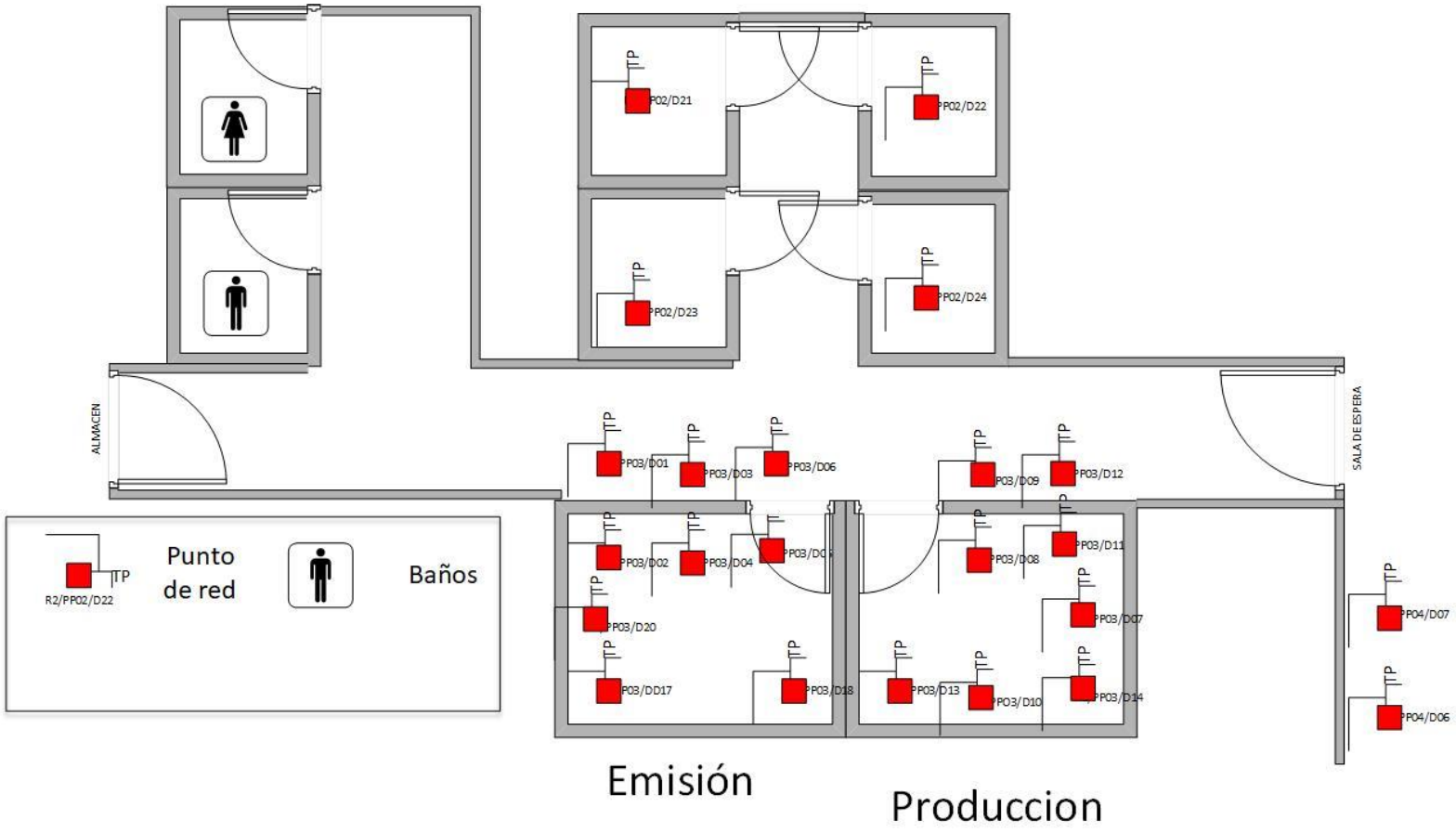


Figura 7. Puntos de red primer piso

Estructura Plataforma equipos VSN canal TRO

La Plataforma VSN es una herramienta de automatización para el flujo de trabajo audiovisual del Canal TRO; permitiendo mejorar el flujo de datos y organización en cada una de las áreas que lo conforma, con sus respectivos procesos, en la figura 8 se detallan a groso modo los equipos dispuestos para la VSN de TRO. Estos equipos, son los encargados de procesar los contenidos que se emiten en el canal, estos dispositivos serán parte del monitoreo a través de SNMP (Dude server).

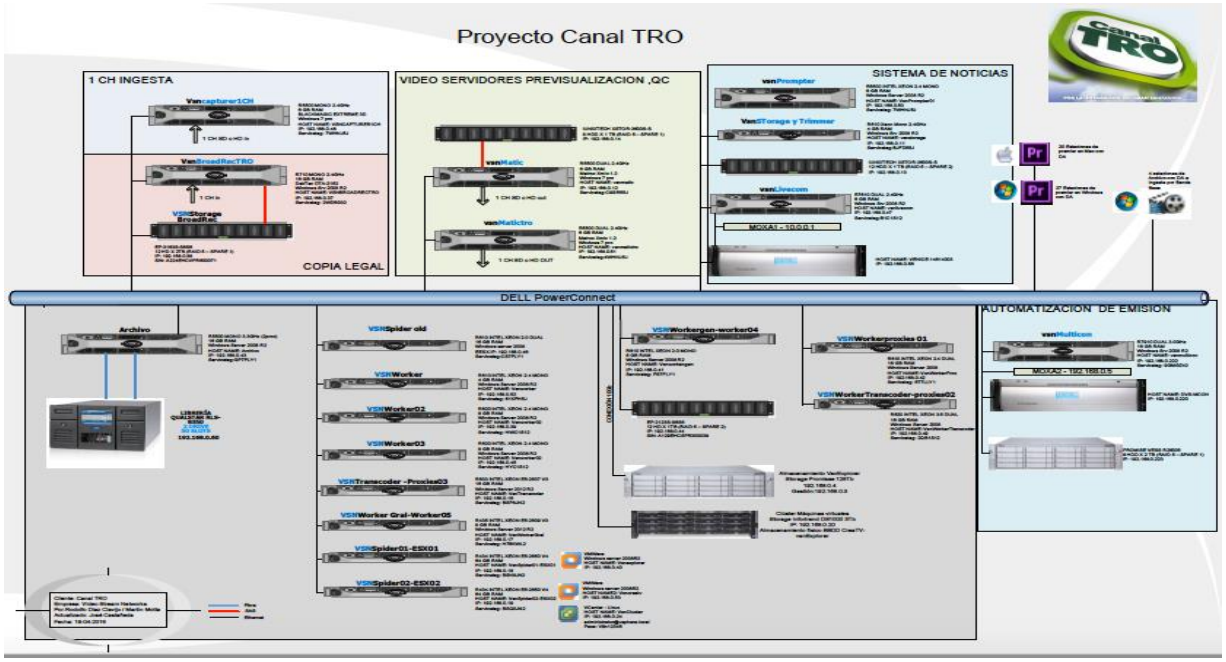


Figura 8. Equipos VSN
Fuente: Área Técnica canal TRO

Equipos que conforman la Plataforma VSN en el Canal y su funcionamiento.

- **VSNcapturer1CH:** Servidor especializado para grabación de material que se le especifique al operador. Se hace con la aplicación Autorec Director.
- **COPIA LEGAL – VSNBroadrecTRO**: Servidor especializado para hacer la grabación de los contenidos del canal al aire en baja y alta resolución. Se puede realizar consulta del material directamente en el servidor o vía web por medio de internet Explorer.
- **PREVISUALIZACIÓN QC - VSNMatic01 y VSNMatic02:** Servidor de *playout*[2] y video servidor diseñado para automatizar la continuidad. Gestiona el canal de forma automática. Se utiliza como respaldo para el Multicom o mcom en caso de falla, como ocurre en este caso. Por medio de estos se realiza el control de calidad de los clips o contenidos del canal para después ser ingestados en el *storage* de los videos servidores de emisión.
- **SISTEMA DE NOTICIAS – VSNPrompter:** Sistema de teleprompter[3] que se integra con el playout. Recibe los textos introducidos en la ficha de la noticia por los periodistas y se sincroniza con los cambios de escaleta.
- **VSN Storage y trimmer:** Trimmer es el servidor y la aplicación que permite la validación de material antes y después de ser ingestados en el sistema. La operadora de ingesta depende de la validación de los operadores de matic para realizar la ingesta de material y la validación de las escaletas que realiza el área de programación. El storage almacena los contenidos del trimmer y se conecta al servidor por conexión SAS.

[2] Término para la emisión de canales de radio y de televisión desde la emisora hasta que se entrega el contenido a la audiencia.

[3] Mecanismo que consiste en una pantalla o espejo que permite a la persona seguir su discurso o texto al mismo tiempo que lo pronuncia

- **VSN Livecom:** Basada en rundownlist[4] de Multicom, se compone del motor de playout, que permite que varios clientes de la aplicación puedan conectarse a la vez al motor de reproducción y cada uno con distintas configuraciones, interactuando sobre el mismo rundown.
- **MOXA:** Este equipo es el encargado de controlar los canales de los videos servidores Venice, así como los dispositivos que están automatizados en las distintas listas de emisión de Multicon. En el caso de los video servidores, el control de los canales se realiza a través del protocolo serie VDCP (Protocolo de control de discos de video).
- **VENICE DVS livecom:** Video servidor de 4 canales de playout donde actualmente hay 2 funcionales para el sistema de livecom. Se encuentra ubicado físicamente en el cuarto cerca a la antena satelital o uplink.
- **Archivo y librería:** El servidor archivo gestiona los procesos para la librería – SGL. Por tanto, debe estar siempre activos los servicios flasnet.
- **SISTEMA MAM - VSNSpider – Explorer:** Es el sistema central que coordina todos los procesos que suceden en segundo plano como copias de material, generación de proxies, borrado de ficheros, envíos de contenido para emisión, etc.
- **VSNSpider – Creatv:** Creatv es el programa que se utiliza para realizar la programación, planeación y escaletas diarias para emisión.

[4] Contenidos de video para crear el resumen.

- **VSNWorker01, Worker02, Worker03, Worker04:** Servidores especializados en tareas generales como movimiento de media, registro en base de datos, generación de *thumbnails*[5].
- **Storage principal Sistema MAM (*Media Asset Management software*):** Es el almacenamiento donde se guarda todo el contenido de consulta, catalogación, transcodificación.
- **VSNworker proxy01:** Servidor que genera los proxys y transcodificación en el sistema MAM para consulta de material en baja resolución por medio de VSNExplorer.
- **VSNworker proxy02 – workerTranscoder:** Servidor que funciona como complemento al proxy01.
- **VSNMulticon:** Servidor que contiene el sistema que crea las listas de emisión ya sea a partir del fichero enviado por el Departamento de Programación, mediante el módulo VSNMULTICOM SCHEDULER, o incluso manualmente desde el propio interfaz de usuario de la aplicación de emisión.
- **Venice DVS-Mcon:** Video servidor de 4 canales de *playout*.

3.2.2 Medios de transmisión

Uplink

En esta área se encuentran los equipos necesarios para transmitir la señal satelital del Canal TRO. allí se cuenta con unidades encargadas de realizar el tratamiento de la señal recibida de Emisión para enviarla al satélite; de tal manera que pueda ser capturada a través de antenas y receptores del territorio nacional, América y parte de Europa.

[5] Imagen de vista previa reducida del original que se utiliza como marcador de posición. Dependiendo de la plataforma, la miniatura debe tener un tamaño determinado.

Figura 9. Salón Uplink

3.2.3 ISP

El canal TRO actualmente cuenta con dos proveedores de Internet, Claro y UNE, quienes registran un servicio de 100Mbps y 80Mbps respectivamente, por medio de fibra óptica a través de un modem suministrado por las empresas contratadas, y debidamente distribuidos para los diferentes departamentos del canal, teniendo en cuenta las necesidades de cada uno.

3.2.4 Arquitectura física

En la primera planta se encuentran los equipos VSN, en la sección de emisión (ver Figura 10), es allí donde se procesan y almacenan los diferentes contenidos audiovisuales del canal.

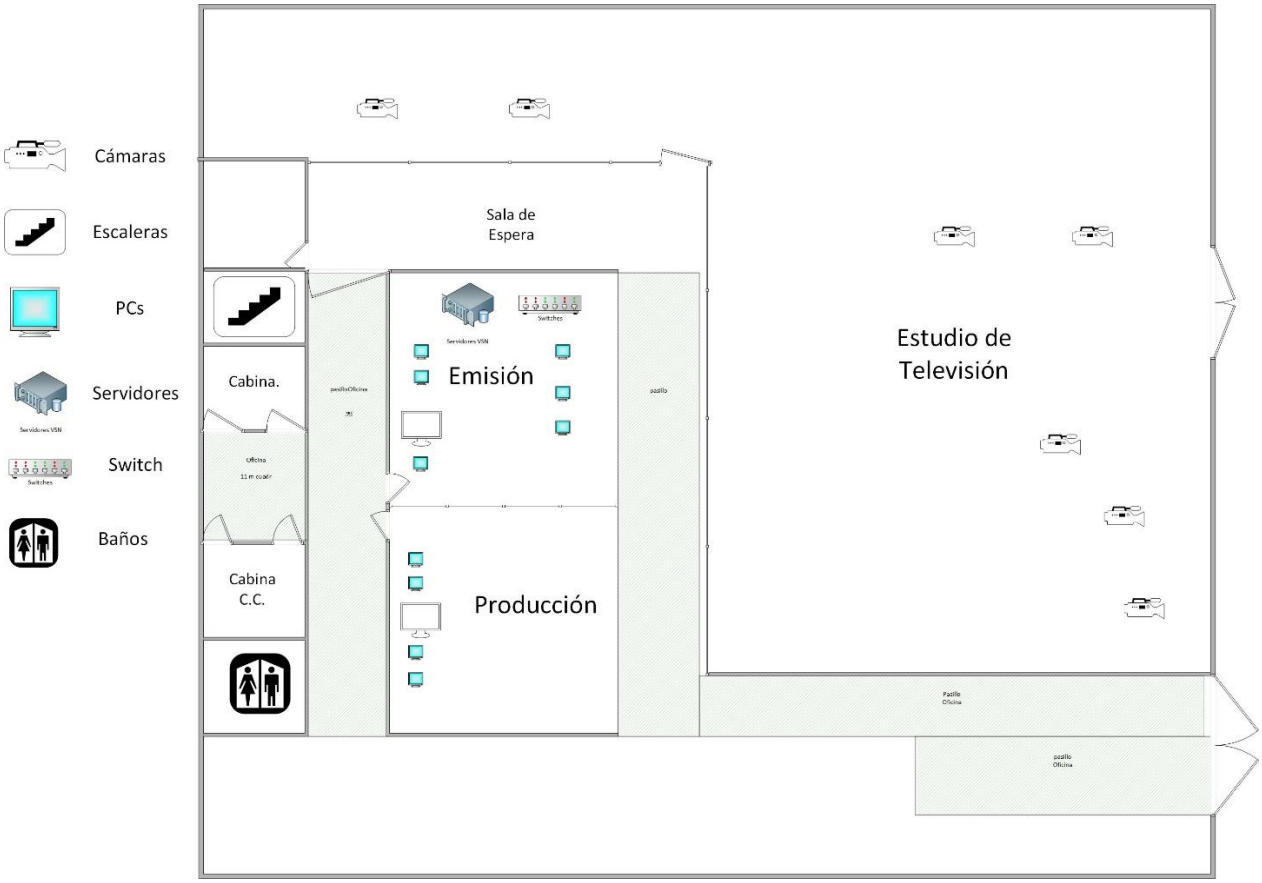


Figura 10. Primer Piso

En la segunda planta, se encuentran en su mayoría oficinas de edición, administración financiera, comercial y técnica; en esta última se encuentran los equipos de capa 2 (Switches), que según lo anterior corresponden a los equipos principales de la red que suministran el servicio de Internet al canal y la comunicación de las diferentes dependencias como se muestra en la Figura 11.

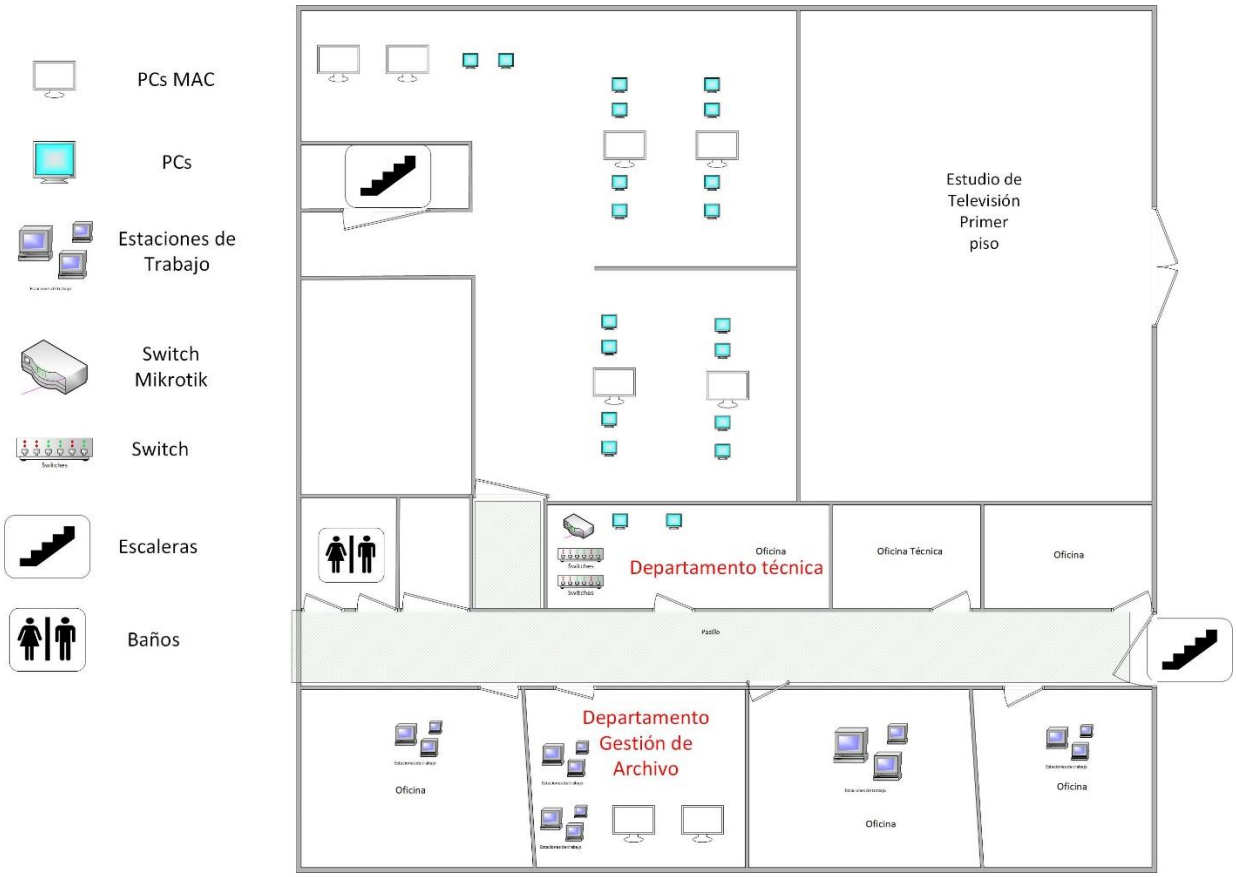


Figura 11. Segundo Piso

3.3 Evaluación del punto A13 de ISO/ICE 27001

En los pasos iniciales para el desarrollo de la implementación de la seguridad de las comunicaciones basado en ISO/ICE 27001:2013, se realiza un análisis que permite evaluar el estado de la empresa respecto al Anexo A13.

Se realizó inspección visual y documental del departamento Gestión de Archivos del Canal TRO, además se realizó una entrevista con el encargado de la red del canal TRO (Área Técnica) como parte de la recopilación de información.

Para la elaboración del estado inicial del departamento, se tomaron tres valoraciones como se muestra en la Tabla 2, la información obtenida que se encuentra en el ANEXO 7.1.

Tabla 2. Parámetros encuesta

SIGLA	Estado	Descripción
NC	NO CUMPLE (NC)	No existe o no está implementado.
CP	CUMPLE PARCIALMENTE (CP)	Lo que la norma requiere (ISO/IEC 27001 versión 2013) Anexo A13.se está haciendo de manera parcial, haciendo diferente, no está documentado y/o no se gestiona.
SC	SE CUMPLE(SC)	Se cumple y es gestionado con lo que la norma solicita y aplicado por todos los involucrados respecto a la seguridad de las comunicaciones.

3.3.1.1 Anexo A.13.Seguridad de Las Comunicaciones.

En cada tabla se detallan los datos obtenidos en la encuesta, donde se denota que la mayoría de los controles se encuentran parcialmente implementados. Éstas preguntas fueron basadas del documento Excel “Estado y Aplicabilidad de controles de Seguridad de la Información”. (Controles Anexo A - ISO 27001 Secutiry)

3.3.1.2 Gestión de la seguridad de las redes.

A nivel de controles de red, TRO no cuenta con un mecanismo de monitoreo de la red, lo que genera impedimento a la hora de generar una respuesta adecuada por parte del encargado, ante un eventual error del sistema. Los otros controles como se muestra en la Tabla 3, se encuentran parcialmente implementados; algunos se

encuentran completos pero no se ejecutan, ya que por diferentes factores de usabilidad se decidió ignorar, conllevando a un riesgo para la red del canal. Debido a esto, no se puede llevar un control preciso de todos los usuarios que se conectan a la red, puesto que, el servidor de dominio permitiría monitorear el tráfico y el registro de usuarios, por ende, al no implementar esta herramienta, se corre el riesgo de permitir el acceso a la red a usuarios no autorizados y sin conocimiento de causa.

Tabla 3. Controles de red.

	NC	CP	SC
¿Existen políticas de redes físicas e inalámbricas?			X
¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red?	x		
¿Existe un mecanismo de registro y monitorización de la red y los dispositivos que se conectan ella?	X		
¿Hay un sistema de autenticación para todos los accesos a la red de la organización?		X	
¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?		X	
¿Los usuarios se autentican adecuadamente al inicio de sesión?		X	
¿Cómo se autentican los dispositivos de red?		X	
¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?			X
¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?			X

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

En las preguntas relacionadas con la seguridad de los servicios de red de la Tabla 4, algunas de las respuestas de la entrevista mostraron que al realizar auditorías de los servicios de red, se efectúan solicitudes externas esporádicamente, ya que solo

se realizan cuando se presenta un error grave que impida el funcionamiento normal del servicio de Internet.

Tabla 4. Seguridad de los servicios de red.

	NC	CP	SC
¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?			X
¿Existe un monitoreo de servicios de red?		X	
¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?		X	
¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?			X
¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS / IPS, WAF, DAM?			X

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

En la Tabla 5, se denota cómo el Canal TRO segmenta la red por VLAN, ésta se divide para que los equipos importantes como los servidores VSN, no se comuniquen a Internet. La segmentación de la red física y la de invitados, se realiza a través de la WLAN, es decir, la red de los invitados se encuentra aislada de la red de TRO y sólo se les permite el acceso por la red inalámbrica a los usuarios invitados, esto se realiza por medio de una única clave conocida por el departamento de técnica, dada a la persona que lo solicite (Empleados e invitados). El proceso para la segmentación de proveedores y clientes no se lleva a cabo, ya que por el momento el canal posee una única salida con el proveedor del servicio de Internet.

Tabla 5. Segregación en redes.

	NC	CP	SC
¿Existe una política de segmentación de red? ¿Qué tipo de segmentación existe?			X
¿Es basada en la clasificación, los niveles de confianza, dominios (público, escritorios, servidor, funciones, etc.)?			X
¿Cómo se monitorea y controla la segregación?			X

¿Se segmenta la red inalámbrica de la red física? ¿Y la red de invitados?		X	
¿Hay controles adecuados entre ellos?		X	
¿Cómo se controla la segmentación con proveedores y clientes?		X	
¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?		X	

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

3.3.1.3 Intercambio de información

Para la realización de procedimientos de intercambio de información, el canal emplea servicios en la nube, discos duros, y además, cuenta con un correo corporativo a través de Gmail que se le otorga a cada persona que lo necesite dentro de la organización; mientras que en los programas de concientización, capacitación y cumplimiento no se implementa ninguna política, llevando a que el personal empleado y algunos dispositivos como los discos de *Backup* se utilicen de forma inadecuada.

Tabla 6.Políticas y procedimientos de intercambio de información.

	NC	CP	SC
¿Existen políticas y procedimientos relacionados con la transmisión segura de información?			X
¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc?			X
¿Está basado en la clasificación de la información?			X
¿Existen controles de acceso adecuados para esos mecanismos?			X
¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)?			X
¿Se sigue el principio de confidencialidad y privacidad?			X

¿Existen un programa de concientización, capacitación y cumplimiento?	X		

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

Se observa que en base a las respuestas, el canal no utiliza protocolos SSL/TLS que conlleva a su vez el empleo de firmas digitales con fines de comprobación de identidad digital, ya que su costo es muy elevado para cada empleado que lo requiera. Por otro lado, cuenta con formatos físicos de recepción de material, a su vez, para establecer comunicación entre las sedes de Cúcuta y Floridablanca hace uso de redes privadas tipo VPN, que permiten una conexión segura y cifrada, de los contenidos compartidos.

Tabla 7. Acuerdos de intercambio de información

	NC	CP	SC
¿Qué tipos de comunicaciones se implementan las firmas digitales?	X		
¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?			X
¿Cómo se mantiene una cadena de custodia para las transferencias de datos?		X	

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

Según la encuesta realizada como método de recolección de información, en la tabla 8, queda constancia de que la organización cuenta con políticas claras para el control de intercambio de información y los controles de cifrado de la misma.

Tabla 8. Mensajería electrónica.

	NC	CP	SC
¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?			X
¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?			X

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

Los acuerdos se encuentran adecuadamente implementados, puesto que son revisados cada tres meses por entidades del gobierno como la contraloría. Los acuerdos de confidencialidad son tratados al momento de contratar al empleado y se actualizan cada 6 meses, lo anterior se desprende de la evidencia que denota la tabla 9.

Tabla 9. Acuerdos de confidencialidad o no revelación

	NC	CP	SC
¿Existen acuerdos de confidencialidad?			X
¿Han sido revisados y aprobados por el Departamento Legal?			X
¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?			X
¿Han sido aprobados y firmados por las personas adecuadas?			X
¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?			X

no cumple (NC) --- cumple parcialmente (CP) --- se cumple(SC)

3.4 Aseguramiento de la Información

El proceso de gestión de sistemas de información constituye un eje central en términos de seguridad informática, pues son basados en estándares

internacionales, se establecen las políticas y procedimientos generalizados para la concepción de los mecanismos de preservación de los tres pilares fundamentales en términos de seguridad de la información. Es así como dichos procedimientos se aúnan con las metodologías de gestión y control de riesgos en las organizaciones, con miras a la realización de los procesos auditables para contribuir a la mejora considerable de la preservación de los recursos informáticos de las organizaciones.

Requisitos de la norma ISO/IEC 27001:2013

La norma ISO 27001 presenta los requisitos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI; este sistema de gestión es la razón de ser de la norma, pues aquí se especifica una estrategia para que las empresas en pro de la seguridad de la información implementen una metodología innovadora en busca de consolidar organizaciones más estructuradas. Para llevar a cabo la labor de implementación y establecimiento del SGSI se tiene consideraciones sobre la estructura interna de la empresa como los objetivos, requisitos de seguridad, procesos organizacionales, necesidades de la organización, tamaño y todos estos aspectos tiene una influencia sobre la implantación del sistema, por tanto, el estudio es amplio y muy específico acerca de la organización y como se encuentra compuesta.

La norma aporta una visión amplia referente a la valoración de riesgos y su apropiado tratamiento, sin importar la naturaleza de las organizaciones, pues esta se encuentra definida en forma general para la aplicabilidad en cualquier organización, de esta manera los requisitos que se mencionan a continuación son necesarios definirlos para el cumplimiento de la norma: (Mesquida, 2010)

1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
   4.1 Conocimiento de la organización y de su contexto

- 4.2 Comprensión de las necesidades y expectativas de las partes interesadas
- 4.3 Determinación del alcance del sistema de gestión de la seguridad de la información
- 4.4 Sistema de gestión de la seguridad de la información

5 Liderazgo
- 5.1 Liderazgo y compromiso
- 5.2 Política
- 5.3 Roles, responsabilidades y autoridades en la organización

6 Planificación
- 6.1 Acciones para tratar riesgos y oportunidades
- 6.2 Objetivos de seguridad de la información y planes para lograrlos.

7 Soporte
- 7.1 Recursos
- 7.2 Competencia
- 7.3 Toma de conciencia
- 7.4 Comunicación
- 7.5 Información documentada

8 Operación
- 8.1 Planificación y control operacional
- 8.2 Valoración de riesgos de la seguridad de la información
- 8.3 Tratamiento de riesgos de la seguridad de la información

9 Evaluación del desempeño
- 9.1 Seguimiento, medición, análisis y evaluación
- 9.2 Auditoría interna
- 9.3 Revisión por la dirección

10 Mejora
- 10.1 No conformidades y acciones correctivas
- 10.2 Mejora continua

Seguridad informática como un proceso

La seguridad informática es un proceso el cual necesita ser monitoreado y evaluado constantemente, es un proceso del cual dependen otros procesos para mantener su estabilidad, y es el encargado de varias funciones que incluyen disminuir la posibilidad de incidentes de seguridad, estudiar los impactos de los riesgos en los sistemas de información y generar estrategias para minimizarlos, establecer planes de continuidad y recuperación, y realizar auditorías de los sistemas para la revisión de medidas de seguridad y actualización de las mismas conforme a las

necesidades, etc. Este proceso al igual que otros procesos productivos y organizacionales es manejado y supervisado por un equipo de expertos que se encarga de direccionarlo y mantenerlo en pie en todo momento, es por esto que en la implantación de la seguridad de la información se establece un departamento distinto el cual también tiene a cargo activos y servicios que realizan los subprocesos al interior de este departamento de seguridad TI, pero que estos activos y servicios a su vez están relacionados con cada parte de la organización, por tal razón su importancia trasciende los niveles de un proceso cualquiera, pues de su disposición y estabilidad depende toda una organización. Los niveles asociados a la seguridad de la información se encuentran subdivididos en seguridad lógica y seguridad física donde allí se tienen en cuenta tanto software, aplicaciones, bases de datos, sistemas operativos y todos los demás medios no tangibles en los que se da manejo a la información, así como la parte física ordenadores, servidores, infraestructura y demás elementos que conforman el sistema y los cuales hacen tratamiento y manejo de la información igualmente. (Solarte, 2015)

Para determinar los roles que permitirán llevar a cabo la implantación de un sistema de gestión de seguridad de la información, es preciso definir una estructura organizacional que permita delegar funciones y responsabilidades dentro del marco de trabajo para la aplicabilidad de la seguridad informática en las empresas, los roles serán mencionados a continuación junto con las funciones que le son atribuidas a cada cargo:

Dirección General

Este ente se encarga del direccionamiento estratégico y promoción del Sistema de Gestión para la Seguridad de la Información, y como parte de sus funciones tiene aprobar y verificar las políticas de seguridad implantadas al interior de la organización, concienciar a la alta gerencia acerca de la criticidad de los activos, y

difundir las responsabilidades que toda la empresa tiene conforme al proceso de implantación de la seguridad de la información.

Nivel Directivo

En el nivel directivo se aplican los lineamientos de sistema a las distintas áreas de la organización, llevando consigo en primera medida y como meta principal los objetivos de seguridad, dentro las funciones que obtiene el nivel directivo se encuentra: liderar y brindar apoyo a proceso de implantación del sistema de gestión, así como también buscar que se les dé cumplimiento a los objetivos de seguridad, determinar funciones específicas para los roles generados en cada área, aportar recursos en pro de la implementación del sistema, brindar un plan de capacitación y concienciación para los involucrados en el área, y finalmente generar sanciones y proceso disciplinario ante un incidente de seguridad. El líder de gobernanza de la organización es quien asumirá este rol.

Oficial de Seguridad de la Información

Es quien vela por el cumplimiento de los aspectos relevantes de la implantación del SGSI como son políticas, objetivos, y el cumplimiento de los mismos, para generar un reporte a un nivel directivo asociado o a la Dirección General, este cuenta con las siguientes funciones dentro del marco trabajo propuesto están: definición y clasificación de los activos de información, definición de un análisis de riesgos, plan de tratamiento de los mismo, y ejecución, definición de las políticas y procedimientos, así como también su constante actualización, definición de planes de preparación y educación de los empleados sobre la seguridad de la información, estas funciones se llevan a cabo con apoyo de cada miembro del personal de la organización.(Mega, 2009)

Comité Operativo de Seguridad de la Información

Es un comité conformado por cada uno de los representantes de cada área o dependencia y este comité es coordinado por el Oficial de Seguridad de la Información, tiene como funciones asociadas a su cargo: verificar la documentación de SGSI con el personal encargado del proceso asociado, apoyo en las funciones que desempeña el Oficial de Seguridad, así como también en otros procesos como participación en la implantación del SGSI, actualización y mejora continua.

Propietario del Activo

Es el encargado de velar por cierto activo, y además de verificar que los controles sean aplicados para el mismo, este rol es determinante por quien está al frente del mismo tiene una total responsabilidad por el activo que le es asignado resguardar, y de él depende mantener sus características de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad del mismo.

Custodio del Activo

Complementa al propietario del activo haciendo revisión sobre los cumplimientos de los requerimientos y haciendo reporte.

Responsable del riesgo

El dueño del proceso se encargará de asumir esta responsabilidad, en la cual su función es determinar el valor del riesgo, hacer gestión y tratamiento del mismo, realizar reportes en caso extremo de riesgo y hacer seguimiento de los controles.

Importancia de las metodologías de gestión de riesgos, ventajas y desventajas

En la rama de la seguridad informática las metodologías de análisis de riesgos conforman una porción indispensable para el desarrollo de las buenas prácticas en pro de la seguridad de los activos TI, estas metodologías comprenden procesos organizacionales más amplios que mejoran la toma de decisiones, y son una guía para determinar vulnerabilidades de los sistemas, generar planes de continuidad y

recuperación y generar de políticas de seguridad más adecuadas conforme a la organización. En la implantación de un SGSI son necesarias las metodologías pues es allí donde de determinan las verdaderas insuficiencias que poseen las empresas en cuanto a seguridad y de esta manera estructurar un sistema de gestión de seguridad de la información más completo y eficiente, estas se componen de diversos modelos y procesos que se llevan a cabo para la generación de un estudio sistemático y finalmente generar tácticas de reducción y prevención de riesgos. A continuación, se presentaras algunas de las principales metodologías de gestión de riesgos empleadas actualmente, y un análisis de sus principales características, ventajas y desventajas. (Solarte 2015)

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*)

Esta es una de las metodologías más empleadas por las empresas y se enfoca en la evaluación de riesgos y proponer un plan de mitigación para aplicar control sobre los mismos, sus objetivos son básicamente el generar conciencia sobre lo falso que resulta la determinación de la seguridad informática simple y únicamente en el ambiente técnico, y con esto adjuntar prácticas internacionales para contribuir con asuntos no técnicos. Octave realiza una evaluación de los activos que están involucrados con la información discriminando dos grupos principales Sistemas (Hardware, Software y Datos) y personal, y determina la importancia de cada uno de estos para la organización, partiendo de este primer análisis se encarga de realizar una proyección, clasificación y consultoría de los riesgos en las empresas, basándose en tres principales fases:

- Elaborar perfiles de amenazas en base a los activos
- Identificación de la infraestructura de las vulnerabilidades
- Desarrollo de estrategias y planes de seguridad

A partir de esta metodología la responsabilidad de generar estrategias de seguridad y planes a base de análisis de riesgos recae únicamente sobre las personas que conforman la organización, y esto implica que tiene un enfoque auto dirigido, además de esto esta metodología se centra en obtener resultados a corto y largo plazo por tanto la implantación de planes estratégicos se propone sobre lapsos de tiempo, donde con el aumento de este se genera un plan mucho más detallado para lograr adoptar las mejores prácticas y alcanzar los estándares actuales.

Esta metodología le brinda una orientación a las empresas que le aporta soluciones que ayudan a proteger los activos determinantes de las organizaciones, además de esto implanta una nueva práctica de regulación de la seguridad de la información, la evaluación que realiza en las empresas ofrece un amplio visión acerca de los riesgos de seguridad de las empresas y la importancia de comprender las situaciones que enfrentan y generar finalmente un equilibrio entre los riesgos, las nuevas prácticas de seguridad y la tecnología implementada para contribuir a esta mejora.

Tabla 10. Ventajas y desventajas de la metodología OCTAVE

OCTAVE	
Ventajas	Desventajas
• Es de uso libre y gratuito • Involucra al personal de la organización en los procesos de gestión con enfoque auto dirigido. • Orienta en la creación de un equipo funcional y multidisciplinario que	• Es una metodología adoptada únicamente por pequeñas y medianas empresas. • No posee herramientas de software que contribuyan en pro de la gestión de riesgos, el proceso se realiza a

trabaje conjuntamente de forma colaborativa en los procesos de gestión. • Realiza una evaluación general de las empresas, sin concentrarse únicamente en el sistema de información, sino que tiene todos los aspectos organizaciones en cuenta. • Relaciona amenazas y vulnerabilidades. • Es una metodología flexible pues el análisis es adaptable a los diferentes entornos de cada organización, sus objetivos y capacidad de recuperación. • Los posibles incidentes de seguridad que son provistos por la metodología es bastante extendida, y ayuda a dar una visión más amplia de cómo prevenir ciertas situaciones y establecer las medidas de seguridad.	base de una documentación de soporte. • Al implementar gran volumen de documentación la tarea de gestión resulta ser complicada. • Es una metodología sesgada a las competencias del personal que está a cargo de su ejecución, por lo tanto, si los individuos involucrados no cuentan con el conocimiento suficiente sobre los procesos y la seguridad la metodología presentara fallos. • Es un análisis cualitativo por lo tanto no permite que se modele matemáticamente el riesgo.

MAGERIT

Esta es una metodología de análisis y gestión de riesgos en los sistemas que manejan las tecnologías de la información, y fue desarrollado por el Consejo

Superior de Administración Electrónica, dentro de sus funciones principales están generar un estudio detallado de los riesgos a los que puede estar expuesto el sistema de información y los que puede soportar, así como también generar las acciones que ayudaría a la organización en la prevención y control de las situaciones de riesgo encontradas en el estudio inicial.

Los elementos importantes para establecer un análisis de riesgos sólidos y en los cuales enfoca el estudio MAGERIT están dados por activos, amenazas, impacto, riesgos y salvaguardas (procedimientos, funciones y métodos).

Esta es una metodología que prepara a las organizaciones para procesos de auditoria, certificación y acreditación. Las tres fases que implementa es su desarrollo son planificación, análisis de riesgos, gestión de riesgos y selección de medidas de seguridad o salvaguardas para los sistemas.

Tabla 11. Ventajas y desventajas de la metodología MAGERIT

MAGERIT	
Ventajas	Desventajas
• Análisis cuantitativo y cualitativo de los riesgos. • Utiliza gran variedad de técnicas que dan confiabilidad en el procedimiento de análisis de riesgos. • Mediante el estudio se genera un documento extendido de los recursos TI, las amenazas y	• Alto costo pues es necesario traducir las valoraciones de riesgo en función de costo para las organizaciones y esto implica costos altos extras. • Los procesos y las vulnerabilidades no son tenidos en cuenta como parte formal del modelo de la metodología.

vulnerabilidades relacionados coherentemente dando una visión más específica de los riesgos en las organizaciones. • Es de libre utilización. • Cuenta con un software de apoyo llamado EAR/PILAR. • El cumplimiento de los objetivos es la tarea más primordial para la metodología, y los objetivos son: divulgar y concientizar de la existencia de los riesgos en las organizaciones y la exigencia sobre establecer procedimientos que apliquen control sobre los mismos, generar un procedimientos y métodos sistemáticos en la identificación de los riesgos mencionados, y finalmente generar medidas pertinentes que conlleven a mantener el control sobre estas situaciones adversas. • Brinda apoyo a las organizaciones para enfrentar y actuar convenientemente en procesos de	• Las políticas son parcialmente contempladas en el análisis, por tanto, la valoración del sistema se encuentra incompleto. • Está concretamente diseñada para empresas que dan manejo a información digital y servicios TI.

acreditación, auditoria o certificación. • Se apoya en documentos que aporta gran variedad de información y estos libros son El método, EL catálogo de los elementos y Guía de Técnicas que cualquier persona puede emplear en el desarrollo de la gestión de riesgos. • MAGERIT actúa dentro de un marco de gestión de riesgos, que involucra a la alta gerencia en la toma de decisiones en base a la evaluación realizada.	

MEHARI

Método armonizado de análisis de riesgos, desarrollada por CLUSIF en 1996, está abierta al uso de cualquier tipo de organización de manera libre, esta metodología contribuye al oficial de seguridad de la información en procesos de gestión de la seguridad informática pero también, como gestor de riesgos, brinda apoyo a los responsables de la seguridad con análisis de riesgos mediante una evaluación cuantitativa, generando una afinidad entre los objetivos estratégicos de las

organizaciones y los nuevos métodos de funcionamiento de la empresa mediante políticas de seguridad y establecimiento del equilibrio de los niveles de riesgo. Centra toda la atención en desarrollar actividades e evaluación y gestión de riesgos conforme a las exigencias y requerimientos de la norma ISO/IES 27005: 2008. Los aspectos más importantes dentro de la metodología buscan desarrollar ciertas actividades que conjuntamente conlleven a determinar las mejores prácticas en pro de la prevención, mitigación o control de riesgos, y estas son: elaborar un diseño de modelo de riesgo, valoración de la eficiencia de las políticas de seguridad implantadas en la organización y su campo de acción. A partir de esta metodología se aprecian las diversas vulnerabilidades de los sistemas, efectuando auditorias que conlleven a estudiar los contextos en las que se están presentando para que los esfuerzos sean enfocados en esa dirección. MEHARI se organiza de la siguiente forma en la ejecución: análisis o evaluación de riesgos, evaluación de seguridad y análisis de amenazas, para finalmente construir un plan de acción idóneo para mantener la seguridad de la información. (Piattini, 2001).

Tabla 12. Ventajas y desventajas de la metodología MEHARI

MEHARI	
Ventajas	Desventajas
• Análisis cuantitativo y cualitativo • Esta metodología se apoya en bases de datos de manuales, guías y herramientas adicionales en la gestión de riesgos.	• No es tenido en cuenta en no repudio de la información como objetivo de seguridad. • Los controles de riesgos como recomendación se mencionan dentro de la gestión de riesgos y no en el análisis de riesgos.

• Es basada en formulas y parámetros con base de conocimiento. • De uso gratuito. • Cuenta con dos herramientas de software que hacen el estudio más sólido y riguroso que son Mehari Basic Tool, el cual es una hoja de Excel gratis, y también Risicare que si es una herramienta comercial. • La detección de vulnerabilidades se da a partir de auditorías estrictas y con carácter riguroso. • A partir de la implementación se pueden obtener dos tipos de evaluación, una evaluación rápida y una evaluación detallada de riesgos. • Es compatible con los requerimientos de las normas ISO 27001, 27002 y 27005. • Es adaptable a las necesidades y madurez de las organizaciones.	• Igualmente, el impacto que generan los riesgos sobre los activos es determinado en la fase final de la aplicación de la metodología que es en el proceso de gestión y evaluación de riesgos, y debería contenerse en la fase inicial de análisis. • Los dos últimos aspectos son consideraciones que hacen parte del análisis inicial de riesgo, y deben ser de conocimiento previo evitando que esta estimación tardía de los efectos sobre los activos pueda afectar a futuro, igualmente los controles, esta estructura de la metodología se encuentra desequilibrada en cuestión de organización de las prioridades.

• Las herramientas y métodos que proporciona MEHARI se pueden emplear de forma modular e independiente fuera del proceso de gestión de riesgos, en cualquier etapa del desarrollo de la seguridad de la información empleando otros enfoques de gestión. • No está limitado en el manejo de sistemas TI sino que posee dominio sobre otro tipo de sistemas.	

NIST SP 800 – 30 (National Institute of Standards and Technology). Es una metodología ideada para sistemas TI, donde se concentran una serie de procedimientos y recomendación para la gestión de riesgos, y hace parte de un proceso más complejo en la gestión de la seguridad de la información con ayuda de la organización completa. Con esta metodología es posible desarrollar un programa eficaz de gestión de riesgos, donde son plasmadas las definiciones suficientes, así como la orientación práctica para dar respuesta a los riesgos estimados. El proceso que sugiera la metodología NIST está compuesto por cuatro fases fundamentales que son evaluación, mitigación, análisis y evaluación de riesgo.

Los pasos que conforman la metodología para el análisis de riesgo:

- Caracterización del sistema
- Identificación de amenazas
- Identificación de vulnerabilidades

- Control de análisis
- Determinación del riesgo
- Análisis del impacto
- Determinación del riesgo
- Recomendaciones de control
- Resultados en la implementación y documentación

Y los pasos para la gestión de riesgo son:

- Priorización de acciones
- Evaluación de opciones de control recomendados
- Análisis coste-beneficio
- Selección de controles
- Asignación de responsabilidades
- Desarrollo de un plan de implantación de salvaguardas
- Implantación de controles seleccionados
- Recomendación de los controles seleccionados

NIST SP 800 – 30	
Ventajas	Desventajas
• Es de carácter internacional lo que permite llevar la evaluación de riesgo de las organizaciones a una estandarización en relación con otros países. • Facilita la certificación 17999. • Realiza un análisis de riesgos completo cualitativo y cuantitativo. • En sus inventarios genera un a información clara y completa de	• Es una herramienta comercial por tanto su licencia de uso tiene un costo. • En sus objetivos de seguridad se encuentran únicamente confidencialidad, disponibilidad e integridad dejando de lado la autenticidad, trazabilidad y no repudio. • No tiene incluido como elemento del modelo a los procesos, activos y dependencias,

los elementos tenidos en cuenta en el modelo.	únicamente tiene en cuenta los recursos, vulnerabilidades, amenazas y salvaguardas. • No posee herramientas ni técnicas adicionales sobre las cuales tener apoyo para el estudio, por el contrario, la única estrategia es designar roles. • A pesar de ser una metodología robusta tiene limitaciones para se implementada en pequeñas empresas debido a sus demandas de recursos. • No se puede emplear para determinar riesgos organizativos, pues no hay una descripción puntual de los activos, por el contrario se analiza la infraestructura específica y la limitaciones en cuanto a seguridad que posee.

Cramm (CCTA risk analysis and management method)

Esta metodología fue desarrollada por el CCTA (Central Communication and Telecommunication Agency) en el Reino Unido, está orientada al análisis de riesgos de las grandes empresas, esta metodología está conformada por tres etapas:

- Establecer los objetivos de seguridad
- Realizar un análisis de riesgos
- Identificar y seleccionar salvaguardas

A partir de las herramientas de esta metodología las organizaciones generan documentación de seguridad y se establecen planes de contingencia a partir de un análisis exhaustivo de los riesgos y vulnerabilidades. (Syalim, 2009)

Tabla 13. Ventajas y desventajas de la metodología CRAMM

CRAMM	
Ventajas	Desventajas
• Es de carácter internacional. • Emplea herramientas extras en el análisis de riesgos, además de definición de roles, comparativas y cuestionarios. • Sirve de apoyo para que las organizaciones obtengan certificaciones como BS 7799 e ISO 17999. • Tiene un alcance amplio tanto en análisis como en gestión de riesgos. • Su análisis es cualitativo y cuantitativo.	• Tiene un costo por la licencia para poder hacer uso de ella. • Hace énfasis únicamente en tres objetivos de seguridad que son integridad, confidencialidad y disponibilidad obviando otros aspectos importantes como trazabilidad, autenticidad y no repudio. • Se enfoca únicamente en los activos y dependencias como elementos del modelo, como elementos del análisis también se encuentran vulnerabilidades, amenazas y salvaguardas, los procesos y los recursos no son

• Los inventarios realizados a partir de esta metodología son muy completos y detallados para cada uno de los elementos del modelo. • Generación de concienciación del personal de las organizaciones sobre la seguridad de la información. • Elaboración de una revisión completa y de alto nivel y una revisión rápida. • La base de datos que se obtiene a partir del estudio de análisis de riesgos es extensa y se actualiza constantemente. • Se da prioridad a las medidas de seguridad teniendo en cuenta que tan eficientes son y el costo que representan para la organización.	tenidos en cuenta por tanto existen aspectos sin someterlos a evaluación. • Es necesario contar con profesionales calificados para el uso de la metodología. • Las revisiones detalladas incurren en grandes gastos, por su larga duración, y el amplio volumen en documentación.

Dominios, objetivos y controles de la norma ISO/IEC 27002:2013

La norma ISO/IEC 27002:2013, cuenta con 14 dominios, 35 objetivos y 114 controles, descritos por el siguiente cuadro: (Disterer, 2013)

Dominios, objetivos y controles de la norma ISO/IEC 27002:2013		
Dominios	Objetivos	Controles
POLITICAS DE SEGURIDAD	Directrices de la dirección en seguridad de la información	Conjunto de políticas para la seguridad de la información
		Revisión de las políticas para la seguridad de la información
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	Organización interna	Asignación de responsabilidades para la seguridad de la información
		Segregación de tareas
		Contacto con las autoridades
		Contacto con grupos de interés especial
		Seguridad de la información en la gestión de proyectos
	Dispositivos para la movilidad y teletrabajo	Política de uso de dispositivos para la movilidad
		Teletrabajo
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	Antes de la contratación	Investigación de antecedentes
		Términos y condiciones de contratación
	Durante la contratación	Responsabilidades de gestión
		Concienciación, educación y capacitación en seguridad de la información
		Proceso disciplinario

	Cese o cambio de puesto de trabajo	Cese o cambio de puesto de trabajo
GESTIÓN DE ACTIVOS	Responsabilidad sobre los activos	Inventario de activos
		Propiedad de los activos
		Uso aceptable de los activos
		Devolución de activos
	Clasificación de la información	Directrices de clasificación
		Etiquetado y manipulado de la información
		Manipulación de activos
	Manejo de los soportes de almacenamiento	Gestión de soportes extraíbles
		Eliminación de soportes
		Soportes físicos en tránsito
CONTROL DE ACCESOS	Requisitos de negocio para el control	Política de control de accesos
		Control de acceso a las redes y servicios asociados
	Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios
		Gestión de los derechos de acceso con privilegios especiales
		Gestión de los derechos de acceso asignados a usuarios
		Gestión de la información confidencial de autenticación de usuarios
		Revisión de los derechos de acceso de los usuarios
		Retirada o adaptación de los derechos de acceso

	Responsabilidades del usuario	Uso de información confidencial para la autenticación
	Control de acceso a sistemas y aplicaciones	Restricción del acceso a la información
		Procedimientos seguros de inicio de sesión
		Gestión de contraseñas de usuario
		Uso de herramientas de administración de sistemas
		Control de acceso al código fuente de los programas
CIFRADO	Controles criptográficos	Política de uso de los controles criptográficos
		Gestión de claves
SEGURIDAD FÍSICA Y AMBIENTAL	Áreas seguras	Perímetro de seguridad física
		Controles físicos de entrada
		Seguridad de oficinas, despachos y recursos
		Protección contra las amenazas externas y ambientales
		El trabajo en áreas seguras
		Áreas de acceso público, carga y descarga
	Seguridad de los equipos	Emplazamiento y protección de equipos
		Instalaciones de suministro
		Seguridad del cableado
		Mantenimiento de los equipos
		Salida de activos fuera de las dependencias de la empresa

		Seguridad de los equipos y activos fuera de las instalaciones
		Reutilización o retirada segura de dispositivos de almacenamiento
		Equipo informático de usuario desatendido
		Política de puesto de trabajo despejado y bloqueo de pantalla
	Responsabilidades y procedimientos de la operación	Documentación de procedimientos de operación
		Gestión de cambios
		Gestión de capacidades
		Separación de entornos de desarrollo, prueba y producción
SEGURIDAD EN LA OPERATIVA	Protección contra código malicioso	Controles contra el código malicioso
	Copias de seguridad	Copias de seguridad de la información
	Registro de actividad y supervisión	Registro y gestión de eventos de actividad
		Protección de los registros de información
		Registros de actividad del administrador y operador del sistema
		Sincronización de relojes
	Control del software en explotación	Instalación del software en sistemas de producción
	Gestión de la vulnerabilidad técnica	Gestión de vulnerabilidades técnicas
		Restricciones en la instalación de software

	Consideraciones de las auditorías de los sistemas de información	Controles de auditoría de los sistemas de información
SEGURIDAD EN LAS TELECOMUNICACIONES	Gestión de la seguridad en las redes	Controles de red
		Mecanismos de seguridad asociados a servicios en red
		Segregación de redes
	Intercambio de información con partes externas	Políticas y procedimientos de intercambio de información
		Acuerdos de intercambio
		Mensajería electrónica
		Acuerdos de confidencialidad y secreto
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Requisitos de seguridad de los sistemas de información	Análisis y especificación de los requisitos en la seguridad
		Seguridad de las comunicaciones en servicios accesibles por redes públicas
		Protección de las transacciones por redes telemáticas
	Seguridad en los procesos de desarrollo y soporte	Política de desarrollo de seguro de software
		Procedimientos de control de cambios en los sistemas
		Revisión técnica de las aplicaciones tras efectuar cambios en le sistema operativo
		Restricciones a los cambios en los paquetes de software
		Uso de principios de ingeniería en protección de sistemas

		Seguridad en entornos de desarrollo
		Externalización del desarrollo de software
		Pruebas de funcionalidad durante el desarrollo de los sistemas
		Pruebas de aceptación
	Datos de prueba	Protección de los datos utilizados en pruebas
RELACIONES CON SUMINISTROS	Seguridad de la información en las relaciones con suministradores	Política de seguridad de la información para suministradores
		Tratamiento del riesgo dentro de los acuerdos de suministradores
		Cadena de suministro en tecnologías de la información y comunicaciones
	Gestión de la prestación del servicio por suministradores	Supervisión y revisión de los servicios prestados por terceros
		Gestión de cambios en los servicios prestados por terceros
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Gestión de incidentes de seguridad de la información y mejoras	Responsabilidades y procedimientos
		Notificación de los eventos de seguridad de la información
		Notificación de los puntos débiles de la seguridad
		Valoración de eventos de seguridad de la información y toma de decisiones
		Respuesta a los incidentes de seguridad

		Aprendizaje de los incidentes de seguridad de la información
		Recopilación de evidencias
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información
		Implantación de la continuidad de la seguridad de la información
		Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	Redundancias	Disponibilidad de las instalaciones para el procesamiento de la información
CUMPLIMIENTO	Cumplimiento de los requisitos legales y contractuales	Identificación de la legislación aplicable
		Derechos de propiedad intelectual
		Protección de los registros de la organización
		Protección de datos y privacidad de la información personal
		Regulación de los controles criptográficos
	Revisiones de la seguridad de la Información	Revisión independiente de la seguridad de la información
		Cumplimiento de las políticas y normas de seguridad
		Comprobación del cumplimiento

Importancia de la articulación de controles y sus tipos, diferencia entre estándares, directrices, procedimientos, políticas y normas para el SGSI

Es de vital importancia para cada una de las organizaciones que pretendan establecer un modelo de gestión, definir el monitoreo de su SGSI y los controles que se van a utilizar, de esa manera fortalece los controles de todo el sistema. Es por ello, que establecer un adecuado nivel de clasificación de los controles, contribuye a el fortalecimiento de la protección de la información. En ese sentido, se hace necesario implementar procesos de auditoria al interior de las organizaciones, el proceso auditable provee una retroalimentación constante del sistema para mejorar los procesos y la tecnología utilizados para proteger la compañía. (Mega, 2009)

Clasificación de los controles de SGSI

- **Controles de configuración:** hacen referencia a los métodos empleados en la minimización ante la probabilidad de que los atacantes puedan identificar las debilidades que existen en el sistema y que por ende pueden explotar. En esa categoría se encuentran por ejemplo el Análisis de Vulnerabilidades o los Pentreation Test, servicios que hacen parte del ESET Security Services.
- **Controles de accesos:** hacen referencia a herramientas acortan la probabilidad de que un atacante pueda ingresar de manera no autorizada a los sistemas de la organización. Esta categoría se compone por capas de detección de malware además de agregar un firewall personal,

protección para clientes de correo electrónico incluyendo el bloqueo de correo SPAM y un poderoso filtrado de URL.

- **Monitoreo:** es la capa en donde se incluye la documentación y el análisis de logs, cuyo propósito es el de contribuir a detectar problemas y otorgar la información vital para darle solución. A su vez, permite disminuir la probabilidad de ocurrencia a cualquier riesgo que, de una forma u otra, afecte la seguridad de la información por medio de la comunicación retroalimentada hacia las otras dos categorías.

1. Estándares que intervienen en la acentuación de los SGSI

La especificación de lo que se relata a continuación, fue tomado de los documentos originales de los estándares ISO del siguiente enlace web: http://www.iso27000.es/sgsi.html.

- ***ISO/IEC 27000***

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. En este, se definen las directrices, políticas y procedimientos para la ejecución de los SGSI.

- ***ISO/IEC 27001***

Fundamentalmente, se basa en la facultad de proteger la confidencialidad, integridad y disponibilidad de la información al interior de una organización. Para ello establece procedimientos y directrices que contribuyen a investigar cuáles son los problemas potenciales que pudiesen afectar a la información, evaluación de riesgos y finalmente define los parámetros necesarios para mitigar dichos

problemas. En resumen, se puede decir lo siguiente: este estándar se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

- ***ISO/IEC 27002***

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede leer La norma ISO 27002 complemento para la ISO 27001.La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza. La norma ISO 27002 se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles. El documento denominado política es aquel que expresa una intención e instrucción general de la forma que ha sido expresada por la dirección de la empresa. El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y

específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas.

Finalmente, se puede resumir gran parte de la información acerca del levantamiento de los datos en un SGSI con el siguiente cuadro titulado “Programas, procesos y políticas de seguridad informática”.

Tabla 14. políticas de seguridad informática

Programas, procesos y políticas de seguridad informática		
Programa	Procedimiento	Política
Seguridad del recurso humano	PROCEDIMIENTO DE CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL PROCEDIMIENTO DE INGRESO Y DESVINCULACIÓN DEL PERSONAL	POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS
Gestión de activos	PROCEDIMIENTO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS	CLASIFICACIÓN DE LOS RECURSOS
Control de acceso	PROCEDIMIENTO PARA INGRESO SEGURO A LOS SISTEMAS DE INFORMACIÓN PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y CONTRASEÑAS	Ley 527 de 1999: “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Criptografía	PROCEDIMIENTO DE CONTROLES CRIPTOGRÁFICOS PROCEDIMIENTO DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS	POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS
Seguridad física y del entorno	PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS: PROCEDIMIENTO DE RETIRO DE ACTIVOS: PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS:	ISO 27002 “Política para el control de acceso”
Seguridad de las operaciones	PROCEDIMIENTO DE GESTIÓN DE CAMBIOS: PROCEDIMIENTO DE GESTIÓN DE CAPACIDAD: PROCEDIMIENTO DE SEPARACIÓN DE AMBIENTES: PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:	POLÍTICA DE ADMINISTRACIÓN DE BACKUP

Capítulo 4

Gestión de Riesgo

El presente capitulo describe la metodología a utilizar para la gestión de riesgos, con el fin de que los encargados de la red tomen decisiones correctas según los datos tomados con respecto a la seguridad de las comunicaciones, así como el inventario de equipos del canal teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información, teniendo una valoración de los riesgos que se pueden encontrar en la empresa.

4.1 Metodología.

Como metodología a seguir para la implementación de la seguridad en las comunicaciones, se analizaron la ISO/IEC 27005 y la MAGERIT, para compararlas como se muestra en la Tabla 15 y determinar cuál es la más adecuada a la adaptación del proyecto.

Tabla 15. Comparación Metodologías.

METODOLOGÍAS	ISO/IEC 27005	MAGERIT
Fases del Método de Análisis de Riesgo	- Alcance - Normativas de referencia - Términos y definiciones - Estructura - Antecedentes	- **Identificar activos:** activos relevantes, su interrelación y valoración. **- Identificar amenazas:** Determinar las salvaguardas que hay dispuestas y cuan eficaces son frente al riesgo.

	- Visión del progreso de gestión de riesgos de seguridad de la información - Establecimiento del contexto - Evaluación de riesgos - Tratamiento de riesgo - Aceptación del riesgo - Comunicación del riesgo - Monitorización y revisión del riesgo, todas esta establecidas bajo unas cláusulas del estándar internacional.	**- Estimar el impacto:** daño sobre el activo derivado de la materialización de la amenaza. **- Estimar el riesgo:** impacto ponderado con la tasa de ocurrencia de la amenaza.
Ámbito de Aplicación	Puede ser aplicada en cualquier organización pública o sociedades mercantiles, administraciones públicas, organizaciones no lucrativas, agencias públicas, ONGs o bien la entidad que gestione un SGSI y proteger todo lo que afecte la seguridad de la información. Que tengan la intención de manejar los riesgos que podrían comprometer la seguridad de la información de la organización.	Ámbito de aplicación: Gobierno, Organismos, compañías grandes, PYME, compañías comerciales y no comerciales. Magerit ofrece una aplicación para el análisis y gestión de riesgos de un sistema de información denominado PILAR (Proceso informático lógico para el análisis de gestión de riesgos) Esta herramienta es de uso gratuito para la administración española y de uso comercial para las organizaciones privadas.
Ventajas	- Permite identificar las necesidades de la organización sobre los requisitos de seguridad de información. - Ayuda a crear los SGSI eficaz. - Aborda los riesgos de manera eficaz y oportuna, donde y cuando sea necesario. - Es parte de integridad de todas las actividades de gestión de seguridad de la información tanto para su aplicación como	- Es metódica por lo que se hace fácil su comprensión. Los activos se identifican - Tipifican, se buscan sus dependencias, se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad. - Comprende los procesos de Análisis y gestión de riesgos. Usa un modelo de análisis de Riesgos cualitativo y

	para su operación continua de un SGSI.	cuantitativo. - Soporta herramientas comerciales EAR y NO comerciales PILAR, así como las normas ISO/IEC 27001:2013.
Desventajas	No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.	- No toma en cuenta el principio de no repudio de la información como objetivo de seguridad. - No toma en cuenta un análisis de vulnerabilidades. - La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y evaluación. - Comprende como elementos del modelo de análisis sólo: activos y dependencias, vulnerabilidades y amenazas.

Al momento de comparar los beneficios y contraprestaciones de ambas metodologías, se llegó a la conclusión de que la metodología MAGERIT, es la más adecuada a la hora de implementar un método de análisis de riesgos, ya que cuenta con un mayor número de pautas que permiten obtener de manera más rápida los resultados del proceso, debido a que posee una estructura mucho más sólida, metodológicamente hablando.

Como se mencionó en el capítulo anterior, MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser explotadas por dichas amenazas, logrando así, una plena identificación de las medidas preventivas y correctivas más apropiadas (Amaya, www.welivesecurity.com, 2013).

Lo interesante de esta metodología, es que presenta una guía completa del paso a paso acerca de cómo llevar a cabo el análisis de riesgos dentro de la organización. Esta metodología está dividida en tres libros, el primero de ellos hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos. Este libro está enmarcado en los lineamientos ISO para la gestión de riesgos.

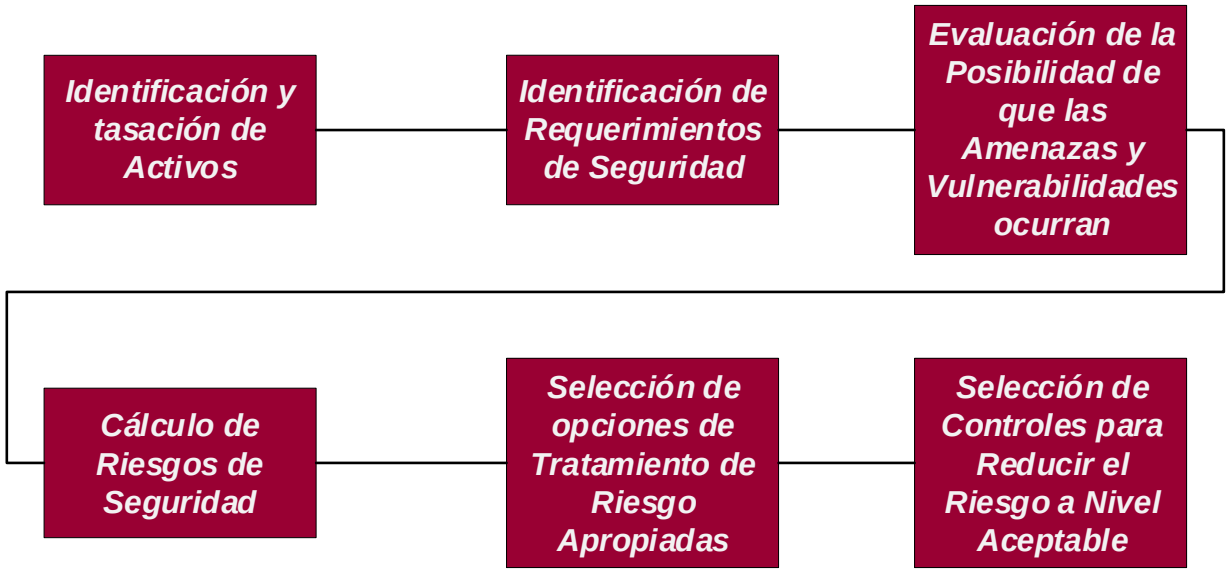


Figura 12. Metodología MAGERIT

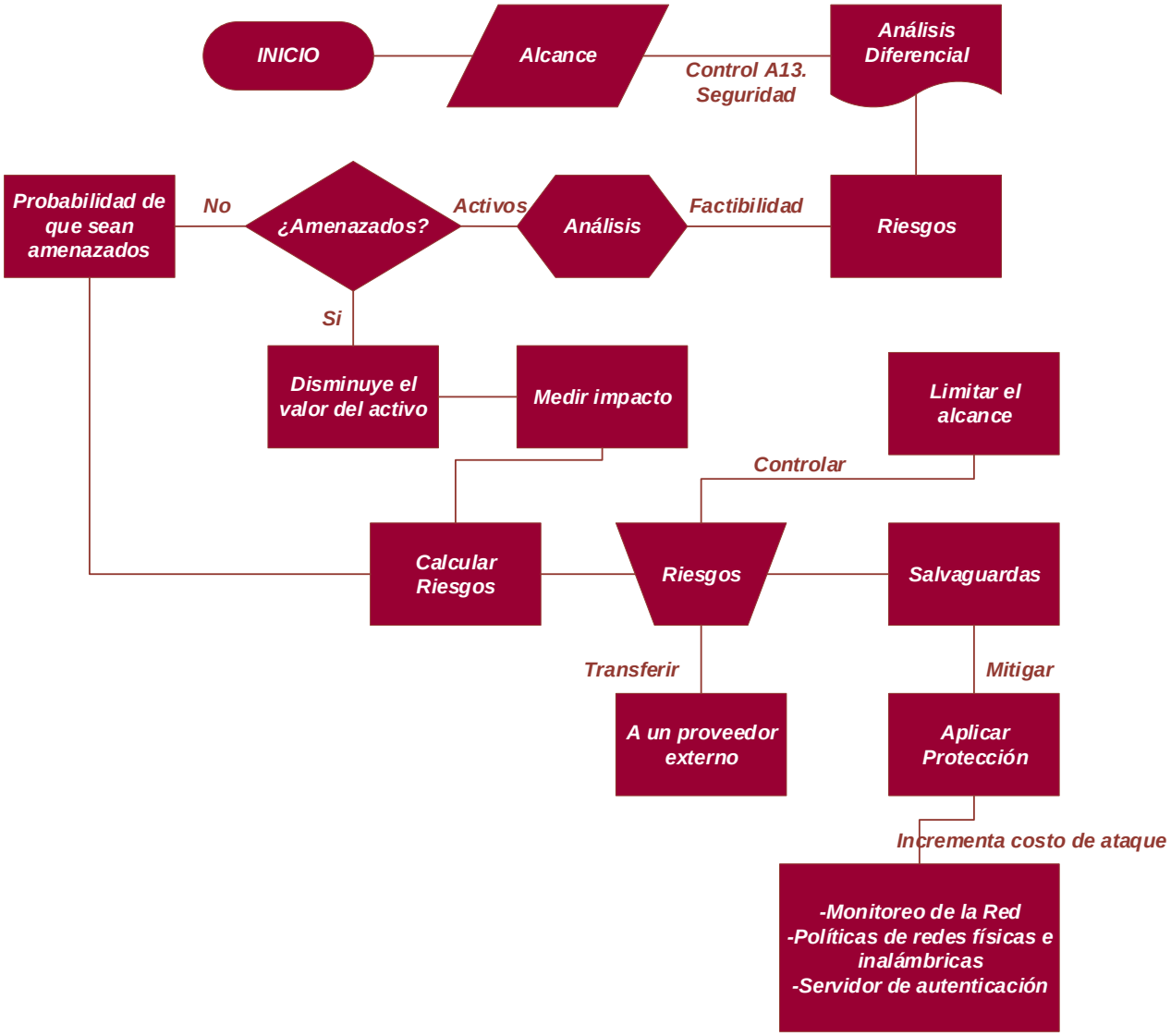


Figura 13 . Análisis de Riesgo

En la Figura 13 se muestran los pasos a seguir, para llevar a cabo de forma correcta el proceso de aseguramiento de la información con respecto al control A.13, eje central de éste trabajo. En concordancia con lo anterior, se analiza el estado actual

de la red, los riesgos posibles en itinerantica con los activos que cuenta la organización, y de cómo éstos riesgos afectan el desempeño de los activos.

Al calcular los riesgos se toman decisiones, dependiendo del alcance de cada uno, dichas decisiones se dividen en 3 categorías: Controlar, Transferir y Mitigar, en ésta última se ejecutan los controles de protección que contribuyen a la disminución de riesgos a ser atacados.

4.2 Análisis Diferencial

4.2.1 Controles de acceso

El canal cuenta con dos entradas a las instalaciones, que se encuentran vigiladas por personal especializado en vigilancia, valga la redundancia. Cada entrada de acceso cuenta con registro físico de entrada y salida de personal, en esa minuta casualmente se toman los datos de personas nuevas que acceden a las instalaciones del canal, así como también el ingreso y salida de equipos.

El canal no cuenta con ningún tipo de equipo o software que facilite al vigilante un registro de identificación de personas, como se muestra en las Figura 14 y

Figura 15, las cámaras solo son gestionadas por el departamento de técnica.

Figura 14. Entrada Canal

Figura 15. Pasillo entrada Estudio

4.2.2 Inventario de Activos

Para comenzar se requiere realizar un inventario de activos. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización, como se visualiza en la tabla 11 “Listado de Activos”. Incluye: información, datos, servicios, aplicaciones

(software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.[6]

Tabla 16. Listado de Activos

Tipo	Activo	Descripción
Datos	*Backups*	Discos duros, memorias USB, Cds. Con información del área de Edición, Archivo audiovisual, camarógrafos, reporteros y otras dependencias que necesiten estos equipos.
Hardware	Routers Inalámbricos	UNIFI ap long RANGE UBIQUITI.
Software	Servidor de Correos	Gmail empresarial, contrato de servicio de correo pago. Con el dominio @canaltro.
Hardware	UPS	Servicio de baterías ante un eventual corte de corriente.
Instalaciones	Sedes de Operación	Cuenta con dos Sedes - Bucaramanga. - Cúcuta.
Instalaciones	Sala Eléctrica	Ubicada en el segundo piso del canal
Software	Base de datos	Servidor storage, donde se almacena registro de actividades dentro de la red.
Hardware	*Switch* CORE	Cloud CORE router CCR-1016 MIKROTIK.
Hardware	*Switch* HP	Filenetwork 5130 JG934A
Hardware	*Switch*	HPE OfficeConnect 1950 series Switch JH295A
Hardware	Servidor de archivos	Equipos VPN, comunicación entre las dos sedes.

[6] [UNE 71504:2008]

Hardware	Equipos VSN	VSNcapturer1CH VSNBroadrecTRO VSNMatic VSNPrompter VSN Storage y trimmer VSN Livecom VENICE DVS livecom SISTEMA MAM – VSNSpider VSNWorker01 VSNMulticon Venice DVS-Mcon
Software	Sistema operativo servidores	Windows server 2008. Windows server 2012. Centos(modo consola)

4.2.3 Valoración de Activos

Siguiendo la metodología se toma una tabla de valoración, que se enfoca en los tres pilares fundamentales en la seguridad de información: Confidencialidad, integridad y disponibilidad.

Para calificar el valor de los activos, se toman valores de riesgo determinando si el activo se encuentra o no en disponibilidad, si ha sido modificado o si por el contrario ha sido manipulado por personal no autorizado, teniendo en cuenta que cuando se visualice una valoración de muy alto (MA), simboliza que se requiere de una acción de ejecución inmediata para mitigar el riesgo, para ello se realiza la valoración teniendo presentes los siguientes niveles de riesgo:

- **MB:** muy bajo

• **B:** bajo

• **M:** medio

• **A:** alto

• **MA:** muy alto

4.2.3.1 Confidencialidad.

Se refiere a como la información debe llegar únicamente a las personas autorizadas, según las características de la información procesada y gestionada. Se toman unas valoraciones que se tienen en cuenta para la evaluación.

¿Qué importancia tendría que el activo no estuviera disponible?

Tabla 17 Valoracion de activos Confidencialidad

ACTIVO	MB	B	M	A	MA
Discos duros, memorias USB, Cds. Con información del área de Edición, Archivo audiovisual, camarógrafos, reporteros y otras dependencias que necesiten estos equipos.					x
UNIFI ap long RANGE UBIQUITI.			x		
Gmail empresarial, contrato de servicio de correo pago. Con el dominio @canaltro.					x
Transferencia de archivos a través de VPN con la sede de Bucaramanga.					x
Servidor storage, donde se almacena registro de actividades dentro de la red.				x	

Cloud CORE router CCR-1016 MIKROTIK.					x
Filenetwork 5130 JG934A					x
HPE OfficeConnect 1950 series Switch JH295A					x
Equipos VPN, comunicación entre las dos sedes.					x
VSNcapturer1CH VSNBroadrecTRO VSNMatic VSNPrompter VSN Storage y trimmer VSN Livecom VENICE DVS livecom SISTEMA MAM – VSNSpider VSNWorker01 VSNMulticon Venice DVS-Mcon					x
Windows server 2008. Windows server 2012. Centos(modo consola)					x

4.2.3.2 Integridad

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Tabla 18. Valoración de activos Integridad

ACTIVO	MB	B	M	A	MA
Discos duros, memorias USB, Cds. Con información del área de Edición, Archivo audiovisual, camarógrafos, reporteros y otras dependencias que necesiten estos equipos.					x
Gmail empresarial, contrato de servicio de correo pago. Con el dominio @canaltro.					x
Transferencia de archivos a través de VPN con la sede de Bucaramanga.					x
Servidor storage, donde se almacena registro de actividades dentro de la red.					X
VSNcapturer1CH VSNBroadrecTRO VSNMatic VSNPrompter VSN Storage y trimmer VSN Livecom VENICE DVS livecom SISTEMA MAM – VSNSpider VSNWorker01 VSNMulticon Venice DVS-Mcon					x
Windows server 2008. Windows server 2012. Centos(modo consola)					x

4.2.3.3 Disponibilidad.

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Tabla 19. Valoración de activos Confidencialidad

ACTIVO	MB	B	M	A	MA
Discos duros, memorias USB, Cds. Con información del área de Edición, Archivo audiovisual, camarógrafos, reporteros y otras dependencias que necesiten estos equipos.					x
Gmail empresarial, contrato de servicio de correo pago. Con el dominio @canaltro.					x
Transferencia de archivos a través de VPN con la sede de Bucaramanga.					x
Servidor storage, donde se almacena registro de actividades dentro de la red.					x
Equipos VPN, comunicación entre las dos sedes.					x
VSNcapturer1CH VSNBroadrecTRO					x

VSNMatic VSNPrompter VSN Storage y trimmer VSN Livecom VENICE DVS livecom SISTEMA MAM – VSNSpider VSNWorker01 VSNMulticon Venice DVS-Mcon					
Windows server 2008. Windows server 2012. Centos(modo consola)					X

Capítulo 5

Resultados de selección y aplicación de salvaguardas

Luego de valorar los activos con respecto al anexo A.13, se buscarán estrategias que permitan controlar, transferir o mitigar el daño (ver Figura 16) causado por algún ataque como la de denegación de servicio (DoS), IP Spoofing que es la suplantación de IP, llamada suplantación de identidad, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema informático buscando soluciones respecto a la norma ISO/IEC 27001:2013, ya teniendo los riesgos identificados en este capítulo se procederá a mostrar las herramientas que pueden ser útiles para el canal TRO, estableciendo un correcto uso de los activos de forma que no vulnere los pilares básicos de la confidencialidad, disponibilidad e integridad de la información tratada por el departamento de gestión de archivo audiovisual. .

5.1 Evaluación de los riesgos

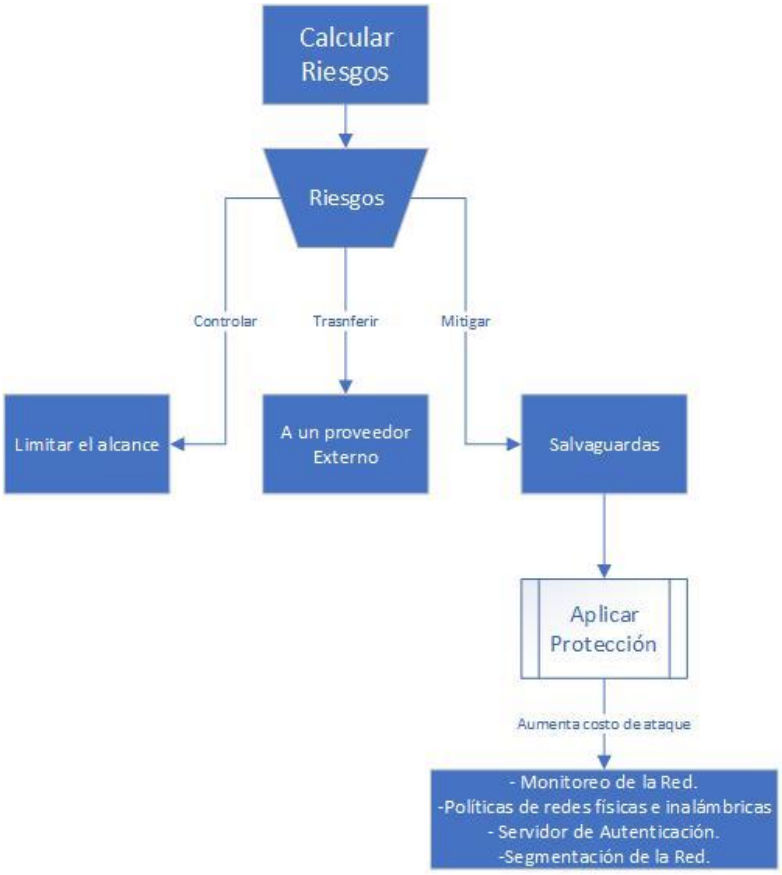


Figura 16. Riesgos

Es necesario para la empresa hacer una adecuada evaluación de riesgos que permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar esas vulnerabilidades. En la medida que el canal tenga clara esta identificación de riesgos, se podrán establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en la información.

Se estipulan tres soluciones: controlar, transferir y mitigar; para una de las vulnerabilidades que se presentan, como lo es el uso de la red inalámbrica cuyas

credenciales representan un fácil acceso. Ahora bien, para limitar esta vulnerabilidad se recomienda el uso de contraseñas por usuario aprovechando el uso de cuentas en un servidor de dominio, a su vez, al tener una vulnerabilidad como el uso de dispositivos externos con riesgo de virus se podría solicitar el uso de un antivirus suministrado por un proveedor externo, por ello se decide gestionar herramientas que ayuden a mitigar el riesgo que se mostraran a continuación.

5.1.1 Selección de salvaguardas controles de red

Siempre es importante resaltar que de acuerdo a las políticas del Canal TRO, se decide mitigar la vulnerabilidad que se presenta en la red inalámbrica con la contraseña única que a final de cuentas es la fuente de la vulnerabilidad, permitiendo así, control de acceso por ataque de fuerza bruta, dicho ataque es un método para averiguar una contraseña probando todas las combinaciones posibles hasta que finalmente se obtenga la correcta. Los ataques por fuerza bruta representan unas de las técnicas más habituales de robo de contraseñas en Internet dado que no es necesario tener grandes conocimientos en seguridad informática para realizar uno y existen programas que realizan de forma automática todo el trabajo.

5.1.1.1 Políticas de redes físicas e inalámbricas.

El canal cuenta con políticas de redes para el mantenimiento y recepción de los equipos, como el procedimiento para la gestión de recursos tecnológicos en donde se particulariza el adecuado manejo de las soluciones web, manejo de servidores locales y externos, de lo anterior se debe resaltar que, la última modificación se realizó en el año 2015. Sin embargo, de lo anterior se puede señalar que, el Canal en este ámbito no cuenta con una óptima seguridad para el acceso a los recursos físicos, sólo se simplifica al empleo de cámaras de seguridad y un vigilante en cada

uno de los accesos al canal, por ello se proponen en los siguientes apartados las herramientas necesarias para mejorar la seguridad de acceso al canal.

5.1.2 Seguridad inalámbrica protocolo WPA2-Enterprise

Para mejorar la seguridad de la red inalámbrica del canal, se propone la implementación de WPA2-Enterprise, aprovechando las tecnologías de Active Directory, Group Policy y un servidor RADIUS, que permitirán emplear configuraciones y generar nuevas credenciales en la red inalámbrica.

De lo anterior, se puede destacar que debido al aprovechamiento de las políticas de grupo y el servidor RADIUS, se podrán enviar certificados a los dispositivos cliente y crear nuevas políticas de seguridad, que asignen automáticamente los dispositivos a sus redes correspondientes. Lo beneficios más importantes al implementar este servicio son:

- Tener un control real sobre los usuarios que se conectaran.
- Si la clave del usuario ha sido comprometida, es fácil realizar un cambio.
- Si el usuario sale de la empresa, se puede borrar o deshabilitar.

Para que el 802.1X pueda funcionar, se requerirán tres protocolos:

***Extensible Authentication Protocol* (EAP):** este realizará el proceso de autenticación entre el suplicante hacia el servidor de autenticación. (Ver Figura 17)

***EAP over LAN* (EAPoL):** Transporta la comunicación entre el suplicante y el ente autenticador. EAPoL, similar a EAP, es una encapsulación simple que se puede ejecutar en cualquier LAN. Los mismos tres componentes principales se definen en EAP y EAPoL para lograr la conversación de autenticación.

***Remote Authetication Protocol* (RADIUS):** se encarga de transportar los mensajes EAP entre el autenticador y el servidor de autenticación, como se muestra en la figura 17.

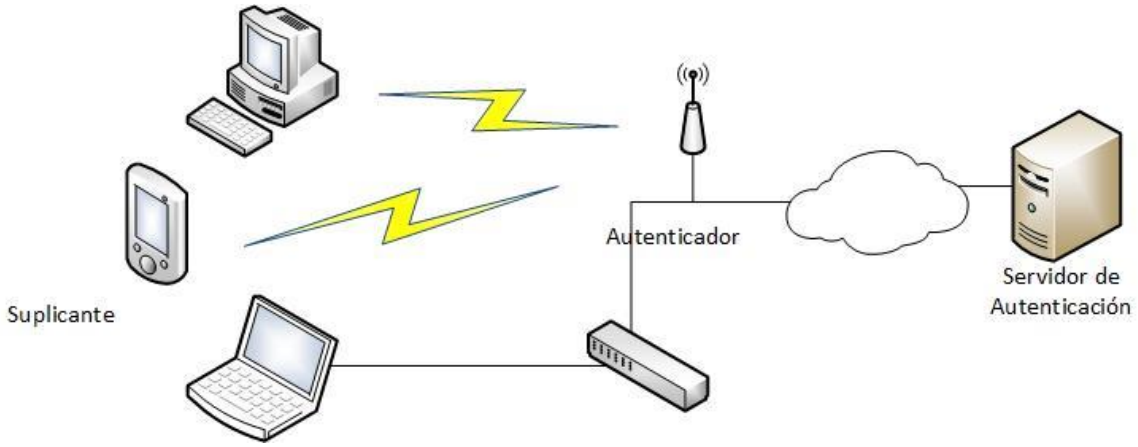


Figura 17. Autenticación EAP

En este caso se configurará un dispositivo mikrotik para que autentique a los usuarios registrados en el servidor de dominio Active Directory. Como se muestra en la Figura 18.

Wi-Fi Protected Access 2 – Enterprise (WPA2-Enterprise): como the WPA-estándar de Enterprise, WPA2-empresa utiliza la 802.1X y un marco de EAP. A su vez, proporciona mayor protección de datos para varios usuarios y grandes redes administradas. Puede definirse como un protocolo eficaz, diseñado para impedir el acceso de red a abonados no autorizados mediante la comprobación de los usuarios de red mediante un servidor de autenticación. La configuración del servicio puede evidenciarse en el perfil de seguridad de la figura 18.

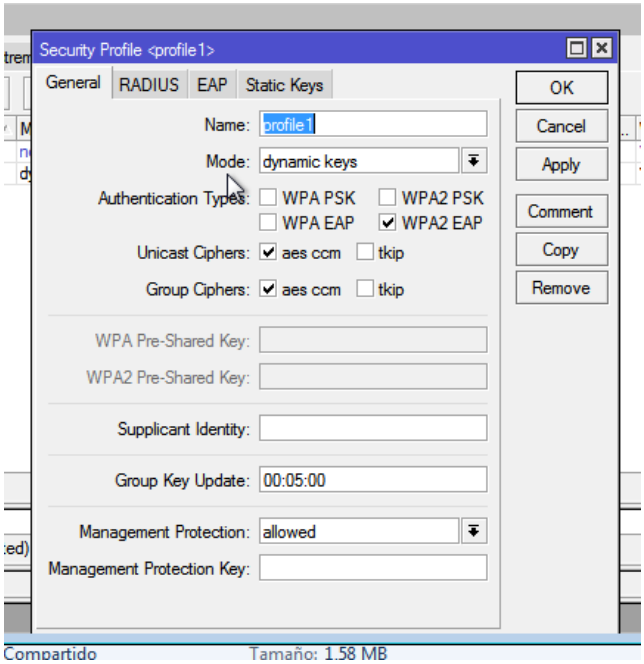


Figura 18. Perfil de seguridad

Previamente configurado el cliente RADIUS, en el servidor de dominio como se muestra en la Figura 19, se ha generado la clave secreta compartida, que será utilizada en la configuración del dispositivo mikrotik y la comunicación segura entre los dos (RADIUS-MICROTIK).

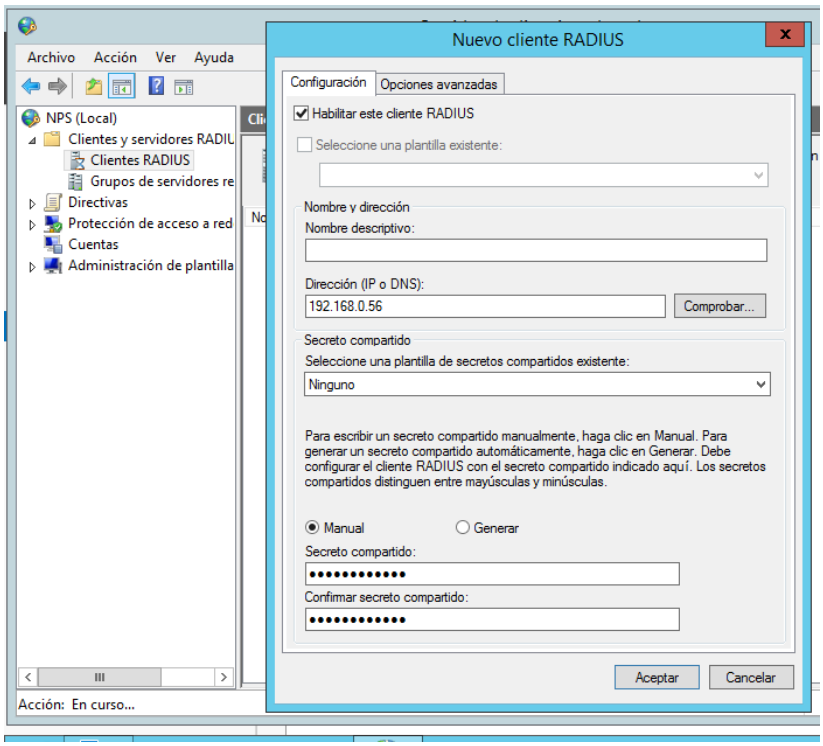


Figura 19. Nuevo cliente RADIUS

Control de Acceso Peatonal

El sistema de control de acceso peatonal permitirá gestionar el acceso de todo el personal que transita en el espacio de la organización, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas en las áreas más importantes. La solución para el control de accesos peatonal es variada dependiendo de las aplicaciones y las necesidades, se pueden tener desde soluciones con un solo dispositivo que controla una puerta, hasta soluciones con múltiples dispositivos integrados a diferentes sistemas electromecánicos gestionados por medio de software centralizado, un claro ejemplo es:

Lector De Huellas Digitales

Figura 20. Lector de huellas
Fuente: http://www.dointech.com.co/control-acceso-peatonal.html

Este dispositivo generalmente dispone una manera de control biométrico, empleada comúnmente como parte integral de un sistema de control de acceso. Los sistemas biométricos forman parte de una gran gama de alternativas usadas para la identificación de individuos, esto se debe a que, los sistemas biométricos hacen un análisis de cualidades personales únicos en cada individuo, como lo son las huellas dactilares, la retina, el iris y la geometría de la mano. El lector de huellas dactilares es la forma de control biométrico más popular y más eficiente en la verificación e identificación para control de accesos.

Ventajas

- Identificación rápida en el dispositivo (menos de 1seg)
- Identificación única por cada usuario

- No es necesario memorizar claves
- No es necesario cargar con tarjetas o controles
- La huella dactilar no es posible extraviarla
- No genera costo extra para cada usuario

Torniquetes de acero

El Torniquete está indicado para control de acceso peatonal en las zonas de la empresa con alto tránsito de personas. Es ideal como barrera de control para sitios donde se desee regular el flujo de personas en las operaciones de entrada y salida. Es perfectamente compatible e integrable con todos los dispositivos de control de accesos según sea la aplicación.

Los torniquetes de acceso son mecanismos electromecánicos de alta confiabilidad, construidos bajo la premisa de que serán sometidos a las más duras condiciones de uso y desgaste. La robustez de todos sus componentes asegura un funcionamiento libre de fallas con un mínimo mantenimiento realizado.

Figura 21. Torniquetes

Fuente: http://www.dointech.com.co/control-acceso-peatonal.html

5.1.2.1 Mecanismos de registro y monitorización de la red

Para poder tener un registro en tiempo real del estado de la red, se propone usar la herramienta de software del fabricante Mikrotik, denominada DUDE server, aprovechando que el canal cuenta con un *Switch* CORE de esta misma marca. De esta herramienta se decide implementar la versión 3.5 que será posteriormente instalada en un servidor Windows server 2012 mostrando las diferentes pruebas y gráficos obtenidos con su configuración, lo anterior se podrá evidenciar en los anexos. En la Figura 22 se muestra una vista general de los equipos monitoreados dentro de la red, como son los equipos VSN, Switch, Mikrotik y otros.

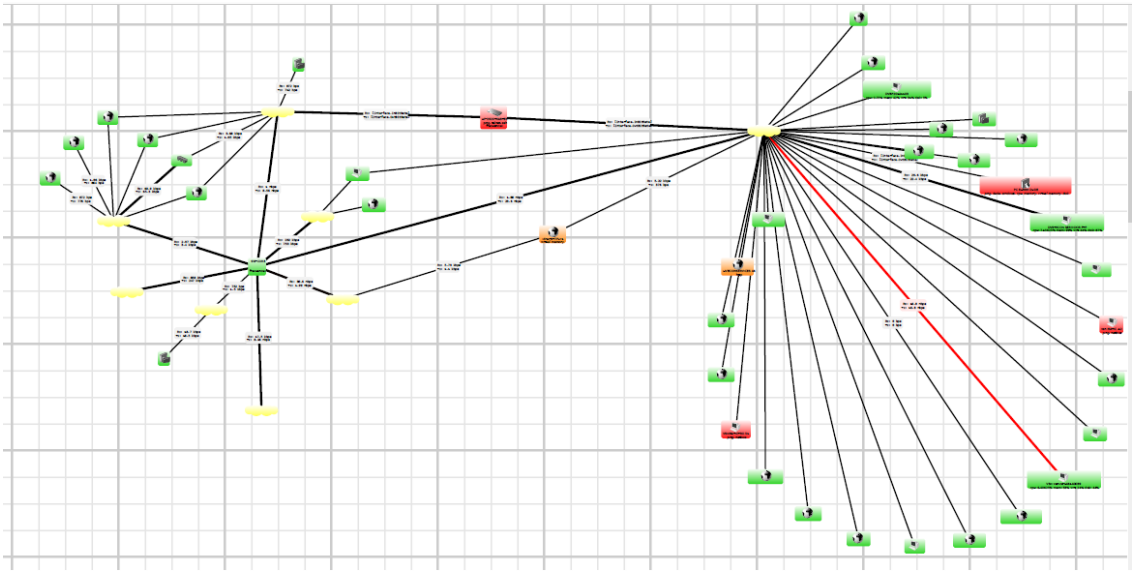


Figura 22. Vista General Dude server

Las conexiones pueden inclusive, mostrar las diferentes velocidades de conexión y servicios que son monitoreados por el dude server (ver Figura 23).

Algunas características interesantes de The Dude son:

1. Soporta autodescubrimiento de nuestra red y de su topología.
2. Es capaz de descubrir elementos de cualquier tipo o marca.
3. Incluye iconos SVG[7] para dispositivos, además de soportar iconos personalizados.
4. Permite dibujar tus propios mapas de red personalizados y añadir dispositivos.
5. Soporta SNMP, ICMP, TCP DNS y vigilancia para los dispositivos que lo soporten.
6. Permite realizar un enlace individual de seguimiento y generar gráficos asociados.

Como se puede observar, The Dude monitoriza correctamente el flujo de datos, Así mismo, se puede observar que tiene la capacidad de recolectar correctamente los datos del router Mikrotik, así como los de la red dedicada.

[7] Scalable Vector Graphics, es un formato de imágenes vectoriales basado en XML, con soporte para interactividad y animación

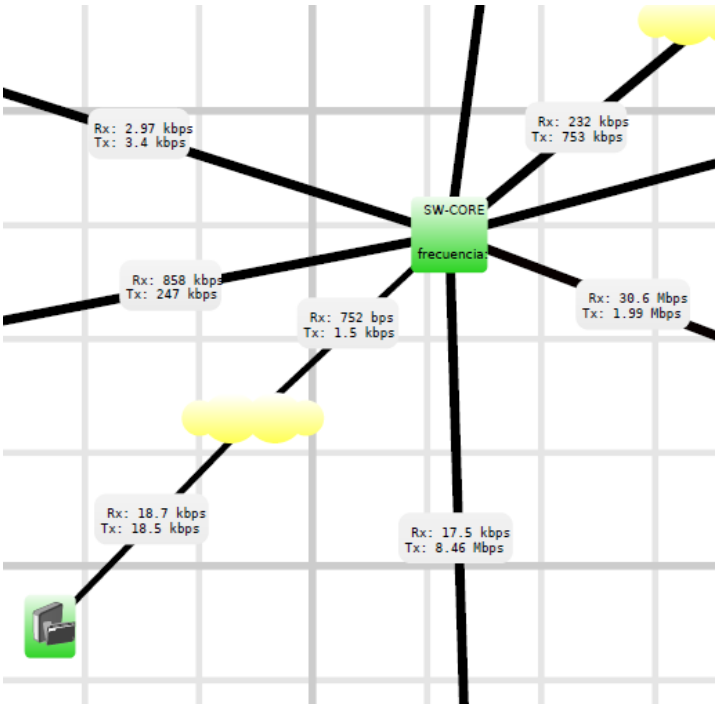


Figura 23. Velocidad de Conexión

Además, el software es capaz de sacar gráficas detalladas del tráfico entrante y saliente de cada red. En este caso se muestra la del SW-CORE. (ver Figura 24).

Como se puede observar, The Dude permite visualizar un resumen detallado del dispositivo en cuestión, mostrando los servicios de activos (SSH, Telnet, PING, HTTP y FTP) y el modelo.

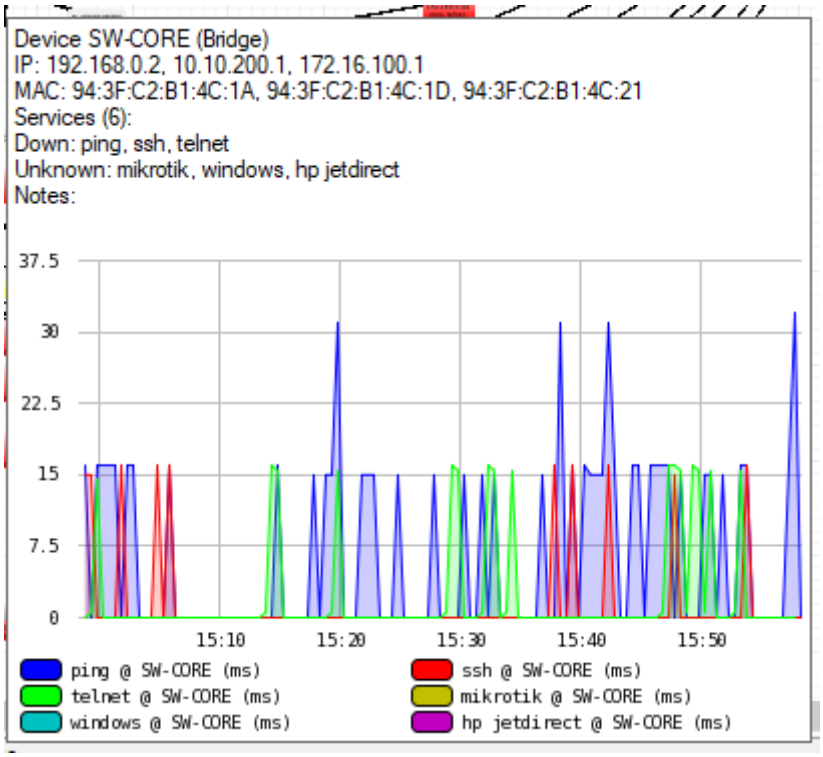


Figura 24. Tráfico en la red.

En las propiedades del dispositivo, vista general, se visualiza el nombre del dispositivo y las direcciones IP a las cuales está conectado, direcciones MAC, la versión SNMP que esta aplicado en el dispositivo (ver figura 25).

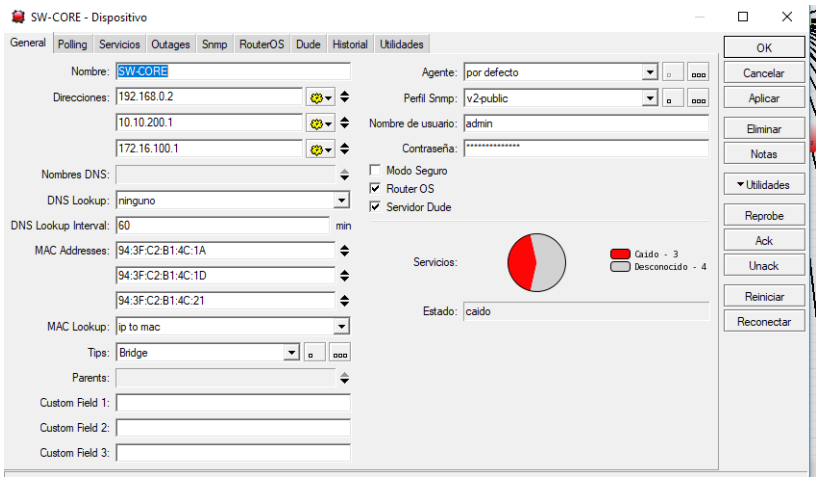


Figura 25. Propiedades dispositivo

En la vista general de la herramienta, se muestra el porcentaje de memoria, CPU, disco y otros parámetros en tiempo real, generando un reporte de eventualidades o cambios realizados en la red, agregando OID's de los dispositivos, lo que es representado como una secuencia de números que se asignan jerárquicamente y que permite identificar objetos en la red. (ver Figura 26).

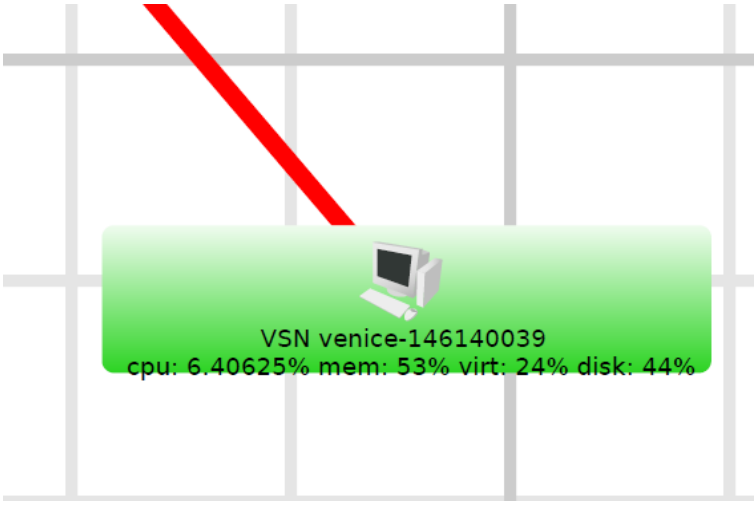


Figura 26. Capacidad en porcentaje

Se realizarán envíos de notificaciones al correo sobre cambios en el estado de los dispositivos ver (Figura 27).

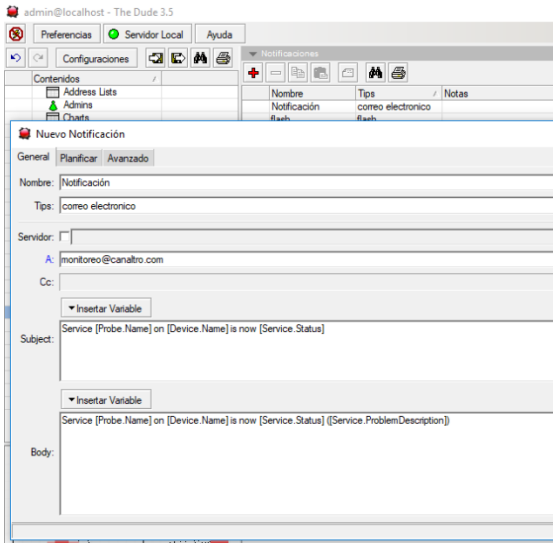


Figura 27. Notificaciones.

5.1.2.2 Sistemas de autenticación para la red.

Para el departamento de gestión de archivo, es notable destacar que éste no cuenta con un servidor de dominio que autentique los dispositivos conectados a esta red. Con base en ello, se propone la implementación de un servidor de dominio configurado en Windows server 2012, el cual, tendrá agregados los usuarios pertinentes para la autenticación. Esta configuración se encuentra detallada en la sección de anexos.

Active Directory utiliza dominios, pero en lugar de mantener cada dominio independiente, se pueden incluir varios dominios en un AD "bosque" (ver figura 28). Esto hace que toda la red esté bajo el control de un solo dominio que supervisa los

otros. El AD le permite al administrador de un bosque que administre múltiples dominios, reduciendo el costo y la complejidad, al tiempo que proporciona una mayor seguridad. Esto también puede ayudar a reducir el número de servidores de controlador de dominio en la organización.

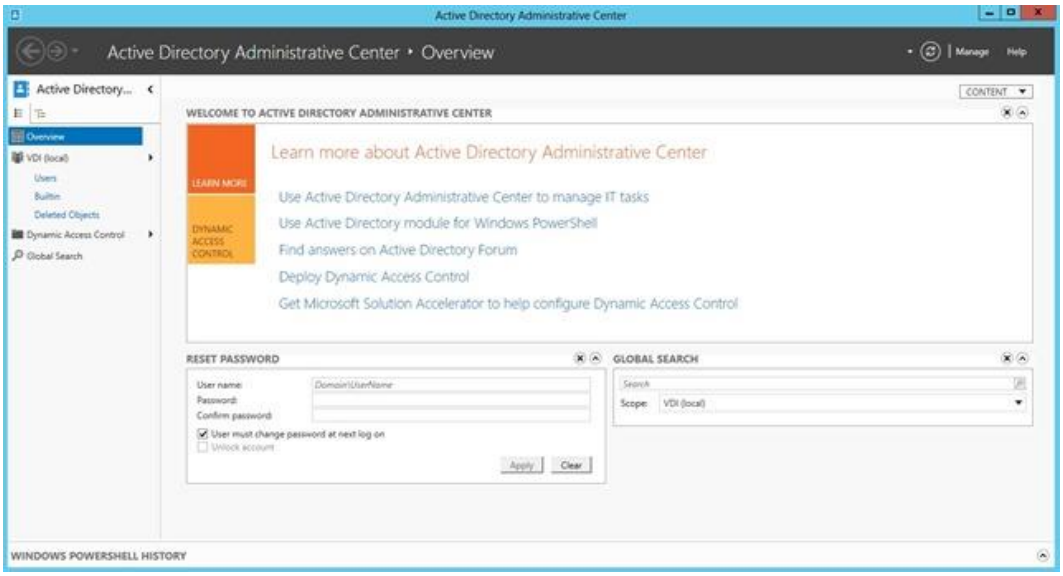


Figura 28. Active Directory

Se agrega un grupo al dominio que contendrá a todos los usuarios que podrán registrarse. (ver Figura 29), los grupos de Microsoft Active Directory son contenedores con otros objetos dentro de ellos como miembros. Estos objetos pueden ser objetos de usuario, otros objetos de grupo, como anidamiento de grupo, y otros, como sistemas un poco más complejos. El tipo de grupo determina el tipo de tarea que gestiona, así mismo, el ámbito de grupo determina si el grupo puede tener miembros de varios dominios o de solo uno. En resumen:

Los grupos suelen ser un conjunto de cuentas de usuario.

Los miembros reciben el permiso otorgado a los grupos.

Los usuarios pueden ser miembros de varios grupos.

Los grupos pueden ser miembros de otros grupos, que son grupos anidados.

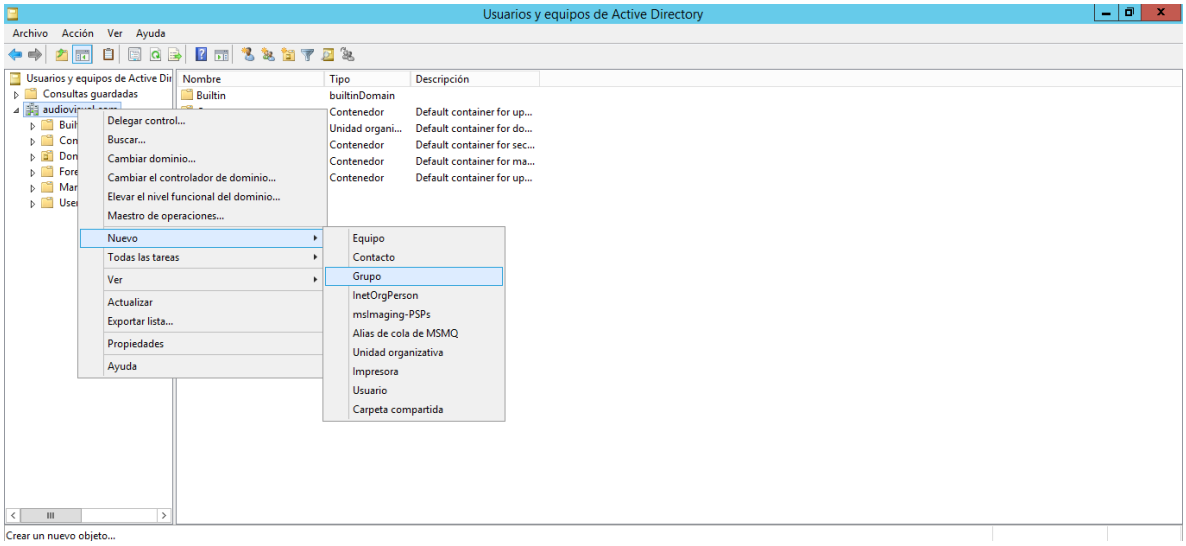


Figura 29. Grupo de dominio

Luego de poseer los grupos gestionados, se procede a la creación del usuario con su respectiva contraseña que luego será agregado a un grupo de dominio. (ver Figura 30)

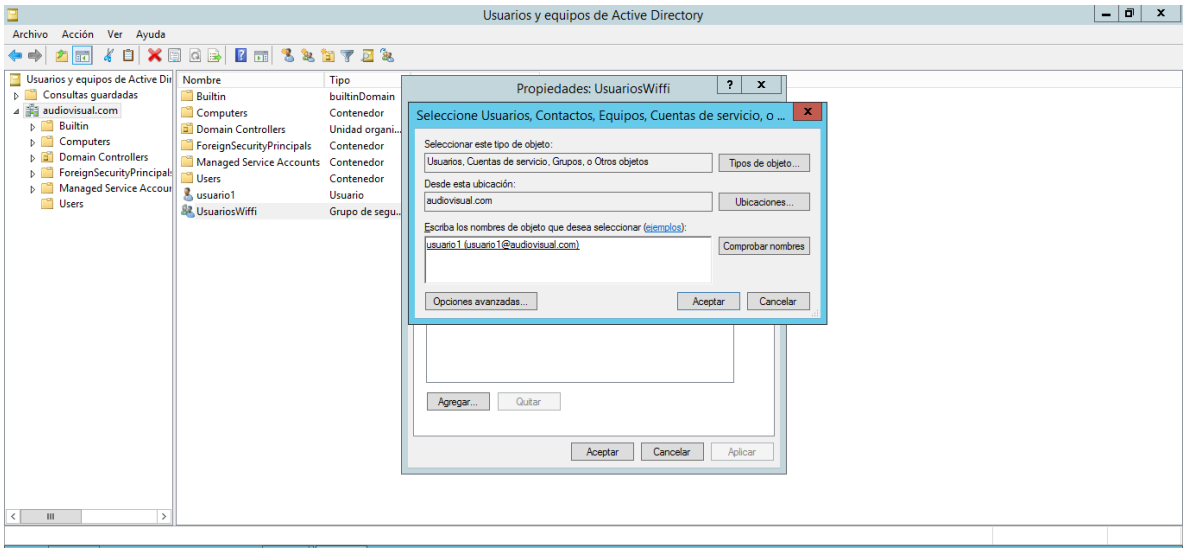


Figura 30. Nuevo usuario

Acto seguido, se proceden a realizar los cambios en la configuración del equipo usuario conectándolo a la red de dominio a la que ha sido agregado con anterioridad, como se observa en la figura 31.

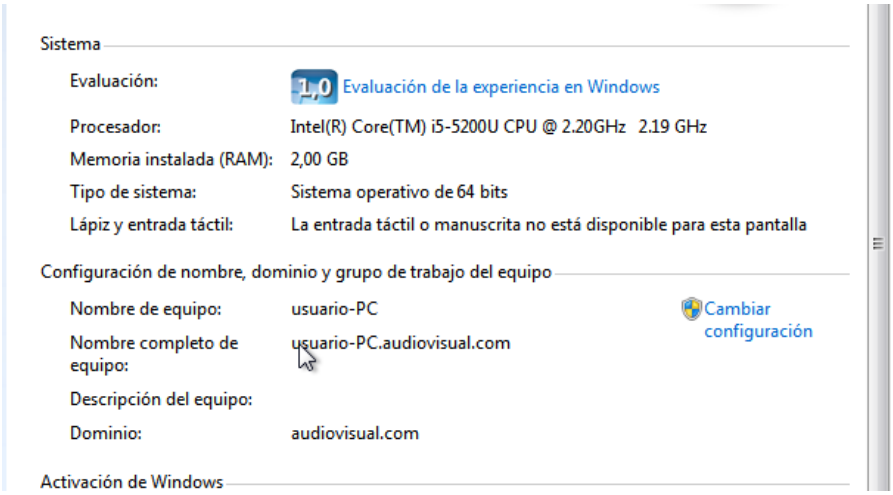


Figura 31. Configuración usuario

5.1.3 Selección de recomendaciones para la Seguridad de los servicios de red

Al realizar auditorías de los servicios de red, se efectúan solicitudes externas esporádicamente ya que solo se realizan cuando se presenta un error grave, que impida el funcionamiento normal del servicio de Internet.

Se recomienda una política de auditoria para la red física orientada a conocer y evaluar los mecanismos de protección del hardware y del cableado, y revisiones lógicas que tienen como propósito contribuir a la verificación y evaluación de las medidas de protección sobre la información y los procesos de la red en general.

Considerar la revisión de las conexiones y su apego a las normas de cableado estructurado establecidas por organismos como ANSI o ISO, así como medidas que protejan tanto el cableado como los dispositivos de red, incluyendo controles aplicados sobre los cuartos de servidores (*sites*).

En las evaluaciones lógicas realizar la revisión continua de los mecanismos de control de acceso a la red, privilegios de cuentas con autorización para conexiones o los protocolos que se utiliza.

5.1.4 Políticas y procedimientos de intercambio de información.

En el Canal TRO, no se aplican de manera adecuada las políticas de concientización, capacitación y cumplimiento de las labores de administración de la red y los activos, lo que conlleva a que algunos activos como los dispositivos externos sean erróneamente empleados por parte del personal encargado.

Para ello se recomienda una capacitación al recurso humano para la concientización y capacitación en el uso adecuado de los equipos, estas serían unas pautas:

Seguridad del intercambio de información unida a los recursos humanos.

1. Antes de la contratación asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
2. Investigación de antecedentes, para ejercer mayor control sobre los nuevos empleados que ingresen a la Entidad.
3. Consolidar de manera más afinada los términos y condiciones de contratación, especificando las responsabilidades y los cuidados que deben tener con la información de la Entidad.
4. Durante la contratación, se debería concientizar a los empleados y contratistas acerca de las responsabilidades que, como deber, poseen enmarcado siempre en la seguridad de la información y hacerlo cumplir.
5. Responsabilizar a los gestores, proporcionando los mecanismos necesarios para asegurar que los mismos, cumplan con sus obligaciones en temas de seguridad de la información desde su ingreso hasta su retiro.
6. Establecer procesos de concientización, educación y capacitación en seguridad de la información, la Entidad debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros, formándolos de manera continua mediante actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
7. Proceso disciplinario, las Políticas de Seguridad de la Información con sus respectivas normas, estándares, procedimientos y demás documentos que se generen y soporten el Sistema de gestión de Seguridad de la Información son de obligatorio cumplimiento. La ejecución de acciones que atenten contra la confidencialidad, disponibilidad, integridad y privacidad de la información

deberá desembocar en una acción disciplinaria que puede incluso acarrear la terminación del contrato de trabajo, y al posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen al caso.

5.1.5 Acuerdos de intercambio de información.

El canal TRO no cuenta con protocolos de aseguramiento por medio de firmas digitales ya que su costo es muy elevado, la firma digital se presenta como una solución para las políticas de seguridad en las redes, específicamente en lo que se refiere a la autenticación. El mecanismo más utilizado hoy en día en Internet (por su simplicidad) es el de nombre de usuario, contraseña. Es claro entonces establecer que, mucho más factible es una combinación de esto último aunado con el empleo de una firma digital, por lo que a corto plazo las firmas digitales y los servicios de certificación se generalizarán con rapidez.

Un sistema de firma digital segura consta de dos partes: un método para firmar un documento de modo infalsificable; y otro para verificar que la firma ha sido generada por la persona a quien representa. Los protocolos de autenticación pueden estar basados en sistemas de encriptación de tipo simétrico o asimétrico. La autenticación y la integridad se salvaguardan con sistemas asimétricos de dos claves denominados generalmente sistemas de clave pública.

Las firmas digitales con criptografía de clave pública tienen una amplia variedad de aplicaciones como:

- Firmas digitales usadas para comunicaciones oficiales entre instituciones públicas (documentos de identidad, declaraciones fiscales, transmisión de documentos legales, etc.).
- Firmas digitales empleadas para relaciones contractuales en redes abiertas (compraventa electrónica, transacciones financieras).

- Firmas digitales estructuradas para identificar o autorizar propósitos (tener certeza de la identidad de una persona autorizada o de sus atributos específicos, p. ej. Una autorización para acceder a un sistema informático, identificación de servidores web, etc.).
- Firmas digitales para sistemas cerrados (p. ej. intranet corporativa).
- Firmas digitales para propósitos personales.

5.2 Dude Server instalación

1. Procedemos a descargar The Dude de http://download.mikrotik.com/dudeinstall-3.5.exe.
2. Procedemos a abrir el Dude.
3. Seleccionamos el idioma de nuestra preferencia (Si se equivocan, se puede cambiar posteriormente en el menú preferencias)
4. Posteriormente nos saldrá una interfaz similar a la de Winbox (Ver Figura 32), el servidor que usaremos para el caso será nuestra propia maquina (localhost) y el password en blanco, posteriormente podremos modificarlo en el menú admins.

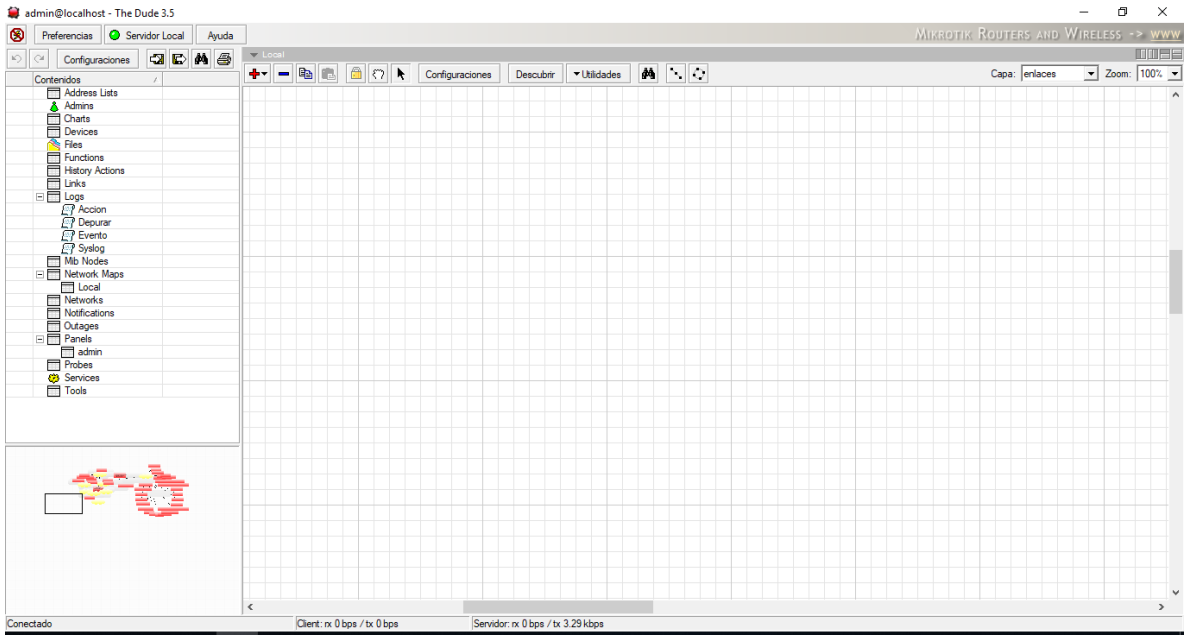
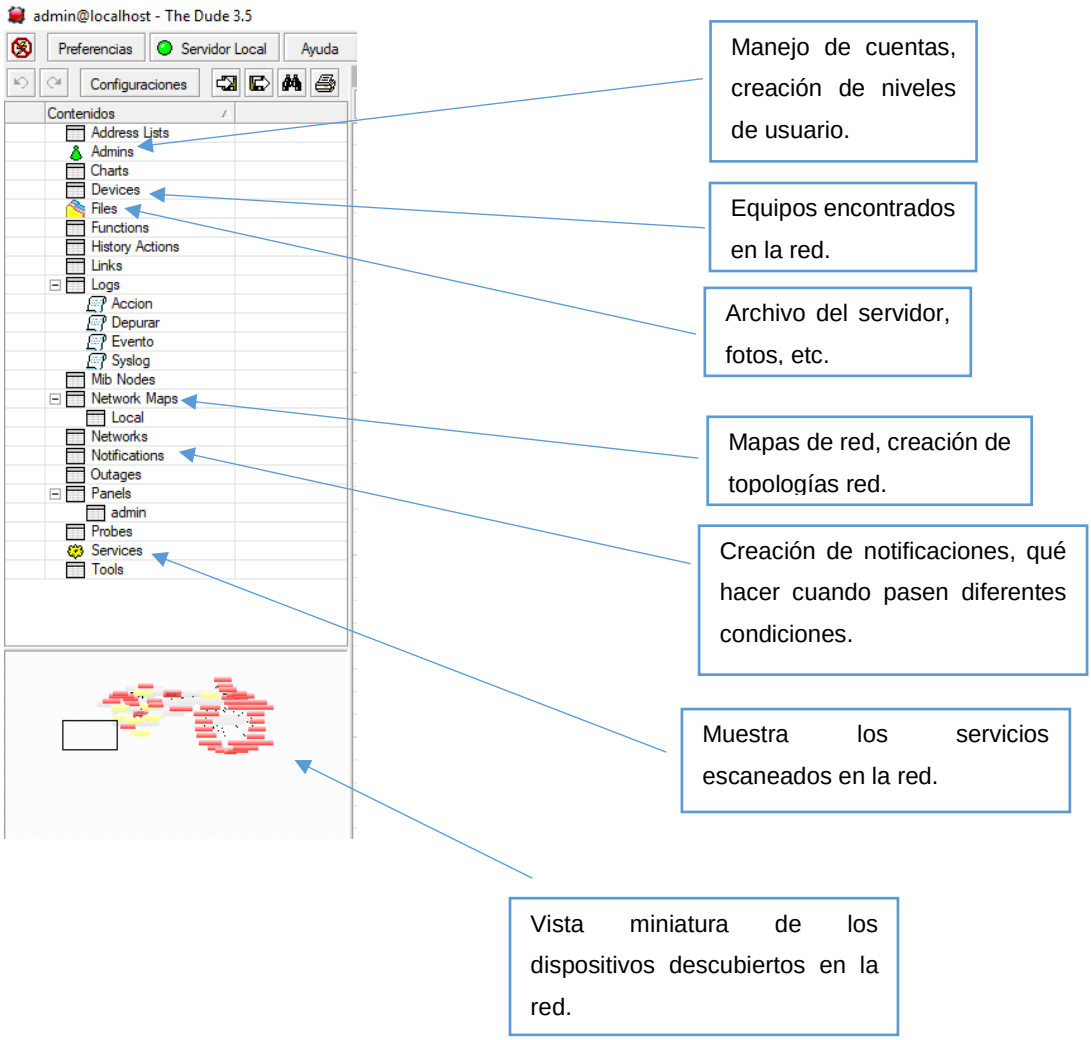


Figura 32. Vista general Dude server

5. Una vez logueados tenemos la siguiente interfaz (solo se nombrará los servicios que posiblemente se usaran).



6. Procedemos a hacer nuestra topología de red como y descubrir las interfaces existentes, asignándole que red es la que deseamos escanear y el agente que lo hará (lo normal es el por defecto y el agente a elegir seremos nosotros por defecto). Dejamos las demás opciones por defecto para un escaneo rápido, en la pestaña servicio, podemos asignar los servicios que se desean escanear, como es el primer escaneo lo dejamos así por defecto (ver Figura 33).

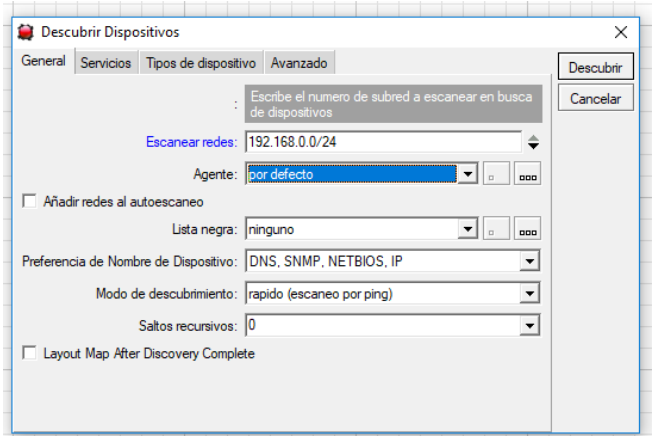


Figura 33. Descubrir dispositivos

7. Como resultado obtenemos los elementos de red que escaneamos, totalmente desordenados y adyacentes a una nube perteneciente al segmento de red(ver Figura 34).

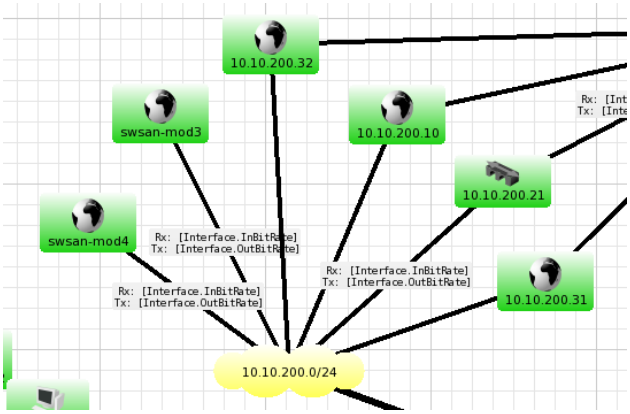


Figura 34. Segmento de red

8. Una vez terminado la autentificación de red, se procede a darle forma a la red que se puede describir como asignar los respectivos enlaces entre cada interfaz (Fast Ethernet, wireless, etc), y ligarlos a una interfaz del equipo routeros o cualquier equipo que posea snmp. Para esto se regresa al mapa de red y se

hace clic derecho sobre cualquier espacio blanco y seleccionamos añadir nuevo enlace. Y al terminar de ordenar podemos obtener algo similar a esto (ver Figura 35), donde se puede obtener datos del equipo o enlace con solo pasar por encima de él (ver Figura 36).

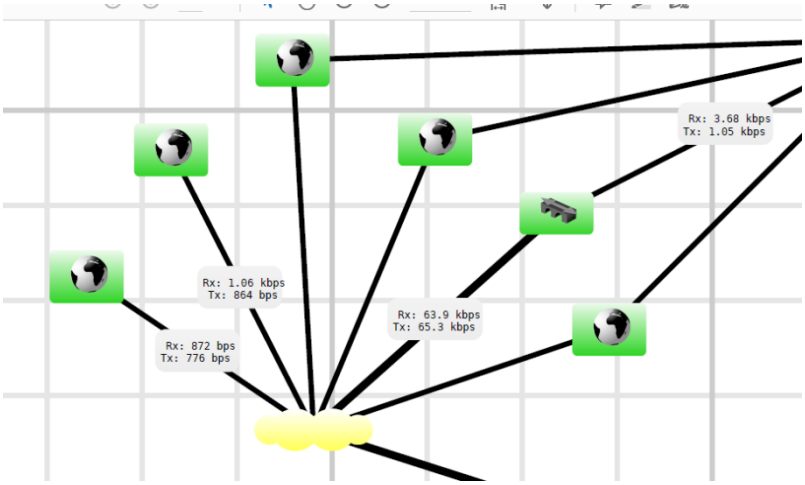


Figura 35. Conexiones de red

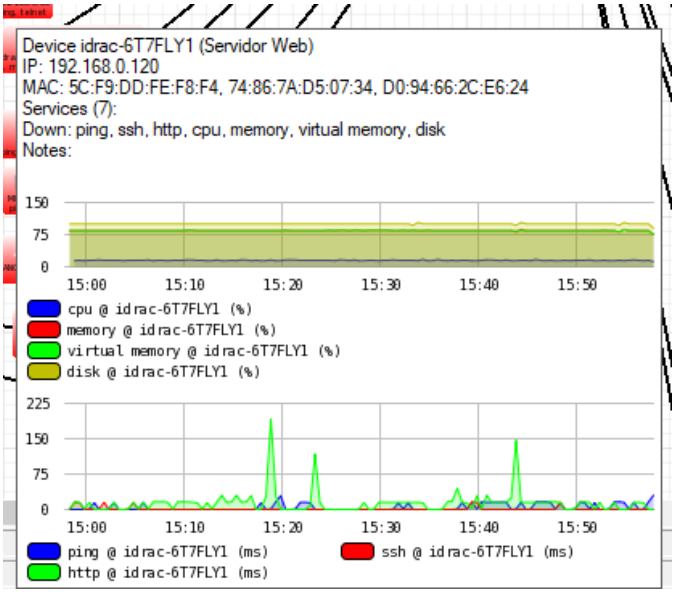


Figura 36. Reportes de funcionamiento

5.3 Instalación Servidor de Dominio.

En el servidor Windows server 2012, ejecutamos el asistente de roles y características, y agregamos las herramientas de acceso y directivas de redes como también las herramientas de actividades de Active Directory. (ver Figura 37), en Active Directory el bosque (forest) es una colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración.

Todos los dominios del bosque cuentan con relaciones de confianza automáticas de 2 vías y transitivas, el bosque representa una instancia completa del directorio y una frontera de seguridad.

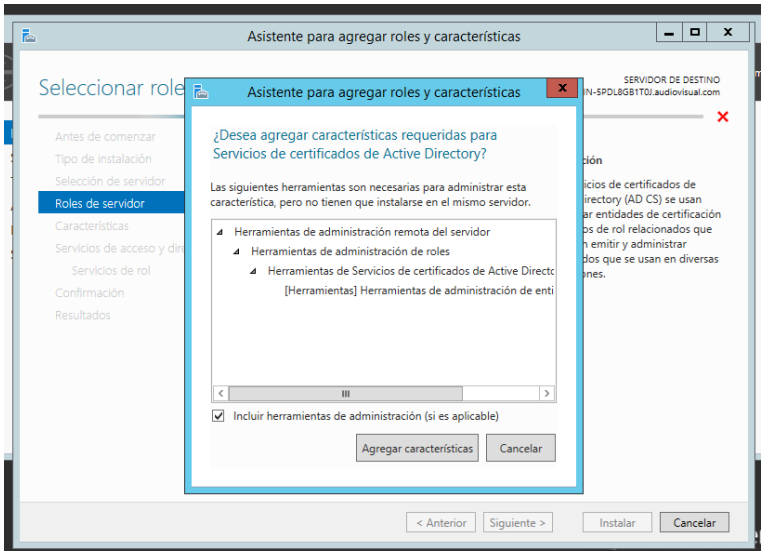


Figura 37. Roles y características

Agregamos un nuevo bosque a nuestro servidor que se llamara audiovisual.com, previamente instalado el servicio de DNS.

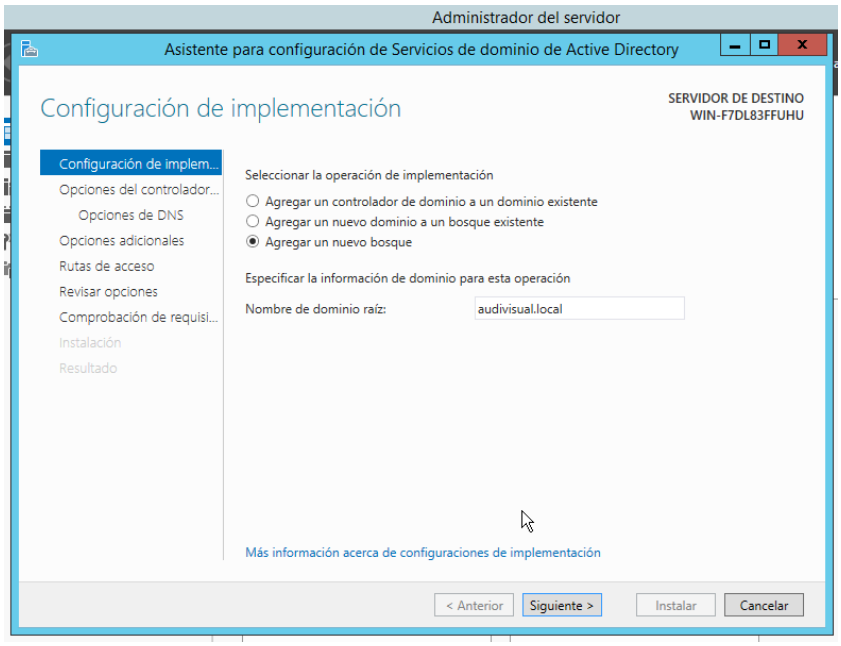


Figura 38. Nuevo bosque

Se asigna un nombre NetBios, que se llamara igual que el dominio.

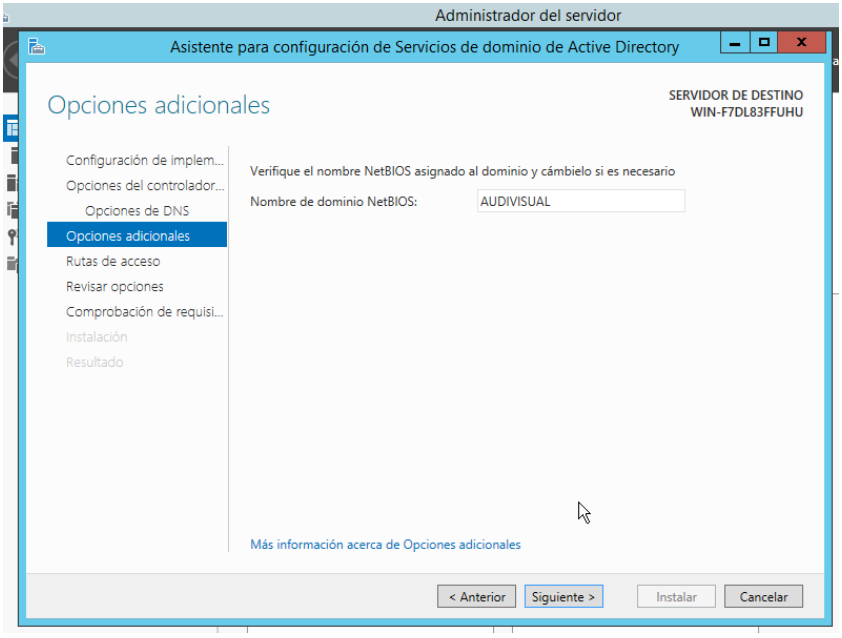


Figura 39. Dominio NetBIOS

Se verifica la configuración.

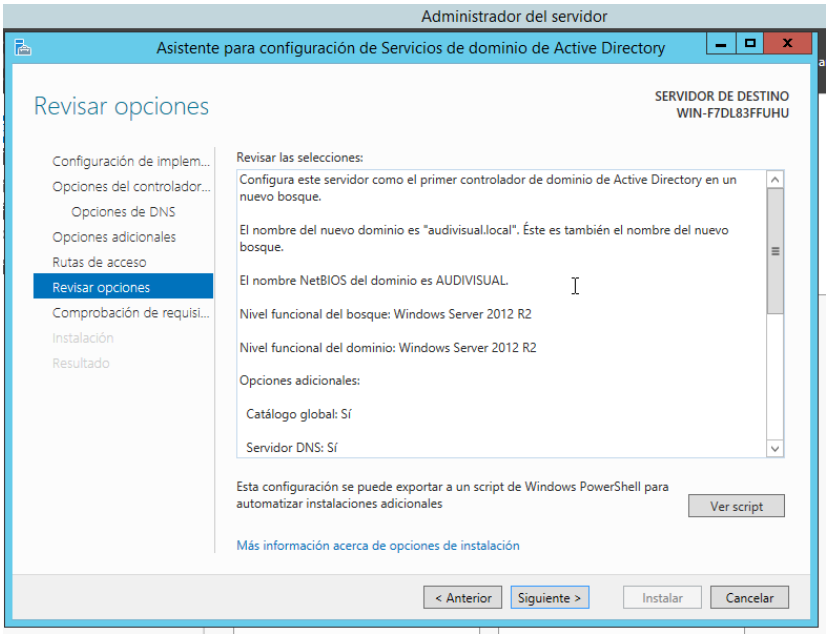


Figura 40. Revisión de Opciones

Verificamos que la administración de directivas de grupo este instalado. Posteriormente, asignamos un IP estática a nuestro servidor que permita la autenticación del servidor.

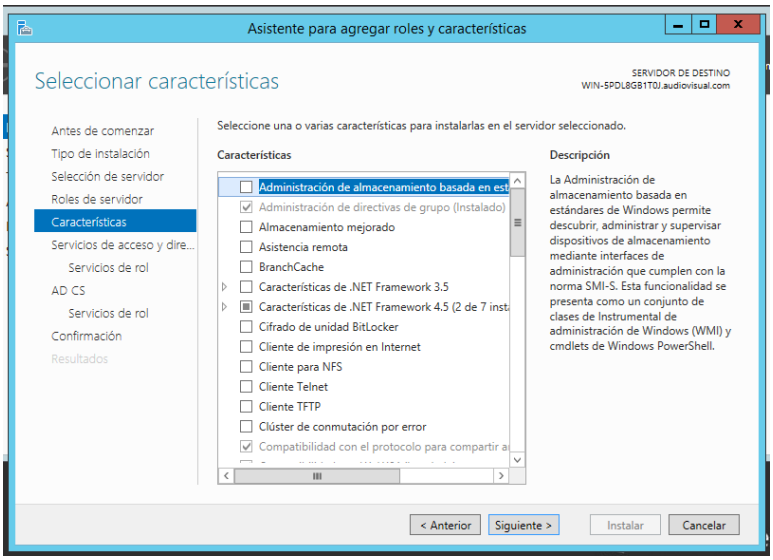


Figura 41. Características servidor

Verificamos que el proceso de instalación de las características instaladas.

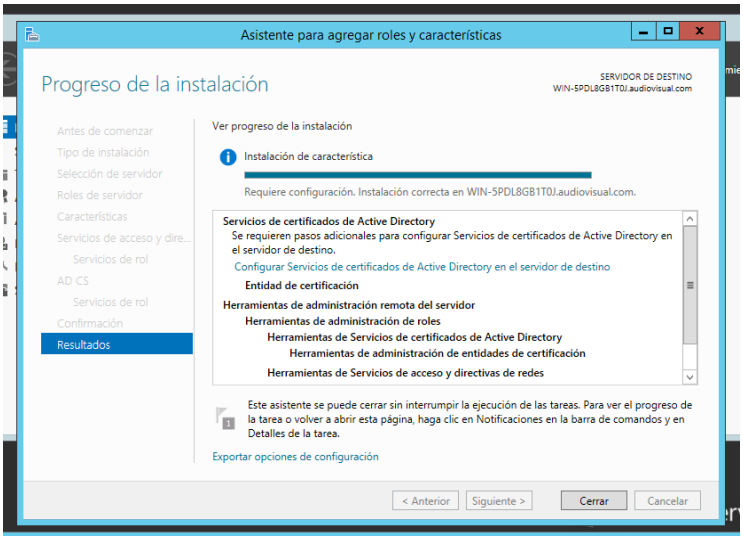


Figura 42. Proceso de Instalación

Ingresamos a herramientas/usuarios y equipos Active Directory, creamos un grupo y asignamos usuarios a ese grupo, que serán los que se autentiquen en ese dominio.

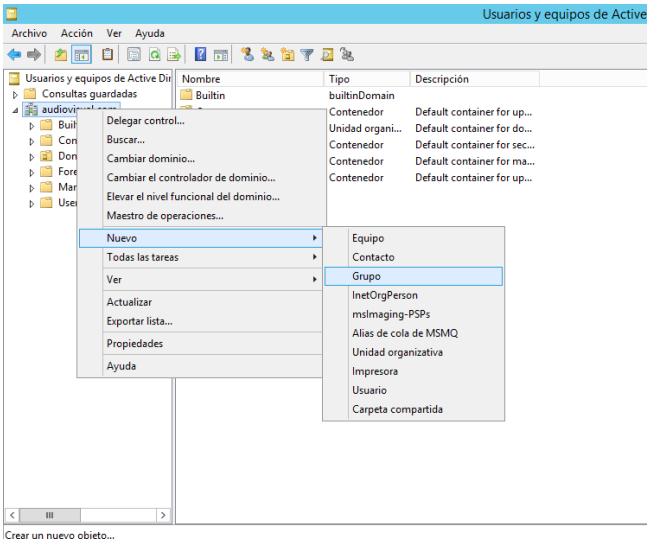


Figura 43. Usuarios de equipos de active.

Registrar un NPS en el dominio.

En el NPS, en el Administrador del servidor, haga clic en Herramientas y luego en Servidor de políticas de red. Se abre la consola del Servidor de políticas de red. El NPS nos permite configurar las políticas de acceso de redes, dichas políticas pueden estar relacionadas con accesos remotos, como las VPN o estar relacionadas con la salud del cliente que es cuando entra en juego el NAP, inclusive podemos configurar el NPS para que nos brinde un funcionamiento de RADIUS PROXY que permita redireccionar la petición a otro servidor que se encargue de autorizar o negar el acceso al recurso de red solicitado.

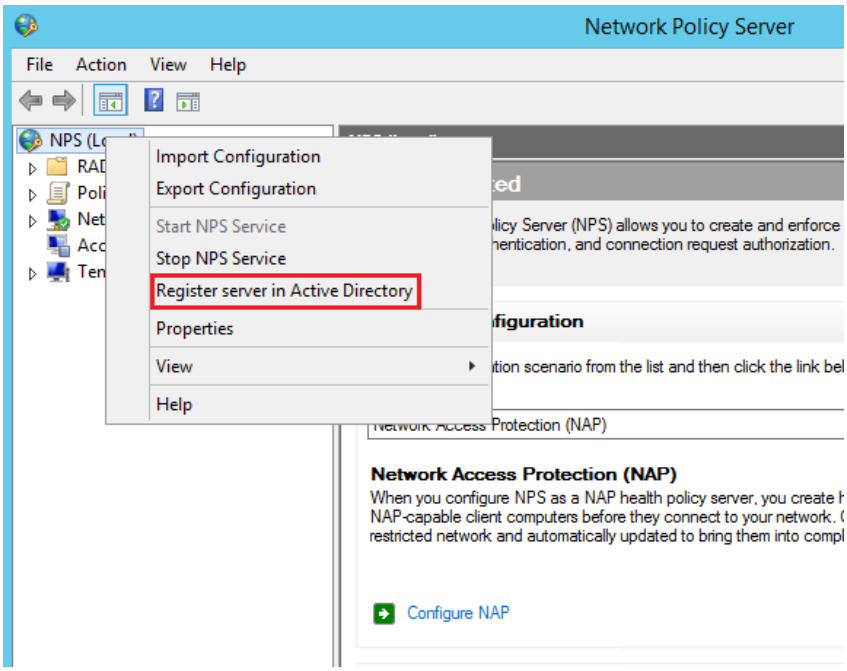


Figura 44. Registrar NPS

Haga clic con el botón derecho en NPS (Local) y luego haga clic en Registrar servidor en Active Directory. Se abrirá el cuadro de diálogo Servidor de políticas de red, En el Servidor de políticas de red, haga clic en Aceptar y, a continuación, vuelva a hacer clic en Aceptar.

5.4 Configuración protocolo RADIUS.

Anteriormente en el servidor se instalaron y configuraron los servicios los AD y servicios de dominio la configuración de los grupos y usuarios.

Se añadió el rol de NPS y ADCS (Active Directory Certiificate Services)

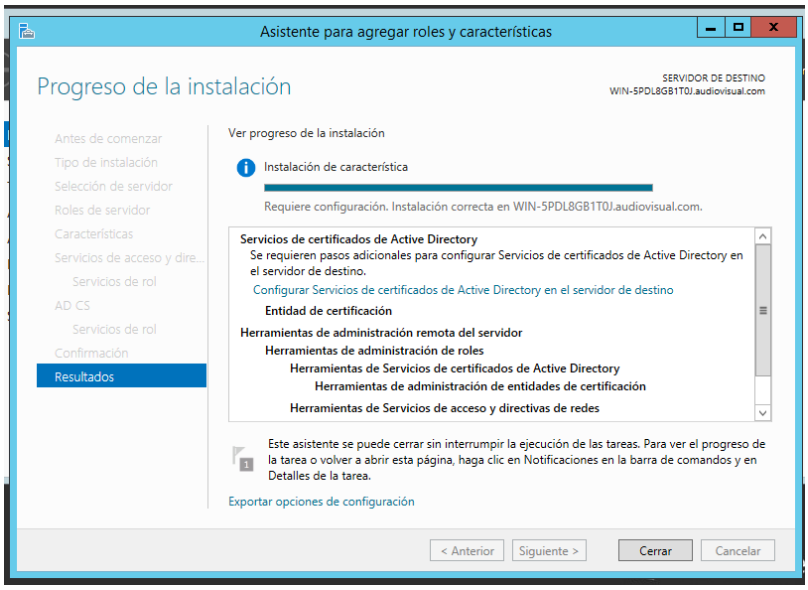


Figura 45. Añadiendo roles.

Se configura los servicios de certificados y se crean, se configura NPS.

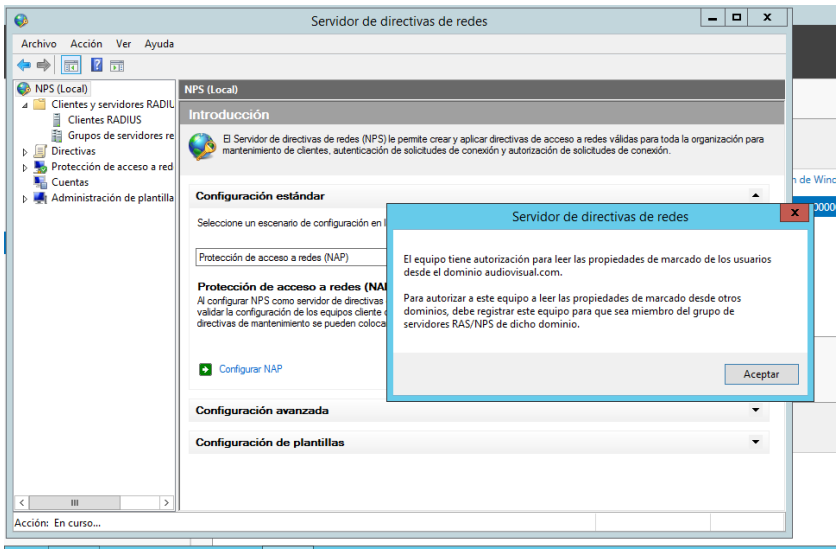


Figura 46. Activación NPS

Definimos el tipo de autenticación Cert, EAP, PEAP.

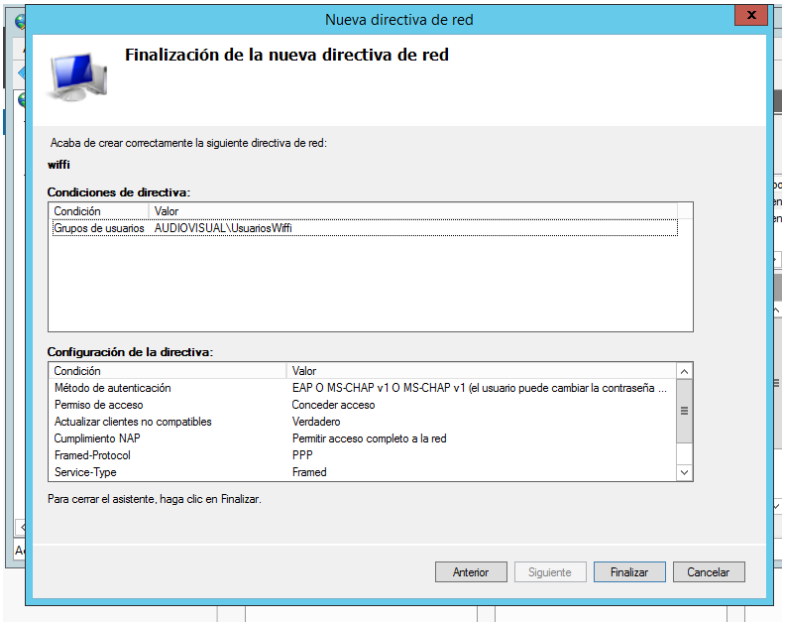


Figura 47. Nueva directiva de red

Especificar grupos de acceso a la red Wireless, son los usuarios que se podrán conectar al servidor de dominio.

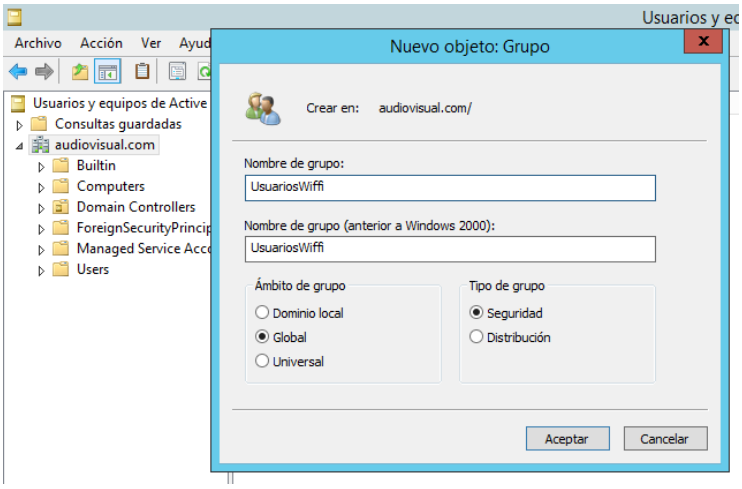


Figura 48. Creacion grupos de usuario.

Se especifican los grupos de usuarios y el grupo al que pertenecerán.

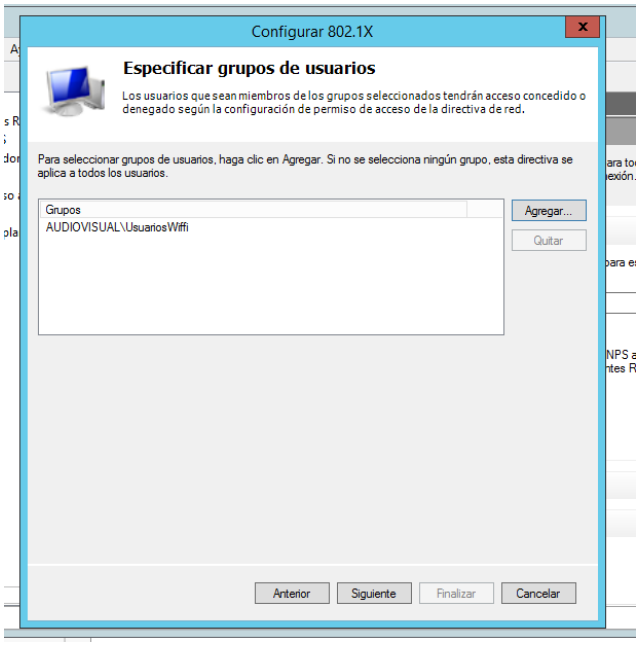


Figura 49. Especificar grupo de usuarios.

5.4.1 Configuración Mikrotik AP.

Previo al inicio de la configuración debemos tener:

• Crear una interface bridge en el router que serán los puertos del mikrotik que estará en el rango de Ip, donde encuentra el servidor.

• Asignarle una dirección IP a la interface bridge creada, en este caso sería la 192.168.10.15.

• Crear un DHCP Server en la interface bridge, donde se encuentra las conexiones ethernet y las conexiones Wlan inalámbrica.

Creamos un perfil de seguridad para el uso en la interface bridge, donde solo se señalará la seguridad WPA2 EAP.

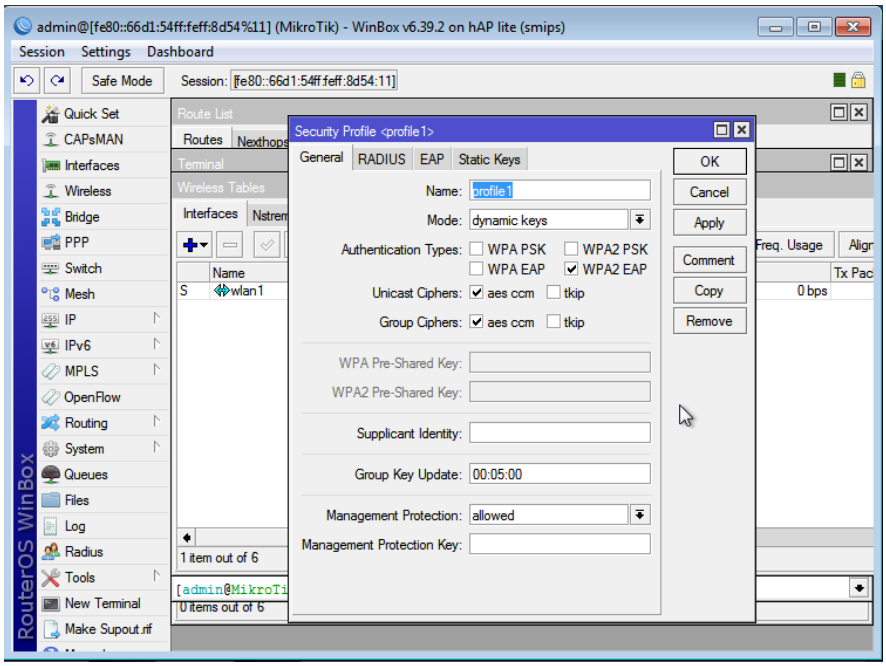


Figura 50. Perfil de seguridad.

En la pestaña RADIUS del perfil de seguridad, seleccionamos la opción EAP accounting

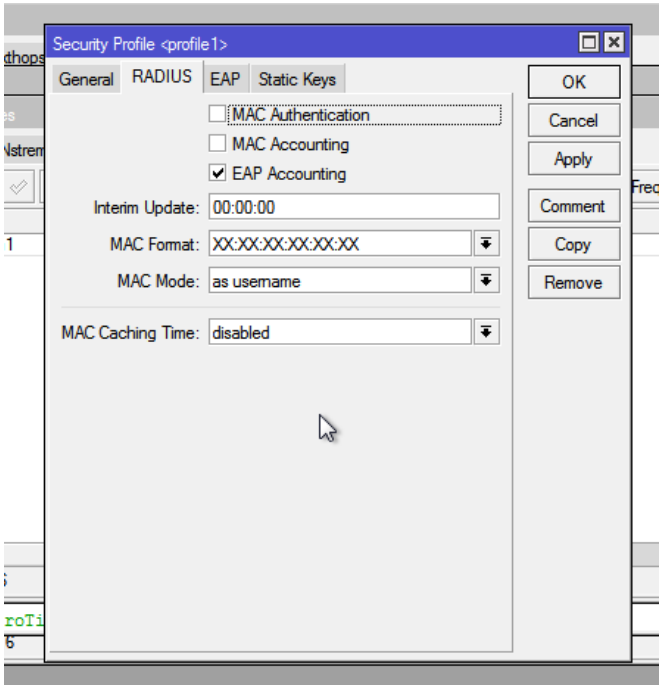


Figura 51. Pestaña RADIUS.

En la pestaña EAP/EAP Methods seleccionamos la opción passthrough que permite habilitar todos los métodos de autenticación que solicite y le damos ok.

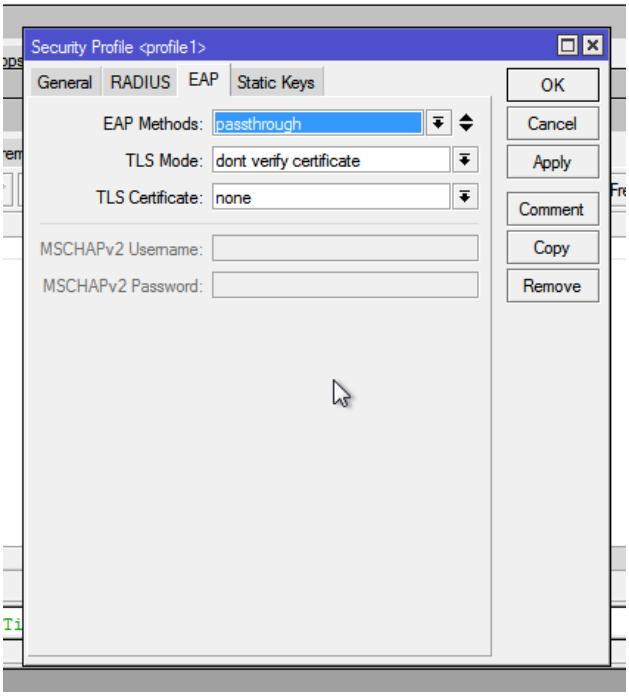


Figura 52. pestaña EAP.

En la configuración de la wlan, en la pestaña wireless, seleccionamos el modo ap bridge, modificamos el SSID al nombre que queramos de nuestra Wlan y en Security Profile seleccionamos el perfil de seguridad antes configurado.

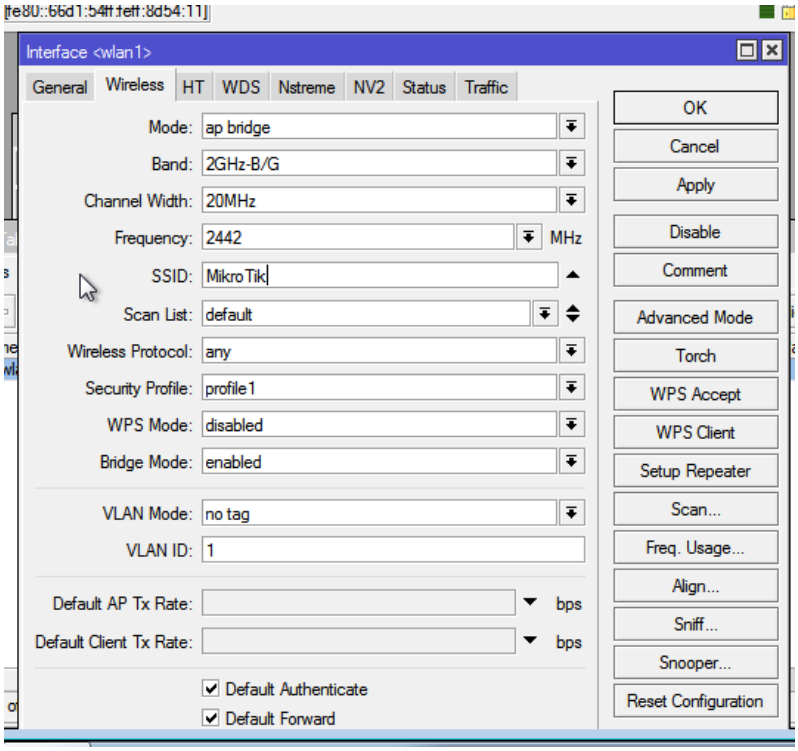


Figura 53. Interface wlan

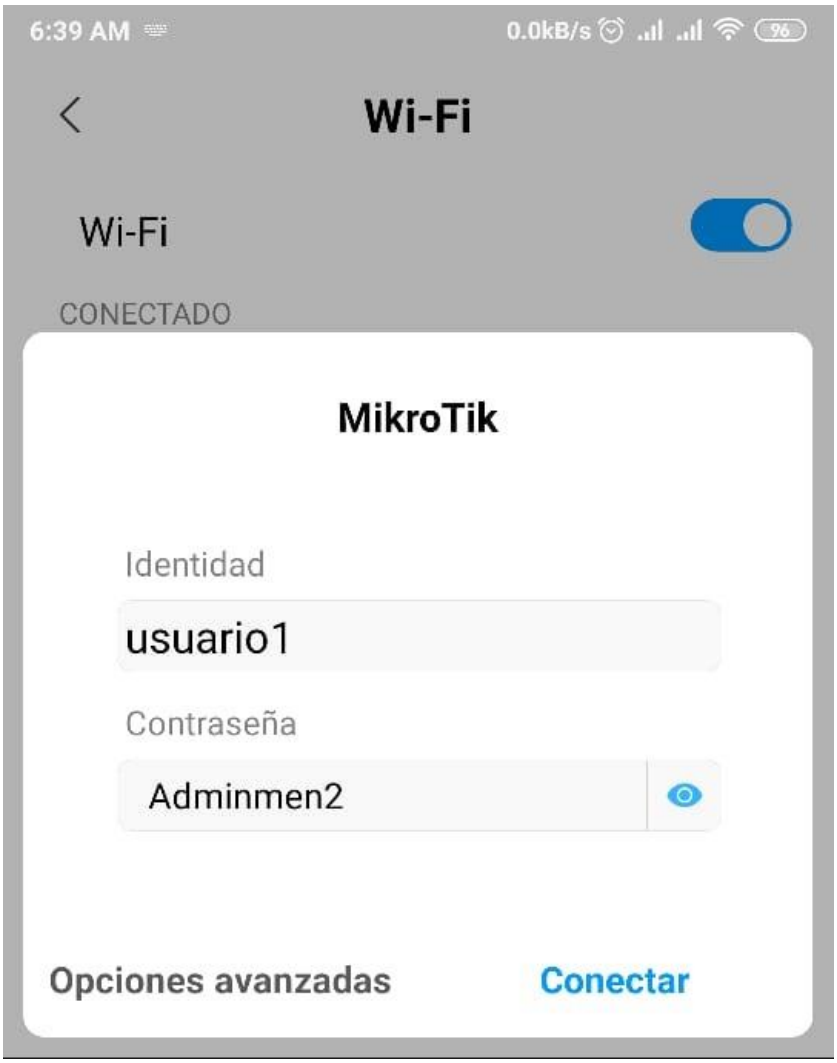


Figura 54. Solicitud de conexión a la red Mikrotik.

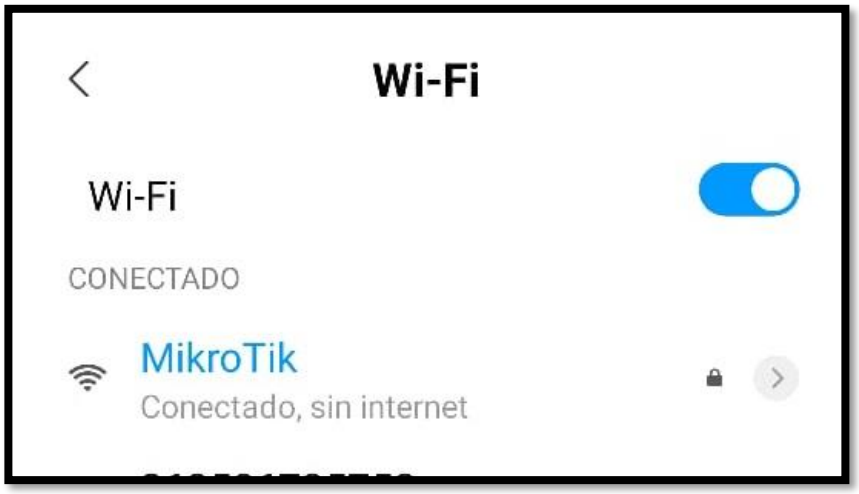


Figura 55. Conexión Exitosa.

Capítulo 6

Conclusiones y Recomendaciones

6.1 Conclusiones

- La norma ISO/IEC 27001 aporta una visión amplia referente a la valoración de riesgos y su apropiado tratamiento, sin importar la naturaleza de las organizaciones, pues se encuentran generalizadas bajo lineamientos estrictos que se ajustan a cualquier organización con el ánimo de presentar la posibilidad de establecer un SGSI adecuado. Los procesos de control y gestión de sistemas de información son de vital importancia para cada una de las organizaciones que pretendan establecer un modelo de gestión, definir el monitoreo de su SGSI y los controles que se van a utilizar, de esa manera fortalece los controles de todo el sistema.
- Es necesario comprender que los procesos de auditoría por sí solos no son la solución de los problemas de ataques informáticos, más bien, son una herramienta que nos proporcionan la información suficiente para determinar si en algún caso ha habido algún tipo de ataque cuyo objetivo ha sido la vulneración de la información, como se muestra en este caso. Ahora bien, si se fusiona el proceso de auditar con un conjunto de herramientas que contribuyan al proceso de identificación de la vulnerabilidad, se podría establecer un sistema mucho más sólido, para identificar la amenaza, con sus causas y consecuencias, y así, finalmente poder contrarrestar el proceso, asegurando de una u otra manera la metodología de salvaguarda de todo el

sistema, soportado bajo los lineamientos del manual de análisis de riesgos y vulnerabilidades en organizaciones de la metodología MAGERIT V3.

- Una vez analizados todos los parámetros vulnerables en la red de TRO, se establecieron varios mecanismos de salvaguarda, con la finalidad de proveer un estatus de seguridad mucho más robusto. De lo anterior se puede destacar el empleo de un servidor de dominio AD, que trajo consigo diversos beneficios, como lo es la centralización de todos los dominios de la red dispuestos en árbol, con la finalidad de disminuir la cantidad de administradores de los diferentes puntos de la red del canal y a su vez, ejercer control sobre las conexiones de los usuarios a las redes inalámbricas, gestionando así, dominios para visitantes separados de los usuarios frecuentes y constantes del canal. Por otro lado, se emplea un sistema de control de acceso a las entradas de TRO, soportado en un sistema biométrico con acceso por torniquete; cabe aclarar que, la disposición de esta tecnología surge por dos razones principales, la primera radica en la eficiencia en las prestaciones que puede proveer luego de su instalación, aunado a que las capacitaciones del personal para su uso apropiado no requieren de un desgaste muy grande, lo que genera una reducción de costos a la hora de capacitar a los usuarios de control. Finalmente, para poder abarcar todos los activos de la red, para su gestión, se valida de manera virtual la factibilidad del empleo de herramientas como DUDE server y protocolos de SNMP, aprovechando la tecnología Mikrotik que posee TRO, como una forma general de controlar y monitorear todo el tráfico circundante.

6.2 Recomendaciones

El canal está avanzando en el proceso de seguridad de las comunicaciones tomando un proceso de concientización, empleando las acciones preventivas adecuadas según las prioridades existentes y siempre soportado en lo expuesto en este documento. Para ello se sugiere que:

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con los servicios de tecnología de información y comunicación.

Los directores deben revisar con regularidad el cumplimiento de los procesos y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de las comunicaciones.

Se recomienda expresamente la implementación del servidor de dominios, puesto que durante las simulaciones de software se obtuvo excelentes resultados a nivel de segmentación de la red, así como el monitoreo de los usuarios conectados y el tráfico mediante la herramienta SNMP

Como punto final, se aconseja realizar capacitaciones constantes y jornadas de sensibilización a todos los empleados del canal, como método persuasivo para fortalecer la cultura de la seguridad de la información y el buen uso de los activos, esta estrategia puede fomentar la preservación de los pilares de la seguridad de la información y así disminuir el riesgo que representa el factor humano.

ANEXOS.

7.1 Entrevista.

Preguntas realizadas al encargado de la red basados en el documento Excel, sobre auditoría interna sobre una SGSI.

1. ¿Existen políticas de redes físicas e inalámbricas?

Si, Anexos en los documentos (formatos) entregados a los encargados de la red y gestión técnica.

2. ¿Existe una separación de la administración de las operaciones de sistemas y la de infraestructuras de red?

No hay. Todo lo maneja el departamento del área técnica.

3. ¿Existe un mecanismo de registro y monitorización de la red y los dispositivos que se conectan ella?

No. Solo cuenta con un monitoreo del equipo VSN básico, consola de winbox.

4. ¿Hay un sistema de autenticación para todos los accesos a la red de la organización?

Se encuentra parcialmente, ya que el servidor de dominio se eliminó por falta de capacitación de los encargados.

5. ¿El sistema limita el acceso de personas autorizadas a aplicaciones / servicios legítimos?

Si limitados.

6. ¿Los usuarios se autentican adecuadamente al inicio de sesión?

SI, a través de un usuario local en cada equipo.

7. ¿Cómo se autentican los dispositivos de red?

De forma remota o por consola. (ssh, telnet, rdp, rdpx, https).

8. ¿Existe una segmentación de red adecuada usando cortafuegos, VLAN, VPN, etc.?

Si. No se pudo obtener datos (Documentos, gráficos) sobre su configuración.

9. ¿Se controlan los puertos y servicios utilizados para funciones de administración de sistemas?

Si, recientemente se bloquearon puertos que se evidenciaron que no se usaban y que podían ocasionar peligro.

1 ¿Se gestionan, clasifican y protegen los servicios de red de forma adecuada?

si

2 ¿Existe un monitoreo de servicios de red?

Si, a través de winbox.

3 ¿Se mantiene un derecho a auditar servicios de red gestionados por terceros (contratos, SLA y requisitos de informes de gestión)?

Si internamente, se hace solicitudes externas a los proveedores de Internet, esporádicamente.

4 ¿Se emplean mecanismos de autenticación en la red, cifrado de tráfico de red?

Si, para la transferencia de datos por túnel VPN, con la sede de Cúcuta.

5 ¿Se hace una revisión periódica de las configuraciones de cortafuegos, IDS (sistema de detección de intrusos) / IPS, WAF(web aplicación firewall), DAM?

A través de Herramientas externas. A consideración del encargado de la red.

6 ¿Existe una política de segmentación de red?

Si, no se encuentra documentación.

7 ¿Qué tipo de segmentación existe?

Por VLAN.

8 ¿Cómo se monitorea y controla la segregación?
Se segmento en un documento a través de una política de red.

9 ¿Se segmenta la red inalámbrica de la red física? Si ¿Y la red de invitados?
Si se segmenta, si hay una separación física de la red, en la organización no cuenta con la red invitados.

10 ¿Hay controles adecuados entre ellos?
No aplica.

11 ¿Cómo se controla la segmentación con proveedores y clientes?
No aplica. No depende de proveedores.

12 ¿La seguridad es adecuada dados los riesgos y el apetito de riesgo de la organización?
A nivel de políticas de manejo de datos, según la necesidad. Actualización de Antivirus.

13 ¿Existen políticas y procedimientos relacionados con la transmisión segura de información?
Si.

14 ¿Contempla mecanismos como correo electrónico, FTP y otras aplicaciones de transferencia de datos y protocolos Web (ej. Los grupos / foros, Dropbox y

servicios en la nube similares), WiFi y Bluetooth, CD / DVD, almacenamiento externo USB, mensajería, etc.?

Si, discos duros externos, nube, plataformas de transmisión de videos, unidad de DVD etc.

15 ¿Está basado en la clasificación de la información?

Si.

16 ¿Existen controles de acceso adecuados para esos mecanismos?
Si. Cambios de claves

17 ¿Cómo se implementa el uso de criptografía para los mecanismos aceptados (ej. TLS, cifrado de correo electrónico, ZIP codificados)?

Si, certificados de seguridad vigentes (correo, FTP y servicios web)

18 ¿Se sigue el principio de confidencialidad y privacidad?
Si.

19 ¿Existen un programa de concientización, capacitación y cumplimiento?
No. En la práctica no se cumple.

20 ¿Qué tipos de comunicaciones se implementan las firmas digitales?
No se encuentra implementado.

21 ¿Qué tipo de responsabilidades se asocian a la perdida, corrupción o divulgación de datos?
Legal de derechos de autor y contractual.

22 ¿Existe una identificación y sincronización de los niveles de clasificación de información de todas las partes involucradas?
Si, soporte de correos, soporte de vpn

23 ¿Cómo se mantiene una cadena de custodia para las transferencias de datos?
Se lleva con formatos recepción de material, y monitoreo de cámaras y sistemas de software.

24 ¿Existe una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP, etc.?
Si. Sistema de tareas de VSN,

25 ¿Hay controles de seguridad adecuados (ej. cifrado de correo electrónico, la autenticidad, la confidencialidad y la irrenunciabilidad de mensajes, etc.)?

Si

26 ¿Existen controles de seguridad para la interacción con sistemas Internet, Intranet relacionados con foros y tableros de anuncios electrónicos?

No aplica.

27 ¿Existen acuerdos de confidencialidad?
Si. Delegado con departamento de jurídica.

28 ¿Han sido revisados y aprobados por el Departamento Legal?

Si.

29 ¿Cuándo fueron revisados por última vez (periódicos o basados en cambios)?
Cada 3 meses se presentan informes.

30 ¿Han sido aprobados y firmados por las personas adecuadas?
Si, departamento de jurídica, gestión técnica y gerencia.

31 ¿Existen sanciones adecuadas y acciones esperadas en caso de incumplimiento y / o beneficios por el cumplimiento (ej. una bonificación de rendimiento)?
Acciones de mejora, hallazgos, llamados de atención, Cancelación del contrato, Cobros, Sancionar.

Bibliografía

9tut.com. (16 de Junio de 2014). *9tut.com*. (9tut.com) Recuperado el 19 de Febrero de 2019, de https://www.9tut.com/simple-network-management-protocol-snmp-tutorial

Amaya, C. G. (18 de Octubre de 2013). *welivesecurity*. Recuperado el 10 de marzo de 2019, de https://www.welivesecurity.com/la-es/2013/10/18/renovados-anexos-iso-iec-27001-2013/

Amaya, C. G. (2013). *www.welivesecurity.com*. Recuperado el 2019, de https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Armando, L. Q. (2016). *Investigación Del Protocolo SNMP .* Mexico: Tecnológico Nacional De México.

Camerfirma S.A. (s.f.). *Tutorial Firma Electrónica*. Recuperado el 2015 de Abril de 22, de http://www.camerfirma.com/

Canal TRO. (2016). *Plan Estratégico Situacional 2016 - 2019*. Recuperado el 10 de Marzo de 2019, de https://www.canaltro.com/images/descargas/CONOCENOS/PLANEACION/PLAN_ESTRATEGICO_CANAL_TRO_2016-2019.pdf

CanalTRO. (s.f.). *Misión y Visión*. Recuperado el 10 de Marzo de 2019, de https://www.canaltro.com/intitucional/quienes-somos/mision-y-vision/

Cano, J. (2012). XII Encuesta Nacional de Seguridad Informática. *XIII Jornada Internacional de Seguridad Informática.* Bogotá. Obtenido de http://www.acis.org.co/

Cano, Saucedo, & Prandini. (2013). V encuesta Latinoamérica de seguridad de la información. *XIII Jornada Internacional de Seguridad Informática.* Bogotá. doi: http://www.acis.org.co/

cisco. (2017). *www.cisco.com.* Recuperado el junio de 2019, de https://www.cisco.com/c/es_mx/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf

Clavijo, C. A. (2006). *revistas.unilibre.edu.co.* Recuperado el junio de 2019, de https://revistas.unilibre.edu.co/index.php/entramado/article/view/3293/2687

Controles Anexo A - ISO 27001 Secutiry. (s.f.). Recuperado el 2019, de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwjS9Iral_jiAhWFjlkKHXP_CHAQFjACegQIARAC&url=https%3A%2F%2Fiso27001security.com%2FISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx&usg=AOvVaw3hummNKtxn-H

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2001). Introduction to Algorithms. En *Section 31.7: The RSA public-key cryptosystem* (págs. 881–887.). MIT Press and McGraw-Hill.

EMC Coroporation; RSA. (Febrero de 2013). *Fraud report: Phishing Kits – the same wolf, just a different sheep's clothing.* Recuperado el 30 de Octubre de 2014, de http://www.emc.com/

Enterprise, R. H. (2018). *web.mit.edu*. Recuperado el Marzo de 2019, de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-intro.html

Escalnate Acosta, F. D., Arcia Arévalo, K. J., & Mayo Bautista, M. I. (2006). Sistema ADMONPROJECTS: Herramienta de Integración de Diferentes Aplicaciones para la Administración de Proyectos. En *Avances en Informática y Sistema Computacionales* (pág. 115). Juárez, México: CONAIS.

forsenergy. (2016). *forsenergy*. Recuperado el 2019, de https://forsenergy.com/es-es/tscc/html/ca9804df-42f5-47b8-9f29-941cfb218a0a.htm

Icontec. (4 de Diciembre de 2017). NTC-ISO-IEC27000. En *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27000* (págs. 7-8). Bogotá. Recuperado el 10 de Marzo de 2019, de https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27000.pdf

Möller, B., Duong, T., & Kotowicz, K. (2014). This POODLE bites: exploiting the SSL 3.0 fallback. . *Google*.

NIEVES, A. C. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA.*

ORJUELA, L. A. (2017). *PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013 PARA LA EMPRESA INTERFACES Y SOLUCIONES.* Bogota.

pmg-ssi. (23 de Abril de 2015). (pmg-ssi) Recuperado el Febrero de 2019, de https://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

RSA laboratories. (3 de Junio de 1991). *PKCS#3: DIFFIE-HELLMAN KEY AGREEMENT STANDARD.* Recuperado el 23 de Abril de 2015, de ftp://ftp.rsasecurity.com/pub/pkcs/ascii/pkcs-3.asc

Schneie, B. (1996). *Applied Cryptography* (Vol. II). New York, USA: John Wiley & Sons.

Simmons, G. J. (Mayo 1988). A survey of information authentication. *Proceedings of the IEEE 76.5, 76*(5), 603 - 620.

SUÁREZ, A. E. (2015). *DISEÑO E IMPLEMENTACIÓN DE UN SGSI PARA EL ÁREA DE INFORMÁTICA DE LA CURADURÍA URBANA SEGUNDA DE PASTO BAJO LA NORMA ISO/IEC 27001.* Pasto.

Tanenbaum, A. S. (2003). Establecimiento de una clave compartida: El intercambio de clves de Diffie-Hellman. En *Redes de computadoras* (págs. 791-792). Pearson Educaction Inc.

Tiwari, H., & Asawa, K. (2010). Cryptographic hash function: an elevated view. *European Journal of Scientific Research, XLIII*(4), 452-465.

TRO. (2019). *canaltro*. Obtenido de www.canaltro.com/intitucional/quienes-somos/organigrama/

TRO, C. (31 de Diciembre de 2017). *ESTADO DE SITUACION FINANCIERA* . Recuperado el 10 de Marzo de 2019, de https://www.canaltro.com/images/descargas/CONOCENOS/FINANCIERA_Y_CONTABLE/ESTADOS_FINANCIEROS/2017/ESTADOS_FINANCIEROS_CANAL_TRO_2017_NIIF.pdf

TRO, C. (s.f.). *Plan Estrategico situacional 202 - 2015*. Recuperado el 10 de Marzo de 2019, de https://web.archive.org/web/20150923200148/http://www.canaltro.com/webtro/images/pdf/pes.pdf

winex. (2017). *http://www.winex.com.py*. Recuperado el junio de 2019, de http://www.winex.com.py/2017/03/05/segmentacion-y-direccionamiento-ip/