AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.

JESUS GERMAN CORTES CAMACHO

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO, COLOMBIA
2016

AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.

JESUS GERMAN CORTES CAMACHO

Proyecto de Grado para optar al título de: Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO, COLOMBIA
2016

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

San Juan de Pasto, Diciembre de 2016

Dedico este trabajo a mis padres Jesús Cortés y Luz Betty Camacho, quienes gracias a su apoyo incondicional, consejos, paciencia y comprensión, alcanzo uno de los logros más importante en mi vida profesional y también a mi novia Daissy Ordoñez quien gracias a ella me inspiro para realizar este posgrado y fomentar más aun mi vida académica.

Jesús Germán Cortés Camacho

AGRADECIMIENTOS

Como autor, expreso mis más profundos agradecimientos, en primer lugar al ingeniero Francisco Nicolás Solarte, docente de la UNAD, por brindar la atención y ayuda para el desarrollo del presente trabajo, a mis compañeros de posgrado, Javier Mesías y Diego Solarte, que contribuyeron con su apoyo y aportes en la culminación de este trabajo.

A los funcionarios de la empresa Panavias S.A. quienes colaboraron de manera desinteresada con el desarrollo de la presente auditoria y a todos los compañeros y amigos que contribuyeron de alguna forma en la elaboración del presente trabajo de grado, gracias a todos por su apoyo.

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pag.

.

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: Se define como la información o datos de alta relevancia para una empresa. Los activos de información pueden ser bases de datos, datos de usuarios, números de cuentas, contraseñas, etc

ACTIVO INFORMATICO: Se define como aquellos recursos, ya sean físicos o lógicos, hardware o software, con los que cuenta la empresa y comprenden procesos de comunicación, partiendo desde la información que estos contienen, el emisor, el medio de transmisión y el receptor. Los activos informáticos pueden ser servidores, routers, cable de red, aplicaciones cliente servidor, aplicaciones web, etc.

ACCION CORRECTIVA: En auditoria, se define como la acción tomada para eliminar o mitigar una condición existente con el objetivo de minimizar su riesgo.

AMENAZA: Son eventos que pueden causar alteraciones en los activos informáticos o activos de información de una organización, siempre y cuando una vulnerabilidad pueda ser explotada.

ANALISIS DE BRECHA: Es un diagnostico detallado de la distancia que existe entre cada evaluación del dominio o proceso auditado, con la situación actual de la organización. Las brechas se refieren al funcionamiento actual de la organización y son comparadas con estructuras de planes formulados, con el objetivo de crear estrategias óptimas de negocio para la empresa.

ANALISIS DE RIESGOS: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

AUDITORIA: Es un proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

AUDITOR: Persona que ejerce y ejecuta el proceso de auditoría.

CONTROL: Son aquellas prácticas, procedimientos y estructuras organizativas creadas para mantener o controlar los riesgos de alta criticidad por debajo del nivel de riesgo asumido.

CONFIDENCIALIDAD: Según [ISO/lEC 13335-1:2004]: se define como: " característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados".

COPIA DE RESPALDO: Se refiere a las copias de seguridad que se realiza a aquella información relevante en una organización ante una posible catástrofe informática o natural.

CRIPTOGRAFÍA: Es la ciencia que se ocupa del diseño de procedimientos para cifrar los datos; es decir, para enmascarar una determinada información de carácter confidencial.

CUESTIONARIO DE CONTROL: instrumento de recolección de información utilizado dentro de la auditoria para determinar el nivel de riesgo al que se encuentra expuesto el proceso auditado.

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el diseño del SGSI de la organización, que se obtienen tras el resultado de los procesos de evaluación y tratamiento de riesgos.

DIRECCIÓN IP: Es el numero único e irrepetible que identifica una interfaz de red

DISPONIBILIDAD: Según [ISO/lEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

DNS: Sistema de nombres de dominio. Es un sistema jerárquico que asigna un nombre de dominio a los dispositivos o equipos conectados a una red.

EVALUACIÓN DE RIESGOS: Según [ISO/lEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

FINGERPRINTING: Dentro del Pentesting, se define como el proceso de recopilación que permite identificar el sistema operativo de un punto objetivo.

FIREWALL: O cortafuegos, es un sistema de red, el cual está diseñado o configurado para bloquear accesos no autorizados a una red local o red privada.

GUIA DE HALLAZGO: Instrumento de auditoria, el cual es utilizado para la organización de los resultados de los procesos verificados y documentar sus acciones correctivas o recomendaciones.

HOST: Se define como un anfitrión, el cual es el punto donde reside un sitio o aplicación web el cual posee una dirección única (dirección IP) y un nombre de dominio único (DNS).

INCIDENTE: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORME DE AUDITORIA: Es un informe ejecutivo, donde se redactan los resultados finales de la auditoria. Este contiene la breve descripción del proceso de auditoría, los riesgos encontrados y las recomendaciones para realizar las respectivas acciones correctivas.

IMPACTO: Resultado de un incidente o el efecto que produce una amenaza.

INTEGRIDAD: Según [ISO/IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso

LISTA DE CHEQUEO: Instrumento de recolección de la información utilizado dentro de los proceso de auditoría para determinar si la empresa cumple o no cumple con la normatividad o proceso con la que se está evaluando.

MANTENIMIENTO: Conjunto de acciones o procedimientos tendientes a preservar o restablecer un bien, a un estado tal que le permita garantizar la máxima confiabilidad

MONITOREO DE RED: Conjunto de acciones que permiten gestionar, controlar, supervisar y administrar todas las actividades y eventos de una red, a través de herramientas de control de tráfico, inspección y de identificación de vulnerabilidades.

NIVEL DE RIESGO: escala cualitativa-cuantitativa, que permite identificar el nivel de criticidad de un riesgo evaluado.

NIVELES DE MADUREZ: Son aquellos valores con los que la administración o el grupo auditor determina, evalúa, gestiona y controla los riesgos

NORMATIVIDAD: Documento aprobado por una institución reconocida, que prevé, para un uso común y repetido, reglas, directrices o características para los productos o los procesos y métodos de producción conexos, servicios o procesos, cuya observancia no es obligatoria.

PAPELES DE TRABAJO: Son aquellos instrumentos con los que realiza el proceso de auditoría, para la recolección de la información, la evaluación y organización de los resultados. Como por ejemplo: listas de chequeo, entrevistas, cuestionarios de control, guías de hallazgos, guía de pruebas, etc.

PROBABILIDAD: Se define como la posibilidad de que la amenaza ocurra o se materialice.

PUERTO DE RED: Es una interfaz de comunicación utilizada por dos ordenadores para el intercambio de datos o información.

PRUEBA DE PENETRACION o PENTESTING: Es un procedimiento de tipo metódico y sistemático con el objetivo de identificar vulnerabilidades, amenazas y riesgos, en una red o sistema informático a través de distintas fases, como lo son recolección, análisis, explotación y post explotación de esas vulnerabilidades,

RIESGO: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información

SERVICIO DE RED: Se refiere a los recursos o aplicaciones que se ejecutan en uno o más servidores de una red.

TRACEROUTE: Es el registro que permite seguir los paquetes que vienen desde un host (punto de red), hasta su punto objetivo

UTP: Siglas en ingles, *Unshielded Twisted Pair.* Cable par trenzado no blindado utilizado específicamente para comunicaciones de red. Este se encuentra estandarizado por dos normas, una estadounidense y la otra internacional las cuales son TIA/EIA-568-B y a la internacional ISO/IEC 11801

VISITAS TECNINAS: Dentro de la auditoria, se refiere a las visitar que realiza el auditor a la empresa, con el objetivo de observar el estado de la misma. Posteriormente, emite un informe de su estado actual y los comentarios técnicos de la misma.

VULNERABILIDAD: Según [ISO/lEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

RESUMEN

El presente proyecto aplicado, tiene como finalidad realizar una auditoría de seguridad a la red de datos de la empresa Panavias S.A. en la ciudad de San Juan de Pasto el cual tiene por objetivo formular controles y procedimientos con el fin de establecer un sistema de gestión adecuado, identificando vulnerabilidades y amenazas por medio de pruebas de penetración y los procesos de auditoria de sistemas.

Para el desarrollo de la auditoria se aplicaran las cuatro fases:

La primera consiste en la recolección de la información pertinente a la red de datos, por medio de visitas técnicas guiadas y verificando la documentación existente a los procesos de servicio de red.

En la segunda fase de planeación, donde se seleccionaran los respectivos instrumentos de auditoria para la recolección de información y las pruebas de penetración a ejecutar en la red de datos de la empresa Panavias S.A., como también la normatividad a aplicar en la presente auditoria.

En la tercera fase de ejecución, se aplicaran los instrumentos seleccionados y las pruebas de penetración, con el fin de detectar vulnerabilidades existentes en la red de datos de la empresa Panavias S.A. Con estos hallazgos, se realizara el análisis de riesgos para determinar la probabilidad y el impacto que tienen estos riesgos sobre la red de datos de la empresa.

En la cuarta y última fase, se organizaran los resultados de la anterior fase y se determinara los niveles de madurez, respecto a la normatividad seleccionada y se realizara una declaración de aplicabilidad, que contenga los controles y procedimientos con el fin de establecer un sistema de gestión adecuado.

Por último se entregará el informe final de auditoria en la gerencia de la empresa Panavias S.A. para realizar las respectivas acciones preventivas, detecticvas y correctivas.

INTRODUCCIÓN

Hoy en día las tecnologías de la información y la comunicación (TIC) son base fundamental en las organizaciones, ya que apoyan en la realización de sus operaciones y en la continuidad del negocio. Con el uso de la informática y la tecnología en las organizaciones, los procesos se realizan de una manera sistemática, ágil y sencilla, sin embargo estos procesos deben ser confiables y seguros. La seguridad informática permite asegurar las prácticas operacionales que determinan la confiabilidad de la infraestructura tecnológica.

Las tecnologías de la información (TI) son fundamentales en todas las organizaciones ya que su activo más valioso es la información; es por ello que se debe brindar la importancia necesaria y la seguridad correspondiente a partir de las necesidades de los procesos que se manejan, creando estrategias y siendo estas imprescindibles para garantizar el funcionamiento y la seguridad de los sistemas de información organizacionales y la infraestructura tecnológica de las redes empresariales.

Con la evolución en los últimos años de las redes empresariales y el crecimiento en cuanto a la complejidad de estas, se ha visto la necesidad de crear sistemas más seguros ante la presencia de posibles ataques informáticos, los cuales las convierte en vulnerables y amenazan con la continuidad del negocio.

Surge la necesidad de realizar una auditoría a la seguridad de la red de datos en la empresa Panavias S.A. ya que la importancia de la información manejada por esta organización debe garantizar un sistema seguro frente a los distintos tipos de ataques informáticos que se presentan en la actualidad, asegurando la seguridad física y lógica de la red informática.

El presente proyecto de aplicación tiene por objetivo identificar las vulnerabilidades, amenazas y los riesgos que se presentan en la red de datos de la empresa Panavias S.A., por medio de procesos de auditoría aplicados a la seguridad informática donde se establezcan recomendaciones que permitan un enfoque de un sistema de control eficiente por parte de la empresa donde se asegure su red informática.

1. PLANTEAMIENTO DEL PROBLEMA

El problema general que se presenta en la empresa PANAVIAS S.A. es que no existe una adecuada segmentación de la red lo que está generando problemas de confidencialidad de la información que se maneja en las diferentes dependencias ya que todos los usuarios están en una sola red, lo que permite el acceso a los servicios y datos privados de la organización.

Otro de los problemas en la empresa PANAVIAS S.A. es que no cuenta con el personal para la administración de la red de datos, existe personal de sistemas pero no un administrador de red que opere los servicios que están configurados en ella.

También se ha detectado que los usuarios de la red tienen el mismo nivel de acceso a la información y a los servicios, y se han ocasionado problemas tales como: caídas frecuentes del servicio de internet, el sistema operativo de red no está actualizado, los dispositivos de red están obsoletos y en general no existe mantenimiento sobre la red de datos de la empresa.

En la actualidad, la empresa Panavias S.A. posee desconocimiento del estado de seguridad de la red de datos ya que a lo largo de su historia nunca se han realizado auditorias de seguridad informática. Esto la conlleva a tener un sistema de red vulnerable ante los distintos tipos de ataques informáticos que podrían atentar con la integridad, confidencialidad y disponibilidad de la información que soporta su red de datos.

Tampoco existen políticas y procedimientos de seguridad o sistemas de control informático que ayuden a mitigar las vulnerabilidades y amenazas que se podrían presentar. Otros aspectos en cuanto a la seguridad de la información que no se presentan en la empresa Panavias S.A. son manejos y responsabilidades sobre la seguridad de los activos de información, políticas sobre los controles de acceso a los sistemas de información, una gestión ante incidentes en la seguridad de la información y gestión de la seguridad en la red.

Debido justamente al crecimiento de los delitos informáticos que afectan directamente a los datos, la empresa considera de vital importancia realizar una auditoría de seguridad a su red informática, con el fin de generar un sistema de control que ayude a evitar los posibles ataques y reducir los niveles de vulnerabilidad.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo la auditoría a la seguridad de la red de datos permitirá diseñar un sistema de gestión de seguridad informático para la red de datos que contenga los controles dentro de las políticas y procedimientos que evite los posibles ataques y reduzca los niveles de vulnerabilidad en la red de la empresa Panavias S.A.?

2. JUSTIFICACIÓN

Actualmente la empresa Panavias S.A., maneja una infraestructura de información en crecimiento, de la cual dependen muchos de los procesos y del buen funcionamiento de la información de la organización que se encuentran en sus sistemas de información y el intercambio de esta a través de internet, por esta razón es importante desarrollar una auditoría a la seguridad de la red de datos para garantizar un sistema seguro y de calidad en los activos de información que se manejan.

Teniendo en cuenta lo anterior es importante realizar este proyecto, colocando a la empresa Panavias S.A. como el principal beneficiario, ya que la realización de una auditoria de seguridad informática la ayudara a establecer políticas sobre la seguridad de la información tanto interna como externamente, implementando un sistema de gestión de seguridad sobre los activos de información manejados y que son responsabilidad de la organización, además beneficiara a sus clientes y proveedores dándoles mayor seguridad y confianza en la empresa.

El desarrollo de una auditoria de seguridad informática a la red de datos de la empresa Panavias S.A., permitirá identificar vulnerabilidades y corregir los fallos de seguridad de la red antes de que sean explotados, con lo que la empresa podrá asegurar la calidad en su red informática. Además se verán beneficiados los funcionarios de la empresa ya que contaran con un sistema de red confiable en el manejo y gestión de la información.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Desarrollar una auditoría a la seguridad de la red de datos que permita diseñar un sistema de gestión de seguridad informático que contenga los controles y procedimientos para la red en la empresa Panavias S.A.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la empresa Panavias S.A. para verificar la existencia de las vulnerabilidades y amenazas existentes en los activos informáticos y de información.

- Seleccionar la norma que se va a aplicar, dominios, diseñar los instrumentos de recolección de información y pruebas aplicables a la red de datos de la empresa Panavias S.A.

- Aplicar los instrumentos diseñados y ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a seguridad de la red de datos de la empresa Panavias S.A.

- Elaborar un informe de los resultados obtenidos en la auditoria que contenga los hallazgos y recomendaciones para el diseño de un SGSI que contenga los controles que permitan mitigarlos.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El proyecto se llevará a cabo en la red de datos de la empresa Panavias S.A. ubicada en la ciudad de San Juan de Pasto.

Para el proyecto se tendrán en cuenta las normas internacionales ISO/IEC 27001:2013, la ISO/IEC 27002:2013 y se seleccionara una metodología para el análisis y gestión de riesgos

Dentro de la norma se seleccionarán solamente los dominios relacionados con la red de datos. Estos serán los dominios directamente relacionados:

A9. Control de acceso
A13. Seguridad en las Telecomunicaciones

Además se tendrán en cuenta otros aspectos relacionados en los dominios:

A5. Políticas de la Seguridad de la Información
A6. Organización de la Seguridad de la Información
A11. Seguridad Física y del Entorno

Se aplicarán pruebas de penetración que sirvan de evidencia de las vulnerabilidades y posibles amenazas existentes en la red de datos de la empresa Panavias S.A.

5. MARCOS DE REFERENCIA

5.1. ANTECEDENTES

La empresa Panavias S.A. a lo largo de los 30 años de funcionamiento se ha consolidado a través de la ejecución de importantes proyectos gracias a la idoneidad y capacidad del recurso humano con que cuenta, comprometido con el desarrollo integral de la organización, contando con números proyectos y obras a nivel nacional en las distintas ciudades del país, por lo que la información que se maneja en los diferentes sistemas necesita ser protegida por cualquier amenaza sobre todo al momento de ser transmitidos a través de los medios de comunicación como son las redes informáticas en si es de vital importancia preservar las características de la seguridad de la información que se identifican por la confidencialidad, integridad y disponibilidad de la información.

Los siguientes proyectos de investigación servirán como antecedentes al desarrollo de la auditoria de la seguridad de la red de datos de la empresa Panavias S.A. ya que aportaran técnicas de análisis de riesgos y evaluación de controles de seguridad de la información.

El proyecto denominado “Auditoria Informática a la parte física y lógica de la red de datos en la empresa solidaria de salud Emssanar E.S.S. sedes corporativa Pasto y sedes alto Putumayo” de los ingenieros Acosta Diego Alexander y Caicedo Heider Henry (2014) de la Universidad de Nariño, presenta el proceso de auditoria en una red, esencial al caso a aplicar en el presente proyecto, donde se realizó la identificación de riesgos y vulnerabilidades de la red.

El proyecto denominado “Auditoría de Sistemas Aplicada al Sistema Integral de Información en la Secretaría de Planeación Municipal de la Alcaldía de Pasto” del ingeniero Estrada Oscar Julián (2009) de la Universidad de Nariño, presenta una evaluación de los controles relacionados con la seguridad de la información, identifica las fallas en cuestión de seguridad y plantea las posibles soluciones para mejorar las condiciones de seguridad físicas y lógicas del Sistema Integral de Información.

El proyecto denominado “Auditoría de Sistemas al aula de informática de la Universidad de Nariño” de los ingenieros Mesías Javier Orlando y Benavides Edgar Osvaldo (2009) de la Universidad de Nariño, aporta diferentes técnicas y herramientas para la auditoria y en ella se examinó la gestión informática, la

seguridad del personal, de las instalaciones físicas, la red de datos, las bases de datos, la red eléctrica, el hardware y el software.

5.2. MARCO CONTEXTUAL

5.2.1. Nombre de la Empresa

Panavias S.A.

5.2.2. Misión

Panavias S.A. es una empresa dedica al desarrollo de obras civiles, tales como la constitución y mantenimiento de vías, cumpliendo las especificaciones de los clientes, contando con personal altamente calificado y comprometido con la empresa para continuar conservando el prestigio y buen nombre.[1]

5.2.3. Visión

Panavias S.A. tiene el objetivo de ser una empresa altamente competitiva en el mercado, desarrollando grandes obras de la Ingeniería Civil, ofreciendo calidad, un excelente servicio al cliente, respaldado en la solidez, ética y profesionalismo de sus colaboradores.[2]

5.2.4. Organización

La empresa Panavias S.A. tiene como finalidad dentro de los proyectos de infraestructura vial que desarrolla, lograr la satisfacción de sus clientes y cumplir las especificaciones técnicas apoyándose en el mejoramiento continuo del sistema de gestión de calidad, capacitación del personal y cumplimiento de la legislación vigente.

La empresa a los largo de su trayectoria ha ejecutado importantes proyectos de infraestructura vial del orden nacional, rural y urbano. La información sobre proyectos que se ejecutan en otras ciudades que tienen convenio con Panavias S.A. se gestionan vía internet, ya sean trámites o servicios de la empresa. La red de instituto tiene una topología hibrida que soporta a sus servidores, y la cual se

[1] PANAVIAS. Misión de la empresa. Archivo Panavias S.A. San Juan de Pasto, Colombia
[2] PANAVIAS. Visión de la empresa. Archivo Panavias S.A. San Juan de Pasto, Colombia

conectan internamente terminales de la organización, y estos se distribuyen entre equipos de escritorio y portátiles.

5.3. MARCO TEORICO

5.3.1. Auditoria

El origen etimológico de la palabra auditoria proviene del verbo latino audire que significa 'revisar', 'intervenir' y se define como un proceso sistemático que comprende una serie de procedimientos lógicos, estructurados y organizados. Se entiende como un examen crítico y sistemático utilizando técnicas determinadas que se realiza a una organización con el fin de evaluar el cumplimiento de normas y objetivos que determinan la eficiencia y eficacia de todos los procesos verificados, estableciendo alternativas y soluciones que mejoren el sistema examinado.

De igual manera la American Accounting Association (AAA) define la auditoria identificándola como "un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso."[3]

Un auditor debe ser una persona con formación personal y normativa y debe reunir cualidades como lo son el análisis, la observación, imparcialidad, discreto e independiente.

5.3.2. Clasificación de la Auditoria

Con base como se ejerce la auditoria, esta se clasifica de dos maneras, auditoria externa y auditoria interna.

- Auditoria Externa
  La auditora externa se caracteriza porque es realizada por un personal que no tiene ningún tipo de vínculo con la empresa el cual se encuentra en

[3] Construcción de un concepto universal de auditoria. Disponible en: http://fccea.unicauca.edu.co/old/tgarf/tgarfse1.html

libertad de aplicar distintos tipos de técnicas, métodos y herramientas con el fin de cumplir con el proceso de auditoría. Por lo general los encargados de realizar las auditorías externas son organizaciones independientes dedicadas a la certificación de calidad quienes evalúan al final si la empresa cumple o no con los requisitos exigidos por cada tipo de certificación.

- Auditoria Interna
  La auditoría interna es aquella evaluación elaborada ya sea por una persona o un equipo de auditorías dentro de la organización con el fin de determinar el desempeño y cumplimiento de actividades de todos los procesos desarrollados en la empresa. Posee ventajas como lo son la revisión más profunda de los procesos y el diagnostico domestico confidencial sobre las actividades de la empresa. Su objetivo es evaluar a cabalidad la eficiencia y eficacia de las funciones, responsabilidades y objetivos con el fin de detectar problemas o fallas a tiempo, cumplir con los requisitos regulatorios y comprender a profundidad los procesos y operaciones de la empresa.

5.3.3. Auditoria Informática

Se entiende como el proceso de recoger, agrupar y evaluar evidencias de todos los recursos informáticos existentes con el fin de evaluar la eficiencia y eficacia de dichos recursos y emitir un informe o diagnóstico de la situación real de su gestión y que permitan concluir si están correctamente encaminados en los objetivos de la empresa. Así mismo, la auditoria informática tiene por objetivo la evaluación de un sistema informático con el fin de emitir un diagnóstico sobre su fiabilidad y exactitud, como también detectar y corregir los errores encontrados durante su evaluación y asegurar la continuidad de la gestión.

Según Juan José Iturmendi, la auditoría informática es “un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente”.[4]

[4] ITURMENDI ACHA, Juan José. Auditoria Informática en la Empresa. 1994, España

5.3.4. Auditoria Informática de Comunicaciones y Redes

Para las organizaciones, hoy en día es de vital importancia que se evalúen contante y regularmente los sistemas de redes y todo lo relacionado con los procesos Telemáticos. Esta se constituye principalmente en la revisión de las redes nodales, redes locales, protocolos, topologías de red, arquitecturas de red, como también la revisión y uso idóneo de los soportes de red como es su hardware y software.

Entre los objetivo de la realización de una auditoria informática de comunicaciones y redes se podrían considera la de asegurar la confiabilidad, confidencialidad e integridad de la información, así como también minimizar la existencia de riesgos en el uso de las tecnologías de la información (TI) y de sus sistemas de información. [5]

5.3.5. Auditoria de Seguridad Informática

En la actualidad, los activos de información se convierten en la pieza más importante en toda organización y la tecnología es clave para su gestión. Así como la tecnología puede ayudar a la organización a lograr sus objetivos y planes de negocio, el no gestionar correctamente su uso la transforma en una amenaza potencial para la organización. Surge entonces la necesidad de implementar auditorias de seguridad informática que permitan a las organizaciones la creación de políticas con el fin de asegurar los activos de información desarrollando un conjunto de principios y reglas que sinteticen como se gestionara la protección de la información y así asegurar la continuidad del negocio.

Las amenazas informáticas ocasionan un gran problema frente a los activos de información de las empresas, que van desde la perdida de datos hasta el robo de información confidencial, por lo que la seguridad informática abarca dos conceptos, el de la seguridad física, que consiste en la protección del hardware y los soportes de datos; y la seguridad lógica que abarca la creación de políticas y procesos de acceso a los datos, aplicaciones y sistemas de información.

---

[5] Auditoria Informática en Redes y Telecomunicaciones. Introducción y Conceptos, Usos, Metodologías y Aplicaciones. Disponible en: http://datateca.unad.edu.co/contenidos/2150517/2150518_Temp/Material_apoyo1/

5.3.6. ISO/IEC 27001:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que tiene por objetivo gestionar la seguridad de la información *(Information technology - Security techniques - Information security management systems - Requirements)* en una empresa. Se publica por primera vez en el año 2005 en base a la Norma Británica BS 7799-2 y se actualiza en el año 2013 bajo el nombre de ISO/IEC 27001:2013. [6]

Esta norma es una guía que puede ser implementada para mejorar los procesos de seguridad de información en todo tipo de organización. Su metodología establece, implementa, mantiene y mejora un sistema de gestión de seguridad de la información (SGSI), siendo coherente y de fácil manejo. Permite la certificación de la empresa por una entidad ya sea pública o privada, confirmando su seguridad en gestión de la información.

En Colombia esta norma se encuentra estandarizada por el Instituto Colombiano de Normas Técnicas y de Certificación ICONTEC (NTC-ISO-IEC 27001:2013).

Un aspecto de la norma ISO 27001 incluye el ciclo de Deming el cual consiste en procesos basados en el método de mejora continua, conocido como el ciclo PHVA: Planificar, Hacer, Verificar y Actuar, el cual se basa en un procedimiento cíclico mediante el cual se determinan las objetivos y procesos necesarios que se planean implementar (Planificar), luego se procede a implementar los procesos (Hacer), posteriormente, se revisan y se evalúan todos los procesos comparándolos con las políticas y objetivos sobre los resultados (Verificar), y por último, se emprenden las acciones para el mejoramiento del sistema (Actuar). [7]

5.3.7. ISO/IEC 27002:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) donde se describen los dominios y mecanismos de control que pueden ser implementados en una organización en cuanto a la seguridad de la información. Esta norma se ofrece como una guía para ser implementada en las organizaciones ayudando a establecer los controles de seguridad y las buenas

---

[6] ISO/IEC 27001. Evolución e historia. Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_27001
[7] ISO 27001, Ciclo de Deming. Disponible en: http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

prácticas para gestionar la seguridad de la información. Se encuentra asociada con el Anexo A de la ISO/IEC 27001:2013.

Como precedentes, esta se publica por primera vez como un cambio de nombre de la norma ISO 17799 la cual tiene su origen la Norma Británica BS 7799-1 que se estandarizo en el año 1995. Luego la Organización Internacional de Normalización (ISO) en conjunto con la Comisión Electrónica Internacional (IEC) en el año 2000 publica el estándar 17799:2000. Tras un periodo de revisión y verificación, en el año 2005 se publica una nueva versión bajo el nombre de ISO/IEC 17799:2005. Con la aprobación de la norma ISO/IEZAC 27001:2005 y el estándar IGFSO/DIEC 17799:2005 paso a llamarse en Julio de 2007 ISO/IEC 27002:2007.[8]

Su versión más reciente es en el año 2013 y contiene catorce (14) dominios principales, los cuales son los siguientes, los cuales son tomados directamente de la norma[9]:

A5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

A6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACÍON.

6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguridad de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.

[8] ISO/IEC 27002. Precedentes y evolución histórica. Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_27002

[9] NTC-ISO-IEC 27002:2013. Tecnología de la Información. Técnicas de Seguridad. Código de Practica para Controles de Seguridad de la Información.

6.2.2 Teletrabajo.

A7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en seguridad de la información.
7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

A8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.

8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

A9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

A10. CIFRADO.

10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

A11. SEGURIDAD FÍSICA Y DEL ENTORNO.

11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

A12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

A13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

A15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

A16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

A17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

A18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Cada subdominio contiene sus controles y su guía de implementación. Para el presente proyecto, se tomaran aquellos dominios directamente relacionados con la auditoria los cuales son el A9. Control de Accesos y el dominio A13. Seguridad en las Telecomunicaciones. Además se tomaran aspectos de otros dominios, los cuales estarán indirectamente relacionados; la documentación de seguridad de la información con los dominios A5. Políticas de Seguridad y el dominio A6. Organización de la Seguridad de la Información, como también del dominio A11. Seguridad Física y del Entorno que tiene que ver con la seguridad física del equipo de cómputo y de red.

5.3.8. Metodología de Análisis y Gestión de Riesgos

De acuerdo a Rodrigo Ferrer, dentro de las auditorias de seguridad informática, es importante establecer métodos que permitan la asignación de valores de impacto o de riesgo de los activos de información, que ayuden en la selección de controles adecuados ante la presencia de un posible evento negativo que amenace las operaciones y la continuidad del negocio de una organización. Estos métodos pueden tanto cuantitativos como cualitativos.

Las metodologías para el análisis de riesgos informáticos ayudan a determinar cómo se encuentran protegidos los activos. Además, en conjunto con los objetivos, estrategias y políticas de la organización, el análisis de riesgos y su gestión permite establecer un plan de seguridad e implementar controles de acuerdo a los niveles de riesgo obtenidos que contribuyan en el desarrollo de la eficiencia y eficacia de los procesos de la organización.[10]

Entre las metodologías de análisis y gestión de riesgos más conocidas se encuentran:

- Magerit
- Octave

[10] FERRER, RODRIGO. Metodología de Análisis de Riesgo. Bogotá. Colombia, 2006. Empresa: SISTESEG

- NIST SP 800-30
- Mehari
- ISO/IEC 25005

Para desarrollar el análisis de riesgos de la presente auditoria, se tomaran aspectos relacionados con la Metodología Magerit, como lo son, la identificación y catálogo de amenazas, identificación de vulnerabilidades, la estimación de la probabilidad y el impacto con el fin de evaluar el riesgo y por último el mapeo de los riesgos o matriz de riesgos con el objetivo de realizar su tratamiento. Por ser una auditoria, se procederá a aplicar el análisis de riesgos para cada uno de los dominios directamente e indirectamente relacionados con el objetivo de establecer, al final de la auditoria, los niveles de madurez del proceso.

En el análisis y evaluación de riesgos, se tomaran los hallazgos obtenidos en las listas de chequeo y los cuestionarios de control cuantitativos. Teniendo en cuenta, que el presente proyecto es una auditoria, se aplicara el análisis de riesgos a cada uno de los procesos o dominios evaluados, esto quiere decir, que se realizara un análisis de riesgo por cada proceso o dominio.

- Valoración del Riesgo: La valoración de los riesgos encontrados se determinara por la siguiente escala, siendo de 1 a 6 considerado como Bajo, de 8 a 9, Medio y de 12 a 16 como riesgo Alto:

Tabla 1. Valoración del riesgo

Escala	Valoración del Riesgo
1 – 6	**BAJO**
8 – 9	**MEDIO**
12 – 16	**ALTO**

- Calculo de Análisis de Riesgos

Probabilidad: es la posibilidad que la amenaza ocurra. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 la máxima que se materialice la amenaza.

Impacto: es el efecto que produce la amenaza. Se mide en una escala de 1 a 4, donde 1 es el más bajo y 4 las máxima que afecte el recurso.

El riesgo total, se calcula de acuerdo a la probabilidad por el impacto de la siguiente manera:

*Evaluación del Riesgo = Probabilidad * Impacto*

Una vez valorados los riesgos, se procede a trasladarlos a una matriz, definidas de acuerdo a un color que corresponde a la escala (Verde = Riesgo Bajo, Amarillo = Riesgo Medio, Rojo = Riesgo Alto) la cual de esta manera se pueda decidir el tratamiento para estos riesgos. Este tratamiento se realizara a aquellos riesgos considerados como altos o críticos en las guías de hallazgo con sus recomendaciones correspondientes a sus controles y planes de mitigación.

5.3.9. Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI es el eje central en el cual se fundamenta y se construye la ISO 27001. Este se podría considerar como un sistema de calidad para la seguridad de la información el cual tiene por objetivo una vez identificados los riesgos, sean gestionados y minimizados por la organización de una manera documentada a través de un proceso estructurado y sistemático, esto con el fin de preservar la confidencialidad, integridad y disponibilidad de la seguridad de la información en la organización. [11]

La implementación de un SGSI en una organización es de gran utilidad ya que proporciona la protección de los objetivos del negocio realizando un modelo de gestión de seguridad con procedimientos adecuados como lo son la planificación e implementación de controles de seguridad basados en un análisis y evaluación de riesgos que se revisan y se mejoran constantemente.

Al finalizar la auditoria, se realizara un informe que contenga los hallazgos y recomendaciones con el objetivo de desarrollar el diseño de un SGSI, de acuerdo a la selección de los dominios directamente e indirectamente relacionados, de la red que contengan los controles que permitan corregirlos.

5.4. MARCO CONCEPTUAL

Para el desarrollo de este proyecto, se definen las siguientes variables, las cuales son tomadas directamente de la serie ISO/IEC 27000:2013 y se definen como[12] :

[11] SGSI. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf
[12] Portal ISO 27000. Glosario. Disponible en: http://www.iso27000.es/glosario.html

- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Integridad: Propiedad de la información relativa a su exactitud y completitud.

- Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- Control: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5.5. MARCO LEGAL

A continuación se presentan las leyes y normas aplicables para el desarrollo del presente proyecto

5.5.1. Ley 1273 de 2009 - ‘De la Protección de la Información y los Datos’

Con esta ley se preservan integralmente los sistemas que utilicen de las tecnologías de la información y la comunicación, entre otros. En esta ley se tipificaron como delitos, el uso abusivo de los datos personales por lo que es de resulta de gran importancia para las empresas que se blinden jurídicamente en este ámbito para evitar incurrir en ciertas conductas estipuladas como delitos penales.

La Ley 1273 de 2009 se compone de dos (2) capítulos y de diez (10) artículos. A continuación se sintetizaran aquellos artículos que correspondan al desarrollo del presente proyecto:

Artículo 269A: Acceso abusivo a un sistema informático toda persona que acceda a un sistema informático y permanezca en el sin autorización.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación incurrir en este delito toda persona que sin estar autorizado no permita el acceso a una red, sistema informático o los datos informáticos.

Artículo 269C: Interceptación de datos informáticos incurrirá en este delito toda persona que sin tener orden judicial intercepte ya sea en su origen, trasmisión, destino o al interior de un sistema informático los datos informáticos.

Artículo 269D: Daño Informático este delito contempla que toda persona quien no tenga la debida autorización que borre, altere, suprima o modifique datos informáticos o dentro de un sistema sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso aquí se contempla como delito la producción, tráfico, venta, distribución importación o exportación de software considerado como dañino o malicioso

Artículo 269F: Violación de datos personales, incurrirá en este delito toda persona que obtenga beneficio para sí mismo o para terceros de información personal contenida en bases de datos, ficheros.

Artículo 269G: Suplantación de sitios web para capturar datos personales, este delito contempla el diseño, creación distribución o venta de sitios web, enlaces o ventanas emergentes diseñados para capturar ilegalmente datos personales.

Artículo 269I: Hurto por medios informáticos y semejantes, incurrirá en este delito toda persona que a través de un sistema informático, red de un sistema electrónico o telemático cometa hurto.

Artículo 269J: Transferencia no consentida de activos. Este delito contempla la trasferencia no autorizada de activos en perjuicio de otra persona, mediante manipulaciones de tipo informático.

Entre los delitos más comunes en Colombia se encuentran:

- Hurto por medios informáticos y semejantes.
- Uso de software malicioso
- Violación de datos personales
- Acceso abusivo a un sistema informático[13]

5.5.2. Ley 1581 de 2012 - Protección de Datos Personales

Esta ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley.

A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia.

A las bases de datos y archivos de información periodística y otros contenidos editoriales.[14]

---

[13] Código Penal. Ley 1273 de 2009 De la Protección de la Información y de los Datos. Colombia, 2009. Ministerio de la Información y las Comunicaciones de Colombia

[14] Ley 1581 de 2012. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

6. MARCO METODOLÓGICO

6.1. METODOLOGÍA DE INVESTIGACIÓN

Teniendo en cuenta el planteamiento del problema propuesto en este proyecto, el enfoque que se quiere buscar en esta investigación es cuantitativo, ya que se busca medir las variables de seguridad de la información en la red de la empresa Panavias S.A., observando los métodos que utilizan para preservar la confidencialidad, integridad y disponibilidad.

El proyecto tendrá los siguientes tipos de investigación:

- Exploratoria: por cuanto se pretende identificar vulnerabilidades, amenazas y riesgos de la seguridad de la red de la empresa Panavias S.A.

- Descriptiva: porque el proyecto presenta medir confiabilidad, disponibilidad y confidencialidad en cuanto a la seguridad de la red de la empresa Panavias S.A.

6.2. UNIVERSO Y MUESTRA

El universo lo conforman los usuarios que integran la planta de trabajo y que se conectan a la red de la empresa Panavias S.A., distribuido entre personal de planta y contratistas, además de todas al entidades en las distintas ciudades del país que tienen convenio con la empresa para ejecutar los proyectos.

Para la muestra se seleccionará solamente al personal encargado del departamento de sistemas.

6.2.1 Fuentes de Recolección de la Información

Para el desarrollo de Auditoria se utilizaran las siguientes fuentes primarias:

- Primarias: la primera fuente de información será a través de las visitas a las instalaciones de la red de la empresa Panavias S.A. y mediante el contacto con el personal de sistemas. La recolección de la información será mediante entrevistas, cuestionarios y listas de chequeo, las cuales permitirán conocer el estado de la red de la empresa.

6.2.2 Técnicas e Instrumentos

Para esta investigación y la realización de la auditoria, se tiene previsto utilizar las siguientes herramientas y técnicas:

- Visitas técnicas: Se realizaran visitas técnicas para verificar aspectos físicos y administrativos de la red.
- Entrevistas al encargado de sistemas y a los usuarios de la red de datos
- Cuestionarios aplicados a los usuarios y encargado de sistemas.
- Listas de chequeo para determinar que controles existen dentro de la seguridad en la red.
- Pruebas de Penetración: se realizarán pruebas para identificar vulnerabilidades de la red de la empresa Panavias S.A.

6.3. METODOLOGÍA DE DESARROLLO

A continuación se muestran las actividades a realizar para conseguir el desarrollo de cada objetivo propuesto:

- Objetivo 1: Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la empresa Panavias S.A. para verificar las vulnerabilidades, riesgos y amenazas existentes.

- Realizar visitas técnicas o para conocer la infraestructura de la red de datos de la empresa.
- Solicitar la documentación de la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos.

- Objetivo 2. Seleccionar la norma que se va a aplicar, dominios, diseñar los instrumentos de recolección de información y pruebas aplicables a la red de datos de la empresa Panavias S.A.

- Seleccionar la normatividad y dominios a aplicar en la auditoria.
- Identificar y seleccionar los métodos y procedimientos necesarios.
- Realizar un plan de pruebas de penetración, donde se escogerán las más relevantes que se acojan al caso del proyecto con el fin de determinar

vulnerabilidades, riesgos y amenazas existentes en la seguridad de la red de la empresa Panavias S.A.

- Objetivo 3: Aplicar los instrumentos diseñados y ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a seguridad de la red de datos de la empresa Panavias S.A.

- Aplicar los métodos e instrumentos seleccionados.
- Aplicar las pruebas seleccionadas, donde siguiendo las fases del test de penetración se realizara reconocimiento, identificación y análisis de las vulnerabilidades encontradas.
- Realizar un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados y las pruebas de penetración.

- Objetivo 4: Elaborar un informe de los resultados obtenidos en la auditoria que contenga los hallazgos y recomendaciones para el diseño del SGSI que contenga los controles que permitan mitigarlos.

- Examinar y recopilar la información y los resultados obtenidos en las pruebas y en la auditoria.
- Presentar el informe de auditoría a la oficina de sistemas y la dirección de la empresa Panavias S.A.

7. DESARROLLO DEL PROYECTO

En una auditoria de sistemas, los papeles de trabajo son de vital importancia ya que son los formatos para la recolección de la información. Estos se preparan de acuerdo a los objetivos de la auditoria y se clasifican en dos tipos de archivos, el Archivo Permanente y el Archivo Corriente.

- Archivo Permanente: hace referencia a la documentación e información de naturaleza propia de la empresa a auditar.

- Archivo Corriente: hace referencia a los formatos e instrumentos propios para el desarrollo de la auditoria.

Para el desarrollo del presente proyecto, se clasificara en primer lugar el archivo permanente como los papeles o documentación propia de la empresa Panavias S.A. con el fin de identificar el estado actual de la seguridad de la red en su parte física y lógica como lo son la información del entorno organizacional, información de la oficina de sistemas, documentación de la red, etc que ayudan a la consecución del primer objetivo específico y en segundo lugar el archivo corriente que serán los papeles propios para el desarrollo del plan de auditoria como lo son el diseño de los instrumentos de recolección de información (cuestionarios y listas de chequeo) y el plan de pruebas aplicables para comprobar la seguridad de la red de datos de la organización, esto relacionado con el segundo objetivo específico del proyecto.

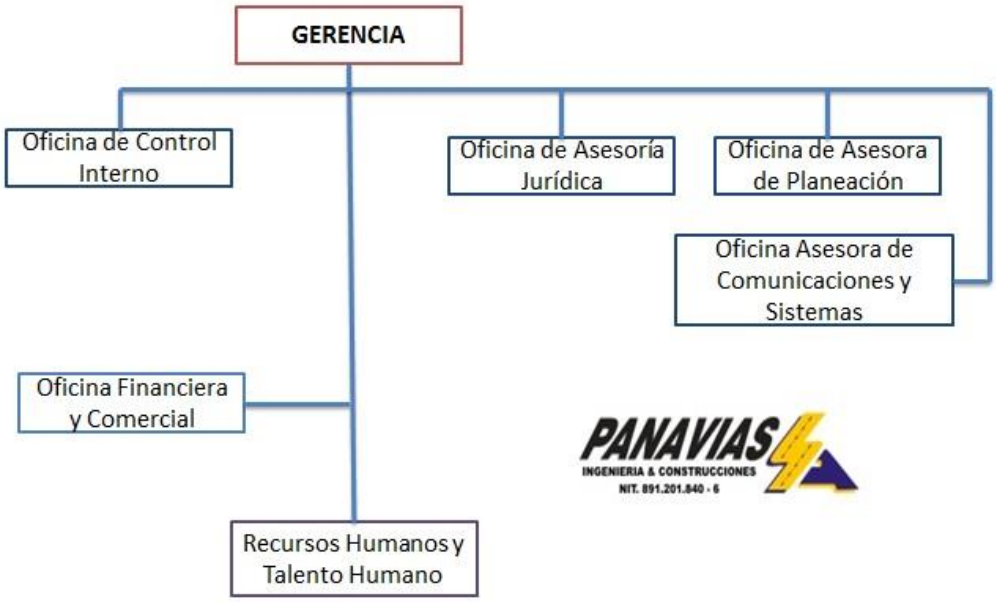
7.1. ARCHIVO PERMANENTE

Lo conforma la documentación de naturaleza propia de la organización. Es preciso conocer el entorno donde se va a realizar la auditoria, este específicamente se centra en la red de datos de la empresa Panavias S.A. En el archivo permanente se incluyen la información tanto del entorno organizacional de como del personal de sistemas, estructura y diagrama de la red y el uso de aplicaciones dentro de la misma como lo es Helysa-GW que es un software administrativo y de gestión de inventarios, archivos fijos y tangibles, nomina, presupuesto, contratación, etc, utilizado dentro de la empresa.

7.1.1. Entorno Organizacional

Panavias S.A. es una empresa que gestiona proyectos de ingeniería civil a través de la construcción de obras en la zona sur del país que incluye los departamentos de Nariño, Cauca y Valle del Cauca. Está conformada por la Gerencia que tiene a su cargo la oficina de Asesoría Jurídica, de Planeación, de Control Interno y la oficina asesora de Comunicaciones y Sistemas, donde en esta última, se realizara el desarrollo de la auditoria ya que en esta se administra el software Helysa-GW y la administración de la red de la empresa Panavias S.A.

Figura 1. Organigrama de la empresa Panavias S.A.



Fuente: Empresa Panavias S.A.

7.1.2. Oficina Asesora de Comunicaciones y Sistemas

La oficina de sistemas de la empresa Panavias S.A. la conforma un funcionario que es el ingeniero Holmes Zuñiga, quien está encargado de la supervisión de la infraestructura tecnológica de la organización. Entre sus funciones se encuentra tanto la inspección y mantenimiento de los equipos de cómputo y de comunicaciones como la administración de la red de la misma. Además de dar soporte técnico local al software administrativo utilizado en todos los equipos de cómputo, el Helysa-GW. También es el encargado de dar soporte a los servicios web de la empresa, aunque esta no presenta muchas funcionalidades, en un

futuro se piensa en actualizarla para realizar trámites en línea, como lo son la consulta de contratistas en la página web de la empresa como también la consulta de las constructoras y proyectos asociados a la misma.

El hecho de haber un solo funcionario encargado de todas las labores de la infraestructura tecnológica de la empresa, representa un gran problema, ya que la oficina no posee una estructura definida de distintos profesionales de sistemas que se encarguen de un área específica de ella.

Para el caso del presente proyecto, en la empresa Panavias S.A. no hay un administrador de red, que se encargue del mantenimiento y seguimiento de todas las funciones de la misma, lo cual conlleva a un descuido tanto en su parte física como lógica.

A continuación se relacionan las funciones del encargado de la oficina asesora de Comunicaciones y Sistemas, el ingeniero Holmes Zuñiga en la empresa Panavias S.A.

Tabla 2. Funciones del encargado de la oficina Asesora de Comunicaciones y Sistemas

Oficina Asesora de Comunicaciones y Sistemas
Profesional Universitario o Especializado
Encargado: Ingeniero Holmes Zuñiga
Dirigir y coordinar la marcha administrativa de la unidad a su cargo, para que cada uno de sus funcionarios laboren con eficacia y eficiencia, cumpliendo a cabalidad con sus funciones y con las normas legales que son de competencia en la empresa Panavias S.A.
Conocer y aplicar la normatividad vigente respecto a las leyes, acuerdos y decretos que rigen en materia de legalización del software, seguridad de la información y en general todo lo relacionado con informática y comunicaciones.
Coordinar el mantenimiento, capacitación y asesoría en el manejo tanto de los sistemas de información, aplicaciones que se manejen en la empresa Panavias S.A. como la usabilidad de los equipos de cómputo y afines.
Informar permanentemente al personal a su cargo acerca de políticas, normas, procedimientos, reglamentos de la administración y a las dependencias en la empresa Panavias S.A.
Informar a la gerencia sobre las eventualidades que se presenten en el normal desempeño de su cargo.

Tabla 2. Funciones del encargado de la oficina Asesora de Comunicaciones y Sistemas (Continuación)

Elaborar anteproyectos de presupuesto de su competencia teniendo en cuenta las nuevas tecnologías en Hardware y Software y las necesidades de cada una de las dependencias de la administración.
Presentar informes periódicos y los que le sean solicitados por la gerencia o jefe inmediato, oportunamente.

Fuente: Empresa Panavias S.A.

7.1.3. Visitas Técnicas

Para el reconocimiento previo al área de la red de la empresa Panavias S.A. en primer lugar se solicita realizar visitas técnicas guiadas, con el objetivo de conocer el estado de la seguridad física y lógica de la red, controles de acceso al área de red, funciones y características de los servidores, software y sistemas de información alojados en los servidores, procedimientos de copias de seguridad, etc.

7.1.3.1. Primera Visita Técnica

Se solicita la documentación relacionada con la oficina asesora de comunicaciones y sistemas como lo son el Inventario de activos, Diagramas de red, Manual de procedimientos, etc. Además se realiza una entrevista previa al encargado de la oficina, con el objetivo de conocer generalmente el área de comunicaciones y sistemas. En la entrevista previa, se realizan las siguientes preguntas:

- ¿Qué características tiene la red de la empresa Panavias S.A.?
- ¿Qué características tiene el servidor del área de redes y comunicaciones de la empresa?
- ¿Existen herramientas para la administración de la red como mapeo de redes, monitorización y control de tráfico?
- ¿Cómo se encuentra distribuido el equipo de red de la empresa Panavias S.A.?
- ¿Se realiza mantenimiento periódico a los equipos de red?
- ¿Qué aplicaciones se manejan dentro de la empresa?
- ¿Se han realizado previamente auditorias de seguridad informática?

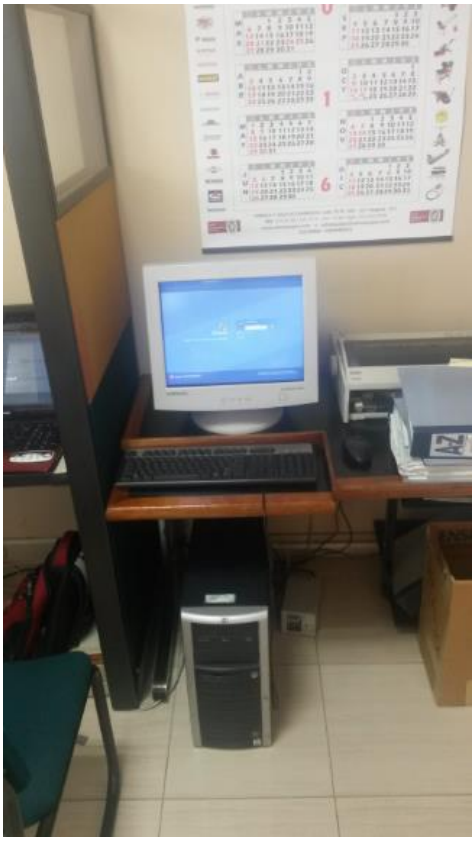
Cabe mencionar que en la fase de ejecución de la auditoria, se aplicaran los instrumentos de recolección de la información como lo son entrevistas para conocer la seguridad lógica y física de la red, listas de chequeo y cuestionarios basados en la NTC/ISO/IEC 27002:2013 para conocer a profundidad las vulnerabilidades y amenazas en la red de la empresa Panavias S.A.

7.1.3.2. Segunda Visita Técnica

Mediante recorridos guiados con el personal encargado del área de redes y comunicaciones, se realizó visitas técnicas con el objetivo de identificar amenazas y vulnerabilidades a los equipos de cómputo y de red de la empresa Panavias S.A.

En primer lugar, se visitó el área donde se encuentra alojado el servidor, este se encuentra en la entrada a la oficina administrativa de Panavias S.A. Se identifica que no hay control de acceso al área donde se encuentra a este y cualquier empleado puede acceder a él.

Figura 2. Servidor de la empresa Panavias S.A.



Fuente: Auto

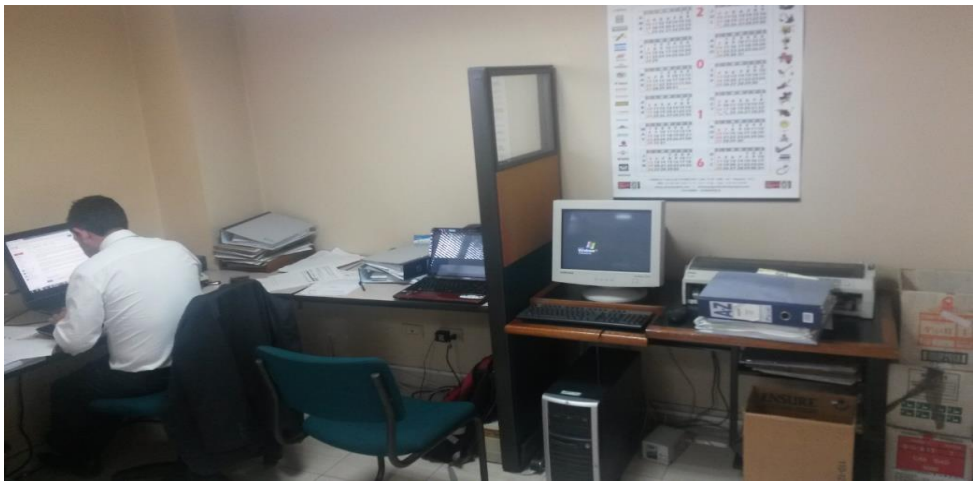
Figura 3. Acceso al Servidor de la empresa Panavias S.A.

Fuente: Autor

Como se muestra en la figura 3, el acceso donde se encuentra el servidor se encuentra a un lado de la oficina de archivo de la empresa, en donde además se han dejado folios en el espacio que le corresponde al servidor. Se identifica que este no se encuentra en el área que corresponde, la oficina de comunicaciones y sistemas, lo que indica que no se han establecido controles de acceso y ubicación de los dispositivos de cómputo en la empresa. Además no hay controles de seguridad como cámaras de vigilancia, los equipos de cómputo y de red son vulnerables a robo.

Como se muestra en la figura 4, el servidor limita por el otro lado directamente con la oficina financiera y comercial de la empresa, solo está separado por un panel de cubículo. No se encuentra en la oficina que le corresponde, el área de comunicaciones y sistemas.

Figura 4. Panorámica del servidor con oficina financiera y comercial



Fuente: Autor

El acceso a la oficina de comunicaciones y sistemas donde se encuentra el equipo de red no tiene protección lo cual el vulnerable a accesos no autorizados, lo cual genera que se genere ataques que atenten en contra de la integridad de los equipos, robos, daño de los dispositivos como también de los medios de transmisión. El acceso consta de una puerta panel donde la llave no tiene seguro. Esto se muestra en la siguiente figura:

Figura 5. Acceso a la oficina de comunicaciones y sistemas

Fuente: Autor

En la oficina de sistemas y comunicaciones, el equipo de red como switches y cableado no se encuentra organizado ni distribuido debidamente en el rack de comunicaciones. Esto representa una gran falla en cuanto a la distribución del equipo de red en la empresa Panavias S.A. Los switchs no se encuentran articulados debidamente al armario y no hay una buena administración del cableado, como también se depositan en el rack, cableado auxiliar y cajas lo que deja en claro que no se ha realizado un debido mantenimiento como se muestra en la figura 6. En la figura 7 se muestra un router sobre el equipo de la oficina de comunicaciones y sistemas.

Figura 6. Rack de Comunicaciones

Fuente: Autor

Figura 7. Router de la oficina de comunicaciones y sistemas

Fuente: el autor

El router para la conexión inalámbrica (WiFi) no se encuentra en el lugar adecuado para brindar una buena cobertura ya que se encuentra debajo de la mesa de un cubículo en la oficina financiera y comercial como se muestra en la figura 8. Este debería estar ubicado en un lugar alto de la pared de la oficina para que brinde una óptima conexión. De acuerdo a algunos funcionarios de la empresa, la conexión inalámbrica del lugar no es la mejor, debido a que nunca se ha ubicado el router para conexión inalámbrica en un lugar estratégico.

Figura 8. Router de conexión inalámbrica (WiFi)

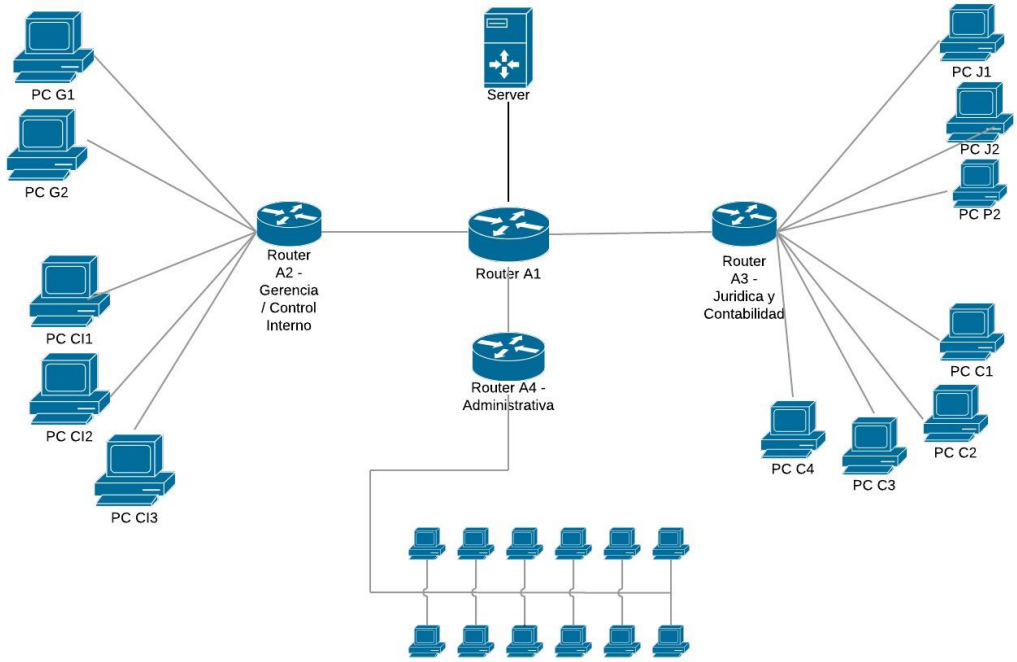
Fuente: el autor

De acuerdo a lo observado en la segunda visita técnica, los equipos de red se encuentran expuestos a gran cantidad de amenazas y vulnerabilidades, debido a la desorganización y la falta de controles, el cual puede afectar el correcto funcionamiento y calidad de vida de estos. La mala administración en el rack de comunicaciones dificulta el ordenamiento correcto del equipo de red, además de la mala distribución de los routers afectan el correcto funcionamiento de las conexiones inalámbricas como también la ausencia de controles de acceso al servidor y a la oficina de sistemas y comunicaciones.

El proceso de pruebas técnicas en la red lógica de la empresa Panavias S.A., se realizara en la tercera fase de la auditoria, la fase de ejecución, donde se utilizaran herramientas de testeo para identificar y analizar las vulnerabilidades existentes en esta.

7.1.4. Red de datos de la empresa Panavias S.A.

Figura 9. Diagrama de red



Fuente: Empresa Panavias S.A.

La estructura de la red de la empresa Panavias S.A. está conformada por una topología en estrella, la cual esta soportada por un equipo donde se aloja el servidor que opera bajo Windows Server 2003, el cual es una versión para servidor desactualizada, en él se encuentra el servidor de archivos y el servidor web. Esto representa una gran amenaza ya que al tener un servidor desactualizado es fácilmente vulnerable a múltiples ataques informáticos.

En su distribución de red, cuenta con cuatro routers, uno el principal que alimenta a los demás ubicados en la oficina de Comunicaciones y Sistemas. Los otros routers se encuentran distribuidos por cada oficina de la empresa comunicando a los equipos que correspondan a cada oficina.

Una característica de la red de Panavias S.A. es que no se encuentra segmentada, esto quiere decir que solo hay una red local para toda la empresa y no una red dividida o por cada dependencia que comunique a los equipos que le corresponda.

La empresa cuenta además con su página web en el dominio http://panavias.com/, el cual cuenta con información básica de la empresa y esperan actualizarla en un futuro para presentar un portal web más funcional.

Las direcciones tanto de la red local, como del host, las cuales se utilizaran para realizar las pruebas de seguridad de la presente auditoria son:

- IP Red local de Panavias S.A.: 186.116.250.224
- IP Host (http://panavias.com): 190.8.176.106

7.1.5. Helysa-GW Software Administrativo y de Gestión

El software Helysa-GW es una herramienta administrativa y operativa regida bajo los parámetros de la Ley 1314 de 2009 además de estar certificada por las NIIF (Normas Internacionales de Información Financiera). Se caracteriza por ser una herramienta sencilla, confiable y de fácil usabilidad, desarrollada en Colombia y actualmente es un gran referente de la industria del software con presencia directa en el país y se encuentra en proceso de expansión por el Caribe (República Dominicana), Centro América (México) y Sudamérica (Ecuador y Chile).

Helysa-GW ha sido un gran referente para la empresa Panavias S.A. ya que lo ha utilizado a lo largo de 10 años, en sus labores administrativas y en él se resguardan los activos de información más relevantes de la organización. Actualmente se encuentra en proceso de actualización a Helisa Cloud, el cual es un servicio en la nube que permite gestionar la aplicación mediante un servicio RDP Web lo cual permitirá la disponibilidad de la información en diferentes dispositivos como móviles, portátiles, tablets equipos de escritorio, etc

Helysa-GW dispone de una serie de opciones para llevar a cabo la preparación y el cálculo del impuesto diferido, donde se puede definir cada uno de los ítems y sus correspondientes valores en la contabilidad local que, de acuerdo a las normas fiscales, estos deberán ser comparados y analizados contra los valores en la contabilidad NIIF y así determinar las diferencias temporales y permanentes. Una vez identificadas estas diferencias y de acuerdo a las tasas correspondientes

podrán ser calculados y registrados en libros los activos y/o pasivos (de ser necesario) por impuestos diferidos así como su impacto en resultados.[15]
El software cuenta con los siguientes módulos:

- Contabilidad general
- Cuentas por cobrar
- Cuentas por pagar
- Administración de terceros
- Renta y complementarios
- Centros de costo
- Control de negocios
- Diseño de formatos para documentos y cheques.
- Análisis financiero
- Inversiones
- Obligaciones financieras

Además cuenta con la extensión llamada Helisa/XBRL (Extensible Business Reporting Lenguage) el cual permite los siguientes módulos:

- Control de nómina y gestión humana
- Liquidación de pagos y reportes
- Manejo de cartillas

También cuenta con el administrador de Talento Humano KORA, el cual permite la gestión de:

- Inventarios
- Activos fijos e intangibles
- Importaciones
- Presupuesto

[15] Helysa NIFF administrador. Disponible en: http://www.guiadesolucionestic.com/sistemas-de-informacion/gestion-financiera/software-contable/1846-helisa-niif-administrador

7.2. ARCHIVO CORRIENTE

Lo conforman los papeles de trabajo para el desarrollo de la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. En él se incluye el Plan de Auditoria que contiene las actividades que serán desarrolladas en el proceso del actual proyecto y el Programa de Auditoria, donde se seleccionaran la normatividad y los dominios propicios para el desarrollo de los instrumentos de recolección de la información, como lo son los cuestionarios y listas de chequeo. Por último el Plan de Pruebas aplicables para comprobar el estado de la seguridad de la red de datos de la organización.

7.2.1. Plan de Auditoria

En el plan de auditoria se especifica el memorando de planeación, donde en él se muestran los objetivos de la auditoria, el alcance de esta, la metodología a utilizar los recursos y el tiempo para llevar a cabo el proceso a cabalidad.

Objetivo General de la Auditoria

Desarrollar una auditoría a la seguridad de la red de datos que permita diseñar un sistema de gestión de seguridad informático que contenga los controles y procedimientos para la red en la empresa Panavias S.A.

Objetivos Específicos de la Auditoria

- Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la empresa Panavias S.A. para verificar la existencia de las vulnerabilidades y amenazas existentes en los activos informáticos y de información.

- Seleccionar la norma que se va a aplicar, dominios, diseñar los instrumentos de recolección de información y pruebas aplicables a la red de datos de la empresa Panavias S.A.

- Aplicar los instrumentos diseñados y ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a seguridad de la red de datos de la empresa Panavias S.A.

- Elaborar un informe de los resultados obtenidos en la auditoria que contenga los hallazgos y recomendaciones para el diseño del SGSI que contenga las políticas y procedimientos que permitan mitigarlos.

Clasificación de la Auditoria

- Auditoria Externa: Ya que el auditor a realizar el proceso no tiene vínculo laboral con la empresa Panavias S.A. y se aplicaran sin restricción distintos tipos de técnicas, métodos y herramientas para el desarrollo de la misma.

Tipo de Auditoria Informática

- Auditoria de Seguridad Informática
- Auditoria Informática de Comunicaciones y Redes

Alcance de la Auditoria

Para evaluar la seguridad de la red de datos de la empresa Panavias S.A. se tendrá en cuenta las siguientes etapas:

- Aplicación de instrumentos de recolección de la información.
- Aplicación de Pruebas de Penetración y Ethical Hacking.
- Realización de un Análisis y Gestión de riesgos informáticos.

Para la aplicación de los instrumentos de recolección de la información se tendrá en cuenta:

- Selección de la normatividad y dominios a aplicar.
- Diseño y aplicación de cuestionarios.
- Diseño y aplicación de listas de chequeo.

Para la aplicación de las pruebas de penetración, se tendrá en cuenta las fases del Pentesting (Ethical Hacking):

- Fase de recolección o reconocimiento.
- Fase de análisis de vulnerabilidades.

Para la realización del análisis y gestión de riesgos de los hallazgos y vulnerabilidades encontradas en los instrumentos de recolección de la información y las pruebas de penetración, se tendrá en cuenta:

- Análisis de riesgos de acuerdo a las vulnerabilidades encontradas
- Matriz de riesgos
- Gestión de riesgos

Metodología de la Auditoria

La metodología se realizara de acuerdo a las fases de la auditoria que son, la fase de reconocimiento, fase de planeación, fase de ejecución y la fase de resultados, esto en relación a los cuatro objetivos específicos del proyecto.

Para la primera fase, la fase de reconocimiento, se realizaran las siguientes actividades:

- Realizar visitas técnicas o para conocer la infraestructura de la red de datos de la empresa.
- Solicitar la documentación de la red para identificar puntos de acceso, topología, la distribución de los equipos y servidores, las características de los equipos.

Para la fase de planeación, se realizaran las siguientes actividades:

- Seleccionar la normatividad y dominios a aplicar en la auditoria.
- Identificar y seleccionar los métodos y procedimientos necesarios.
- Realizar un plan de pruebas de penetración, donde se escogerán las más relevantes que se acojan al caso del proyecto con el fin de determinar vulnerabilidades, riesgos y amenazas existentes en la seguridad de la red de la empresa Panavias S.A.

Para la fase de ejecución de la auditoria, se realizaran las siguientes actividades:

- Aplicar los métodos e instrumentos seleccionados.
- Aplicar las pruebas seleccionadas, donde siguiendo las fases del test de penetración se realizara reconocimiento, identificación y analizando de las vulnerabilidades encontradas.

- Realizar un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados y las pruebas de penetración.

Para la última fase de la auditoria, la fase de resultados, se realizaran las siguientes actividades:

- Examinar y recopilar la información y los resultados obtenidos en las pruebas y en la auditoria.
- Presentar el informe de auditoría a la oficina de sistemas y la dirección de la empresa Panavias S.A.

Talento Humano

La auditoría a la seguridad de la red de datos de la empresa Panavias S.A. se llevara a cabo por el estudiante de Especialización de Seguridad Informática – UNAD, Ing. Jesús German Cortes Camacho. También se contará con la colaboración del ingeniero Holmes Zúñiga, coordinador de la oficina de sistemas de la organización.

Recursos Físicos y Tecnológicos

La auditoría se realizara en la oficina de sistemas de la empresa Panavias S.A. donde se encuentra el área de redes y comunicaciones.

Para recursos relacionados con hardware, se utilizara:

- 2 computadores portátiles.
- Dispositivos de almacenamiento.
- Dispositivos periféricos (impresora y escáner).
- Celular Smartphone o Tablet.
- Papelería.

Para recursos relacionados con el software, se utilizara:

- Herramientas en línea para realizar pruebas de penetración y Ethical Hacking.
- Software Libre para realizar pruebas de penetración y Ethical Hacking, para este caso Kali Linux, el cual cuenta con:
- Herramientas para recolección de información.

- Herramientas para análisis de vulnerabilidades.
- Herramientas de explotación.

Recursos Financieros

Tabla 3. Presupuesto – Plan de Auditoria

Ítem	Precio Total
Computador portátil: cantidad 2	$4’000,000
Impresora	$400,000
Escáner	$300,000
Papelería	$700,000
Memoria USB 32GB	$80,000
Celular Smartphone o Tablet (Cámara fotográfica y de video, grabadora de voz, llamadas telefónicas)	$1’200,000
NTC/ISO/IEC 27001:2013	$53,000
NTC/ISO/IEC 27002:2013	$92,000
Ingeniero ejecutor del proyecto	$3’800,000
Total Presupuesto	**$10’625.000**

Fuente: Autor

Documentos y Manuales Técnicos

- NTC-ISO-IEC 27001:2013
- NTC-ISO-IEC 27002:2013

Cronograma de Actividades

Tabla 4. Cronograma de Actividades – Plan de Auditoria

Actividades		Mes 1				Mes 2				Mes 3				Mes 4			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Fase: Reconocimiento de la Auditoria	Realización de visitas técnicas																
	Recolección de documentación de la red																
Fase: Planeación de la Auditoria	Realización de los instrumentos de recolección de la información																
	Realización del Plan de Pruebas de Penetración																
Fase: Ejecución de la Auditoria	Aplicar los instrumentos seleccionados																
	Ejecución de Pruebas de Penetración																
	Realización del Análisis y gestión de riesgos																
Fase: Resultados de la Auditoria	Examinar y recopilar la información de los resultados de acuerdo a la normatividad																
	Preparar y presentar informe de Auditoria a Panavias S.A.																
	Preparar documento de grado																

Fuente: Autor

7.2.2. Programa de Auditoria

A continuación se define la normatividad y los dominios a aplicar para diseñar los instrumentos de recolección de información. Para el caso del presente proyecto se seleccionara la NTC-ISO-27001:2013 y la NTC-ISO-27002:2013

Para la elaboración de las entrevistas, se toman aspectos relacionados con los controles tanto para la seguridad física como para la seguridad lógica de la red.

Para la seguridad física se tienen en cuenta los siguientes controles:

- Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados.
- Controles de utilización de los equipos de red y de comunicaciones, previniendo accesos inadecuados.
- Controles para la protección y tendido adecuado de cables y líneas de comunicaciones.
- Controles para perdida de la información y desastres.

Para la seguridad lógica se tienen en cuenta los siguientes controles:

- Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red.
- Control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas.
- Controles para asegurar que las transmisiones van solamente a usuarios autorizados.
- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.
- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.
- Controles de Seguridad en la Red.

De la normatividad seleccionada, se escogen para el desarrollo de la auditoria aquellos dominios y subdominios directamente relacionados con la seguridad en redes, los cuales corresponden a:

- A9. CONTROL DE ACCESOS

- 9.1 Requisitos de negocio para el control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

- 9.4 Control de acceso a sistemas y aplicaciones.
- 9.4.1 Restricción del acceso a la información.

- A13. SEGURIDAD EN LAS TELECOMUNICACIONES

- 13.1 Gestión de la seguridad en las redes.
- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

Además se tendrá en cuenta aspectos relacionados con los siguientes dominios, estos son los dominios indirectamente relacionados:

- A5. Políticas de la Seguridad de la Información

- 5.1. Directrices establecidas por la dirección para la seguridad de la información.
- 5.1.1. Políticas para la seguridad de la información.
- 5.1.2. Revisión de las políticas para la seguridad de la información.

- A6. Organización de Seguridad de la Información

- 6.1. Organización Interna.
- 6.1.1 Roles y responsabilidades para la seguridad de la información.

- A11. Seguridad Física y del Entorno

- 11.2.1. Ubicación y protección de los equipos.
- 11.2.3. Seguridad en el cableado

El formato que contiene el programa de auditoria realizado en la empresa Panavias S.A., se incluye en el Anexo A – Formatos y Documentación de la Auditoria, donde se denomina “Panavias_ProgramadeAuditoria.”

7.2.3. Plan de Pruebas de Penetración

Para el plan de pruebas, se seleccionarán herramientas tanto en línea como de software libre para realizar pruebas de testeo, intrusión y seguridad informática, para este caso se seleccionara el software Kali Linux versión 2016.1, que permitirá realizar pruebas para conocer el estado de la red de la empresa Panavias S.A. identificando y analizando las vulnerabilidades presentes en esta.

Tabla 5. Plan de Pruebas

Herramienta	Descripción
1. Fase de Reconocimiento	
CentralOps.net (https://centralops.net/)	Es un servicio en línea que ofrece herramientas para testeo y auditoria de redes. Para la auditoria a la seguridad de la red de la empresa Panavias S.A. se utilizara dos herramientas: 1. Domain Whois record 2. Network Whois record Estas permitirán recolectar información tanto del host como de la red local de la empresa.
Nmap	Nmap, en general, es una de las herramientas fundamentales en una auditoria de redes. Con ella se realizara el mapeo y escaneo de los servicios y procesos de la red de Panavias S.A.
ZenMap	Herramienta grafica de nmap, la cual permite realizar escaneos sigilosos además de graficar las topologías de red y las pistas de paquetes enviados en una red (traceroute).
2. Fase de Análisis de vulnerabilidades	

Tabla 5. Plan de Pruebas (Continuación)

OWASP-ZAP	Permite el análisis de vulnerabilidades en un servicio web. Con ella se realizara el análisis de directorios y archivos presentes en el host de la empresa Panavias S.A.
Nessus	Herramienta fundamental para el análisis de vulnerabilidades. Permitirá realizar un análisis de tanto del host como de la red local de la empresa Panavias S.A.
UpGuard	Permitirá realizar un análisis detallado de vulnerabilidades tanto del host como de la red local de la empresa Panavias S.A.
JumpStart	Herramienta que permite auditar y explotar vulnerabilidades en redes inalámbricas (WEP/WPA/WPA2)

Fuente: Autor

7.2.4. Aspectos de la Seguridad Física y Lógica de la red de la empresa Panavias S.A.

De acuerdo a las visitas técnicas realizadas al área de la red de la empresa Panavias S.A. en conjunto con la información obtenida en la primera fase de la auditoria, la fase de reconocimiento, permiten establecer una vista preliminar de la infraestructura de la red en cuanto a su seguridad tanto física como lógica. De igual manera, se identificaron las primeras vulnerabilidades y posibles amenazas que pueden afectar la disponibilidad, confidencialidad e integridad de los activos informáticos de la red.

También cabe mencionar que la empresa no cuenta con documentación en relación a manual de procedimientos, inventarios de los equipos de red, documentación referente a procesos y procedimientos y registro de problemas e incidentes.

En consecuencia, a manera de diagnóstico, se encontraron los siguientes aspectos relacionados con la seguridad física de la red en la empresa Panavias S.A.

- La red no se encuentra segmentada.
- No existe un administrador de red.
- No existe mantenimiento periódico de los equipos de red y de cómputo.
- Accesos inadecuados al área de redes y comunicaciones.
- Equipo físico de red (cableado TCP, routers) que ha sido utilizado durante bastante tiempo y no se cambiado, tiende a convertiste en caduco, dificultando el correcto funcionamiento de estos.
- El área de red no se encuentra separada de las demás áreas o departamentos de la empresa.
- No existen controles para la utilización de los equipos de red como etiquetados o inventarios.

En cuanto a la seguridad lógica, se encontraron los siguientes aspectos:

- Desconocimiento de la parte lógica de la red ya que nunca se realizaron auditorias de seguridad informática que permitan identificar vulnerabilidades y corregirlas.
- Servidor de red desactualizado.
- Versión de la aplicación Helysa GW desactualizada.
- No existen controles de seguridad en la red.
- La empresa desconoce el uso y no posee herramientas de seguridad informática para la red como lo son herramientas de mapeo y registro de tráfico como también de técnicas de criptografía para protección de los datos sensibles.
- No se cambian las contraseñas periódicamente tanto del software de red como de la aplicación Helysa GW.

Estos aspectos diagnosticados en esta etapa preliminar, servirán como base para desarrollar los instrumentos de recolección de la información en la fase de planeación de la auditoria.

7.2.5. Diseño de Instrumentos

Para el desarrollo de la auditoria a la red de datos de la empresa Panavias S.A., se emplearan instrumentos para la recolección de información e identificar vulnerabilidades como lo son, entrevistas; dos formatos para entrevistas, una para evaluar y conocer la seguridad física y otro para la seguridad lógica de la red de datos de la empresa. También se emplearan listas de chequeo, de acuerdo a los

dominios directamente e indirectamente relacionados con la auditoria. Estas listas de chequeo se diseñaran de acuerdo a la normatividad ISO/IEC 27002:2013. Se emplearan cuestionarios de control para determinar el grado de exposición de los riesgos encontrados y las guías de hallazgos para documentar los riesgos que ayudaran en la elaboración del informe final de auditoria.

7.2.5.1. Formatos para Entrevistas

Se realizan dos formatos para evaluar y conocer la seguridad física y lógica de la red de datos de la empresa Panavias S.A.

El primer formato, se relaciona con la seguridad física de la red de datos. Este contiene:

- Encabezado del formato: este contiene el logo de la empresa a auditar, el nombre del proceso de la auditoria, el logo de la entidad universitaria y la versión del formato.
- Elaborado por: responsable o grupo auditor encargado de llevar la auditoria.
- Fecha: registro del día, mes y año en que se diligencio el formato.
- Respondido por: es la persona a quien se realiza la entrevista.
- Área: es el área auditada que será objeto de estudio.
- Objetivo: es el objetivo con el que se lleva a cabo para realizar la entrevista, que en este caso es conocer acerca de la administración de la red en cuanto a su seguridad física en la empresa Panavias S.A.

El segundo formato, se relaciona con la seguridad lógica de la red de datos. Este contiene:

- Encabezado del formato: este contiene el logo de la empresa a auditar, el nombre del proceso de la auditoria, el logo de la entidad universitaria y la versión del formato.
- Elaborado por: responsable o grupo auditor encargado de llevar la auditoria.
- Fecha: registro del día, mes y año en que se diligencio el formato.
- Respondido por: es la persona a quien se realiza la entrevista.
- Tipo de registro: hace referencia al tipo de instrumento que se aplica.
- Área: es el área auditada que será objeto de estudio.

- Objetivo: es el objetivo con el que se lleva a cabo para realizar la entrevista, que en este caso es conocer acerca de la administración de la red en cuanto a su seguridad lógica en la empresa Panavias S.A.

Tabla 6. Formato para entrevistas

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**			
Respondido por					

ÁREA
Red de datos de la empresa Panavias S.A.

FORMATO DE ENTREVISTA PARA EVALUAR LA SEGURIDAD FISICA Y LOGICA DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.
Objetivo:

1. Control 1
1.1. ¿Pregunta 1.1?
1.2. ¿Pregunta 1.2?
1.3. ¿Pregunta 1.3?
2. Control 2
2.1. ¿Pregunta 2.1?
2.2. ¿Pregunta 2.2?

Tabla 6. Formato para entrevistas (Continuación)

2.3. ¿Pregunta 2.3?
3. Control 3
3.1. ¿Pregunta 3.1?
3.2. ¿Pregunta 3.2?
3.3. ¿Pregunta 3.3?

Fuente: Autor

Estos formatos se incluyen en el Anexo A – Formatos y Documentación de la Auditoria, donde se denominan “Formato_EntrevistaSeguridadFisica” para el formato de evaluación de la seguridad física y “Formato_EntrevistaSeguridadLogica”, para el formato de evaluación de la seguridad lógica de la red de datos de la empresa Panavias S.A.

7.2.5.2. Formatos para Listas de chequeo

Para el diseño de las listas de chequeo, se tiene en cuenta los dominios directamente relacionados con el objetivo de la auditoria que son el A9. Control de Acceso y el dominio A13. Seguridad en las Telecomunicaciones y aspectos de los dominios indirectamente relacionados, los cuales son A5. Políticas de Seguridad de la Información, A6. Organización de la Seguridad de la Información y el dominio A11. Seguridad Física y del Entorno

El formato de lista de chequeo para verificar los controles de los dominios a auditar, contienen los siguientes ítems:

- Encabezado del formato: este contiene el logo de la empresa a auditar, el nombre del proceso de la auditoria, el logo de la entidad universitaria y la versión del formato.

- Responsable: autor o grupo auditor encargado de llevar la auditoria.
- Fecha: registro del día, mes y año en que se diligencio el formato.
- Tipo de registro: hace referencia al tipo de instrumento que se aplica. Contiene el dominio y los subdominios a evaluar.
- Objetivo: contiene los controles de los subdominios a verificar, tomados directamente de la normatividad.
- Pregunta: espacio donde se incluye las preguntas sobre los controles a verificar en la auditoria.
- Si, No, N/A: respuestas posibles a cada una de las preguntas.

Tabla 7. Formato para listas de chequeo

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable		**Fecha**			

ICONTEC	**LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013** **DOMINIO** **Subdominio 1** **Subdominio 2**		ISO
Objetivo:			
Objetivo del dominio **Controles:** Objetivo subdominio 1 Objetivo Subdominio 2			

Descripción del dominio a evaluar			
Ítem	**Si**	**No**	**N/A**
Subdominio 1			
¿Pregunta 1.1?			
¿Pregunta 1.2?			
¿Pregunta 1.3?			

Tabla 7. Formato para listas de chequeo (Continuación)

Subdominio 2			
¿Pregunta 2.1?			
¿Pregunta 2.2?			
¿Pregunta 2.3?			

Fuente: Autor

7.2.5.3. Formatos para Cuestionarios

Los cuestionarios de control se diseñan para cada uno de los procesos evaluados en la auditoria, lo que permitirá hacer un análisis de resultados y obtener el nivel de riesgo asociado a cada uno de dichos procesos.

El cuestionario de control cuantitativo permite dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su nivel de vulnerabilidad. En ellos, se asigna un puntaje dependiendo de la importancia del ítem evaluado en el proceso, el cual va en una escala de menor a mayor, de 1 a 5, donde 1 significa que no es importante tener el control para el auditor y 5 significa que es importante que se tenga el control. Luego se suman los puntajes de las respuestas del SI, NO y N/A, por último se suman el total de los puntajes del cuestionario.

El porcentaje de riesgo, hace referencia a la probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre más alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

El cálculo del porcentaje de riesgo, se realiza de la siguiente forma:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente escala:

- 1% - 30% = Riesgo Bajo
- 31% - 70% = Riesgo Medio
- 71% - 100% = Riesgo Alto

El formato para los cuestionarios de control que se aplican a cada uno de los procesos o dominios establecidos para el desarrollo de la auditoria, estos son los dominios directamente e indirectamente relacionados. El formato de cuestionario de control contiene los siguientes ítems:

- Encabezado del formato: este contiene el logo de la empresa a auditar, el nombre del proceso de la auditoria, el logo de la entidad universitaria, la referencia del formato (AP Auditoria Panavias, CC Cuestionario de Control, 000 hace referencia al serial del documento) y la versión del formato.
- Elaborado por: responsable o grupo auditor encargado de llevar la auditoria.
- Fecha: registro del día, mes y año en que se diligencio el formato.
- Respondido por: es la persona a quien se realiza el cuestionario.
- Dominio: Dominio de la ISO/IEC 27002:2013 auditado.
- Proceso: Son los subdominios del dominio auditado.
- Objetivo: contiene los controles de los subdominios a verificar, tomados directamente de la normatividad.

De acuerdo a lo anterior, el formato para los cuestionarios de control para evaluar cada uno de los procesos de la auditoria, según la normatividad, corresponde a la siguiente plantilla:

Tabla 8. Formato para cuestionarios de control

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-CC-000 Versión 1.0

Elaborado por		**Fecha**			
Respondido por					

Cuestionario de Control	
Dominio	
Proceso	
Objetivo del control	

Tabla 8. Formato para cuestionarios de control (Continuación)

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:				
Pregunta	**Si**	**No**	**N/A**	**Observaciones**
TOTALES				
PUNTAJE TOTAL				

Fuente: Autor

El anterior formato, se incluye en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Formato_CuestionarioControl”.

7.2.5.4. Formatos para Hallazgos

En la guía de hallazgos, se registran los riesgos confirmados a través de las pruebas y lo encontrado durante la ejecución de los instrumentos, lo cual ayuda a la elaboración del informe final de auditoria.

El formato para las guías de hallazgos, donde se registraran lo encontrado durante la auditoria, contiene los siguientes ítems:

- Encabezado del formato: este contiene el logo de la empresa a auditar, el nombre del proceso de la auditoria, el logo de la entidad universitaria, la

referencia del formato (AP Auditoria Panavias, GH Guía de Hallazgos, 000 hace referencia al serial del documento) y la versión del formato.

- Dominio: dominio de la ISO/IEC 27002:2013 al cual corresponde el hallazgo.
- Proceso: subdominio de la ISO/IEC 27002:2013 al cual corresponde el hallazgo.
- Descripción: se exponen los detalles del hallazgo.
- Riesgo: descripción del riesgo que puede ocasionar el hallazgo.
- Nivel de riesgo: valor cualitativo o cuantitativo del riesgo.
- Recomendaciones: se hace referencia a las descripciones de los controles. correctivos y preventivos posibles que ayuden a mitigar el riesgo o hallazgo.

De acuerdo a lo anterior, el formato para las guías de hallazgo donde se registrara lo encontrado y será la base del informe final de la auditoria, corresponde a la siguiente tabla:

Tabla 9. Formato para guía de hallazgos

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-GH-000 Versión 1.0

Guía de Hallazgos	
Dominio/Proceso	
Subdominio	
Riesgo	

Descripción del Hallazgo
Riesgo – Nivel de Riesgo (Causas / Efectos)

Tabla 9. Formato para guía de hallazgos (Continuación)

Recomendaciones – Acciones Correctivas
Evidencias del Hallazgo

Fuente: Autor

El anterior formato, se incluye en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Formato_GuiaHallazgos”.

7.3. EJECUCIÓN DE PRUEBAS DE PENETRACIÓN

De acuerdo a las herramientas seleccionadas en el plan de pruebas del programa de auditoria, se ejecutaran para determinar las vulnerabilidades y amenazas existentes al host y la red local de la empresa Panavias S.A. En primer lugar se hará el proceso de recolección de la información de los puntos a verificar Posteriormente se identificaran vulnerabilidades existentes y por último se analizaran estos hallazgos.

Los puntos a verificar donde se realizaran las pruebas de penetración en la red son los siguientes:

- Red local de Panavias S.A. Dirección IP: 186.116.250.224
- Host (http://panavias.com). Dirección IP: 190.8.176.106

7.3.1. Recolección de Información

Esta es la primera etapa del proceso de pentesting, donde se realizara la recolección de la información del objetivo y esta será la base para las siguientes fases del test de penetración a la red. Para esta primera fase, se utilizara la herramienta CentralOps.net.

7.3.1.1. Recolección de información con CentralOps.net

Es un escáner online que permite recolectar información acerca de los dominios, información de la red y los nombres DNS del objetivo. Para este caso, se aplicara la herramienta en los dos puntos a evaluar, en la red local y el host de la empresa Panavias S.A.

- **Recolección de información de la red local**

Se escanea la dirección IP en CentralOps.net, correspondiente a la red local de la empresa Panavias como se muestra en la figura 10:

Figura 10. Escaneo de la Red Local en CentralOps.net

Fuente: Autor

Los resultados arrojados por CentralOps.net luego del escaneo a la red local de la empresa Panavias S.A. muestran lo siguiente:

```
Network Whois record
Queried whois.lacnic.net with "186.116.250.224"...

inetnum:     186.116/14
status:      allocated
aut-num:     N/A
owner:       COLOMBIA TELECOMUNICACIONES S.A. ESP
ownerid:     CO-CTSE-LACNIC
responsible: Administradores Internet
address:     Transversal 60, 114, A 55
address:     N - BOGOTA - Cu
country:     CO
phone:       +57 1 5339833 []
owner-c:     CTE7
tech-c:      CTE3
abuse-c:     CTE3
inetrev:     186.116/15
nserver:     DNS5.TELECOM.COM.CO
nsstat:      20161020 AA
nslastaa:    20161020
nserver:     DNS.TELECOM.COM.CO
```

```
nsstat:      20161020 AA
nslastaa:    20161020
created:     20110325
changed:     20110325

nic-hdl:     CTE3
person:      Grupo de Administradores Internet
e-mail:      admin.internet@TELECOM.COM.CO
address:     Transversal 60, 114 A, 55
address:     571111 - BOGOTA DC - CU
country:     CO
phone:       +57 1 7050000 [74106]
created:     20090723
changed:     20140318

nic-hdl:     CTE7
person:      Grupo de Administradores Internet
e-mail:      admin.internet@TELECOM.COM.CO
address:     Transversal, 60, 114 A, 55
address:     571111 - BOGOTA DC - CU
country:     CO
phone:       +57 1 7050000 [71360]
created:     20140220
changed:     20140220

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

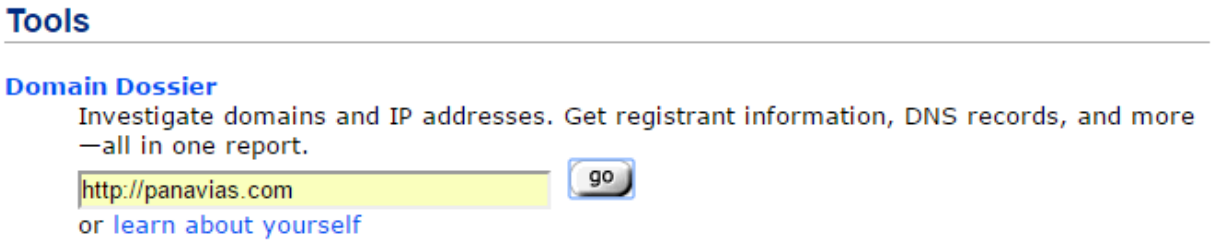
Los datos anteriores corresponden a la información arrojada de los registros de red (Network Whois record) dados por CentralOps.net, donde se muestra la información del proveedor de la red, quien es la empresa Colombia Telecomunicaciones S.A. ESP anteriormente Telecom quien se fusiono con Coltel y Movistar en 2012. Aun se observa en varios grupos de administradores registrados todavía registrados bajo el nombre de Telecom. Por ende se deduce que la red local opera bajo la marca comercial de Movistar.

CentralOps.net no arrojo resultados acerca de los registros de dominio (Domain Whois records) y registros DNS (DNS records).

- **Recolección de información del host**

Se procede a escanear la dirección IP 190.8.176.106, correspondiente al servicio web de la empresa Panavias S.A. (http://panavias.com) o también la url del sitio en CentralOps.net, con el objetivo de obtener información acerca del dominio, los registros de red y DNS del host.

Figura 11. Escaneo del host en CentralOps.net



Fuente: Autor

Se muestra la siguiente información acerca de los registros del dominio del host:

```
Domain Name: PANAVIAS.COM
   Registrar: TUCOWS DOMAINS INC.
   Sponsoring Registrar IANA ID: 69
   Whois Server: whois.tucows.com
   Referral URL: http://www.tucowsdomains.com
   Name Server: NS1.COLOMBIAHOSTING.COM
   Name Server: NS2.COLOMBIAHOSTING.COM
   Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
   Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
   Updated Date: 27-aug-2015
   Creation Date: 03-feb-2012
   Expiration Date: 03-feb-2017

>>> Last update of whois database: Thu, 25 Aug 2016 07:18:28 GMT <<<

For more information on Whois status codes, please visit
https://icann.org/epp

Queried whois.tucows.com with "panavias.com"...

Domain Name: PANAVIAS.COM
Domain ID: 1700263197_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2015-08-27T16:37:08Z
Creation Date: 2012-02-03T16:30:44Z
Registrar Registration Expiration Date: 2017-02-03T16:30:44Z
Sponsoring Registrar: TUCOWS, INC.
Sponsoring Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
Reseller: ColombiaHosting SAS
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited
```

Registry Registrant ID:
Registrant Name: Luis Calderon Torres
Registrant Organization: Panavias SA
Registrant Street: Centro Comercial Valle De Atriz Of 501
Registrant City: Pasto
Registrant State/Province: Narino
Registrant Postal Code: 00571
Registrant Country: CO
Registrant Phone: +57.27311118
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: panavias@yahoo.es
Registry Admin ID:
Admin Name: Luis Calderon Torres
Admin Organization: Panavias SA
Admin Street: Centro Comercial Valle De Atriz Of 501
Admin City: Pasto
Admin State/Province: Narino
Admin Postal Code: 00571
Admin Country: CO
Admin Phone: +57.27311118
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: panavias@yahoo.es
Registry Tech ID:
Tech Name: Soporte ColombiaHosting
Tech Organization: ColombiaHosting SAS
Tech Street: Cra 45 #103-40 Of. 307
Tech City: Bogota
Tech State/Province: Cundinamarca
Tech Postal Code: 00571
Tech Country: CO
Tech Phone: +57.16028584
Tech Phone Ext:
Tech Fax: +57.24858555
Tech Fax Ext:
Tech Email: dominios@colombiahosting.com.co
Name Server: NS1.COLOMBIAHOSTING.COM
Name Server: NS2.COLOMBIAHOSTING.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2015-08-27T16:37:08Z <<<

Los resultados arrojados acerca de la información del dominio, muestran información sensible referente a quien registro el host, en este caso el gerente de Panavias S.A. Luis Alberto Calderón Torres, además de la ubicación geográfica de la empresa que es Pasto, Nariño, Centro Comercial Valle de Atriz Oficina 501 y el correo de registro del host, panavias@yahoo.com. Además del proveedor del host quien es ColombiaHosting, la ubicación geográfica donde opera y sus teléfonos de

contacto. Para los registros de red del host (Network Whois record), se obtuvieron los siguientes resultados:

```
Network Whois record
Queried whois.lacnic.net with "190.8.176.106"...

inetnum:     190.8.176/22
status:      allocated
aut-num:     N/A
owner:       Colombia Hosting
ownerid:     CO-COHO-LACNIC
responsible: Jose David Bravo Álvarez
address:     Calle 64 Norte, 5b146, Oficina 305G
address:     00572 - Bogota -
country:     CO
phone:       +57 2 4854089 []
owner-c:     SOT5
tech-c:      SOT5
abuse-c:     SOT5
inetrev:     190.8.176/22
nserver:     NS1.COLOMBIAHOSTING.COM
nsstat:      20160822 AA
nslastaa:    20160822
nserver:     NS2.COLOMBIAHOSTING.COM
nsstat:      20160822 AA
nslastaa:    20160822
created:     20110722
changed:     20110722

nic-hdl:     SOT5
person:      Jose David Bravo Alvarez
e-mail:      ipadmin@COLOMBIAHOSTING.COM.CO
address:     Cra 45 #103-40, 307,
address:     110111 - Bogota - DC
country:     CO
phone:       +57 1 7428885 [120]
created:     20110718
changed:     20130926

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

En los registros de red del host se obtuvo información acerca del responsable de ColombiaHosting, el proveedor del host de la página web de Panavias S.A., José David Bravo Álvarez, así como la dirección de localización de la empresa Calle 64

Norte, 5b146, Oficina 305G en Bogotá. Además, se obtuvo el hostname de los servidores DNS del host de la empresa siendo ns1.colombiahosting.com, ns2.colombiahosting.com y aaron.colombiahosting.com como se muestra en la figura 12.

Figura 12. Servidores DNS del host

DNS records

name	class	type	data	time to live
panavias.com	IN	TXT	v=spf1 include:_spf.colhost.com -all	14400s (04:00:00)
panavias.com	IN	SOA	server: ns1.colombiahosting.com email: sysadmin@colombiahosting.com.co serial: 2012090801 refresh: 86400 retry: 7200 expire: 3600000 minimum ttl: 86400	86400s (1.00:00:00)
panavias.com	IN	NS	ns1.colombiahosting.com	86400s (1.00:00:00)
panavias.com	IN	NS	ns2.colombiahosting.com	86400s (1.00:00:00)
panavias.com	IN	A	190.8.176.106	14400s (04:00:00)
panavias.com	IN	MX	preference: 0 exchange: 7fbb87d203414eaec2122e66c94c0d.pamx1.hotmail.com	14400s (04:00:00)
106.176.8.190.in-addr.arpa	IN	PTR	aaron.colombiahosting.com.co	86400s (1.00:00:00)
176.8.190.in-addr.arpa	IN	NS	ns2.colombiahosting.com	86400s (1.00:00:00)
176.8.190.in-addr.arpa	IN	NS	ns1.colombiahosting.com	86400s (1.00:00:00)
176.8.190.in-addr.arpa	IN	SOA	server: ns1.colombiahosting.com email: dns@colombiahosting.com serial: 1467298252 refresh: 10800 retry: 3600 expire: 604800 minimum ttl: 3600	86400s (1.00:00:00)

Fuente: Autor

7.3.2. Identificación de Vulnerabilidades

Con la información obtenida en la fase anterior, se procede a realizar el proceso de identificación de vulnerabilidades, donde se escanearan los dos puntos a evaluar, la red local y el host de la empresa. Para este punto se utilizara la herramienta nmap, siendo esta la más idónea y en general la herramienta propicia en la presente fase del pentesting para escanear redes y detectar vulnerabilidades. También se hará uso de la herramienta Zenmap, que es el entorno grafico de Nmap, ofreciendo la gráfica de topologías como tracers y subredes.

7.3.2.1. Identificación de vulnerabilidades con Nmap

Nmap es la herramienta propicia para el escaneo de redes y detectar los servicios que son vulnerables en ella, por lo general, un servicio es vulnerable si el puerto donde este funciona se encuentra abierto. Se procederá a escanear tanto la dirección IP de la red local como del host de Panavias S.A. con el objetivo de identificar las vulnerabilidades que existen en estas.

- **Identificación de vulnerabilidades de la red local**

Se procede a realizar el escaneo con nmap para encontrar vulnerabilidades en la dirección de la red local. Para obtener un informe detallado del escaneo como puertos y servicios abiertos como también del fingerprinting (sistema operativo) y el traceroute, se ejecuta el siguiente comando:

```
nmap –A 186.116.250.224
```

Se obtienen los siguientes resultados tras el escaneo:

```
Starting Nmap 6.00 (http://nmap.org) at 2016-09-13 01:03 EEST
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 01:03
Scanning 186.116.250.224 [100 ports]
Discovered open port 443/tcp on 186.116.250.224
Discovered open port 8000/tcp on 186.116.250.224
Completed SYN Stealth Scan at 01:03, 1.82s elapsed (100 total ports)
Initiating Service scan at 01:03
Scanning 2 services on 186.116.250.224
Completed Service scan at 01:04, 14.60s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 186.116.250.224
Retrying OS detection (try #2) against 186.116.250.224
Initiating Traceroute at 01:04
Completed Traceroute at 01:04, 2.01s elapsed
NSE: Script scanning 186.116.250.224.

[+] Nmap scan report for 186.116.250.224

Host is up (0.19s latency).
Not shown: 91 closed ports

PORT       STATE      SERVICE VERSION
21/tcp     filtered   ftp
22/tcp     filtered   ssh
23/tcp     filtered   telnet
```

```
53/tcp     filtered   domain
443/tcp    open       ssl/http mini_httpd 1.19 19dec2003
445/tcp    filtered   microsoft-ds
631/tcp    filtered   ipp
5009/tcp   filtered   airport-admin
8000/tcp   open http   mini_httpd 1.19 19dec2003
Device type: WAP|general purpose|router|media device|remote management

Running (JUST GUESSING): Linux 2.4.X|2.6.X (97%), Toshiba Linux 2.4.X
(94%), Linksys embedded (93%), Netgear embedded (92%), Western Digital
embedded (92%), Gemtek embedded (92%), Siemens embedded OS CPE:
cpe:/o:linux:kernel:2.4 cpe:/o:toshiba:linux:2.4 cpe:/h:linksys:wrv54g
cpe:/h:linksys:rv042 cpe:/o:linux:kernel:2.6.22

Aggressive OS guesses: OpenWrt (Linux 2.4.32) (97%), OpenWrt White
Russian 0.9 (Linux 2.4.30) (96%), OpenWrt (Linux 2.4.30 - 2.4.34) (96%),
Toshiba Magnia SG10 server appliance (Linux 2.4.18) (94%),

No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 993/tcp)

HOP    RTT     ADDRESS
1    ...
2    27.85 ms   172.21.111.202
3    37.85 ms   Static-IP-1901572189.cable.net.co (190.157.2.189)
4    ...
5    76.77 ms   telecom2-nap.ccit.org.co (206.223.124.156)
6    ...
7    70.21 ms   10.32.0.58
8    ... 9
10   65.03 ms   10.7.39.38
11   88.38 ms   186.116.250.224

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/

Nmap done: 1 IP address (1 host up) scanned in 24.05 seconds
Raw packets sent: 238 (13.424KB) | Rcvd: 4983 (218.696KB)
```

Según los resultados del escaneo a la red local de la empresa Panavias S.A. se puede observar lo siguiente:

- Puertos y Servicios: El resultado arrojo nueve puertos escaneados, entre los cuales aparecen abiertos el puerto 443 correspondiente al servicio SSL y el puerto 8000 que corresponde al servicio http. Los demás puertos aparecen filtrados (filtered) lo que refiere a que nmap no puede determinar si estos puertos están abiertos o cerrados, esto ocurre cuando hay un filtro de paquetes que descarga la consulta, posiblemente de la presencia de un firewall. Aunque de por si aparezcan filtrados, esto puede representar una gran amenaza ya que hay gran variedad de herramientas para evasión de firewalls y se podrían explotar estos puertos. Entre los puertos interesantes filtrados encontrados durante este escaneo se encuentran el puerto 21 que corresponde al servicio FTP, el puerto 22 al servicio SSH y el puerto 23 correspondiente al servicio TELNET. Este último servicio, TELNET, representa una gran vulnerabilidad ya que es un servicio para acceder en modo terminal. Sus datos como nombres de usuario y contraseñas para acceder a dicha terminal viajan en texto plano, resultan fáciles de obtener para cualquiera que utilice herramientas para tráfico de red.

- Fingerprinting: es el proceso de recopilación que permite identificar el sistema operativo del objetivo. Nmap en el escaneo realiza un fingerprinting activo donde detecta el sistema operativo del ordenador donde funciona el servicio de red local en la empresa Panavias S.A. que es un OpenWrt (Linux 2.4.32) seguramente que corresponde al servicio de administración de la red alojado en el puerto 8000 que se encuentra abierto.

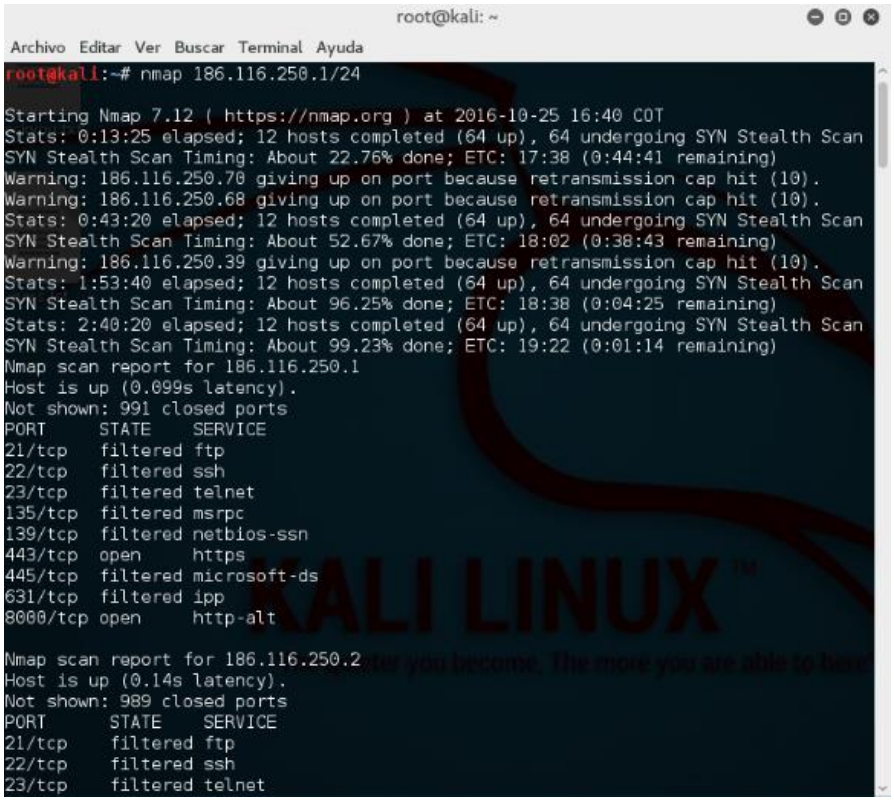
- Traceroute: es el registro que permite seguir los paquetes que vienen desde el servidor local (localhost) hasta su punto objetivo. Se observa que realizo 5 trazas hasta llegar al punto objetivo, que es la dirección IP 186.116.250.224 correspondiente a la red local de la empresa Panavias S.A.

- **Escaneo a la subred con Nmap**

Una vez conocida la estructura general de la red local de la empresa Panavias S.A. se procede a realizar un escaneo a la subred, lo que permitirá observar los equipos conectados a esta, además de los servicios y procesos que se pueden estar manejando en los equipos o dispositivos que están conectados a la subred de la empresa. Para escanear la subred de la empresa Panavias S.A. se ejecuta el siguiente comando:

nmap 186.116.250.1/24

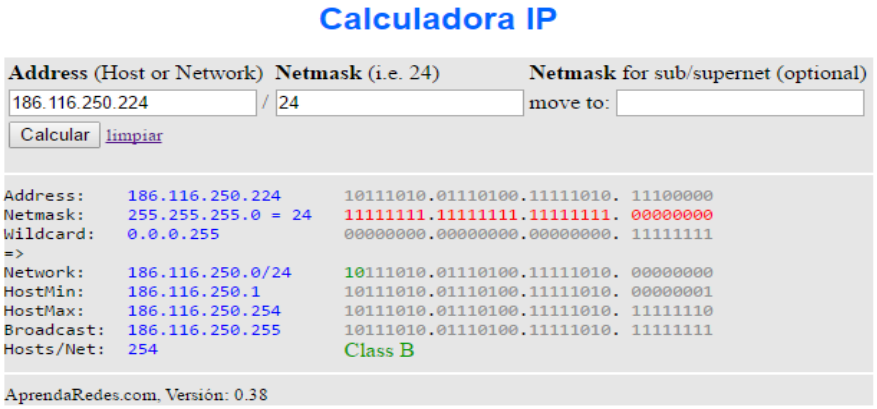
Figura 13. Escaneo de subred



Fuente: Autor

Con la herramienta de Calculadora IP online (http://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc_cgi), se determina cual es la máscara de red y la clase de red. Se identifica que es una red Clase B con Mascara de red 255.255.255.0 como se muestra en la figura 14:

Figura 14. Calculadora IP



Fuente: Autor

Las direcciones IP de los equipos registrados durante el escaneo de nmap se muestran en el Anexo G – Pruebas de Penetración, en el archivo que se denomina “Nmap_equiposSubred”, donde se encuentran listados en una tabla.

Se procede a realizar pruebas en las direcciones IP de la subred con el objetivo de encontrar vulnerabilidades o características en los procesos que se manejan. En primer lugar se procede a verificar la dirección IP 186.116.250.12, donde se realizara un escaneo de los puertos, servicios y el fringerprinting para detectar el sistema operativo y el tipo de dispositivo. Se ejecuta el siguiente comando:

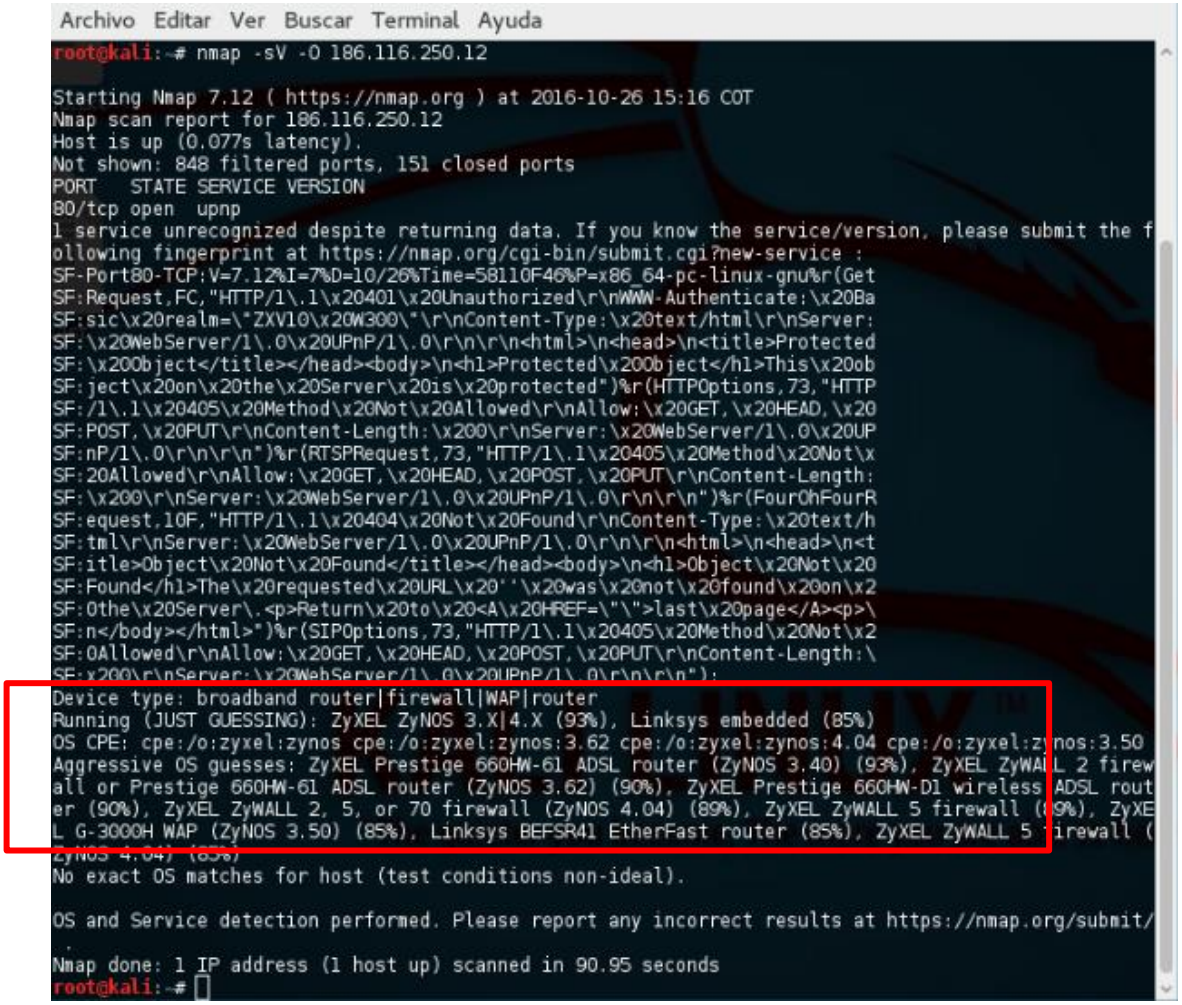
```
nmap –sV –O 186.116.250.12
```

Dónde:

- –sV corresponde a detectar las versiones de los servicios abiertos en los puertos disponibles.
- –O para detectar el sistema operativo (fingerprinting).

El escaneo se muestra en la siguiente imagen:

Figura 15. Escaneo a la dirección 186.116.250.12



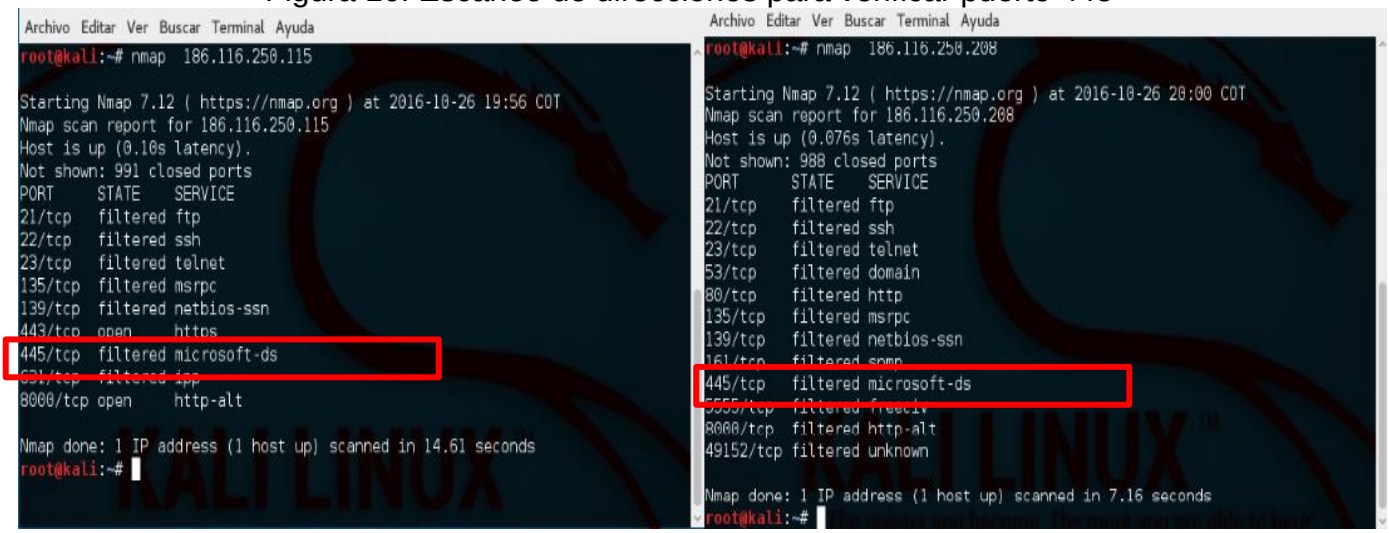
Fuente: Autor

Como se observa en el recuadro de la figura 15, la dirección escaneada corresponde a un router (Device type), de marca ZyXEL ZyNOS, el cual en el fingerprinting muestra que tiene activado el firewall y la red wireless con seguridad WAP. Su consola de administración funciona por el puerto 80, que es el puerto que se encuentra abierto donde se accede a la configuración del router.

Para su funcionamiento, el software Helysa GW comparte sus archivos en una red distribuida donde se conectan todos los equipos que utilizan esta aplicación, lo que ocasiona que se abra el puerto 445, correspondiente al servicio Microsoft-DS (Active Directory). Puede representar una vulnerabilidad al momento de explotar

este puerto, ya que en él se encuentra información contenida en la aplicación Helysa GW como inventarios, información contable, usuarios, etc.

Figura 16. Escaneo de direcciones para verificar puerto 445



Fuente: Autor

Como se observa en la figura 16, se escanearon las direcciones 186.116.250.115 y 186.116.250.208 donde los recuadros corresponden al puerto 445 del servicio Microsoft-ds que sirve para el uso de carpetas compartidas de la aplicación Helysa GW.

- **Identificación de vulnerabilidades en el host**

Se procede a realizar el escaneo con nmap para encontrar vulnerabilidades con la dirección IP del host ejecutando el siguiente comando:

```
nmap –A 190.8.176.106
```

Con este comando se obtiene información acerca de los puertos, servicios y el fingerprinting (sistema operativo) del host de la empresa Panavias S.A. Se obtienen los siguientes resultados:

```
Starting Nmap 6.00 (http://nmap.org) at 2016-09-27 12:05 EEST
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 12:05
Scanning aaron.colombiahosting.com.co (190.8.176.106) [100 ports]
Discovered open port 25/tcp on 190.8.176.106
```

```
Discovered open port 995/tcp on 190.8.176.106
Discovered open port 993/tcp on 190.8.176.106
Discovered open port 587/tcp on 190.8.176.106
Discovered open port 143/tcp on 190.8.176.106
Discovered open port 110/tcp on 190.8.176.106
Discovered open port 53/tcp on 190.8.176.106
Discovered open port 3306/tcp on 190.8.176.106
Discovered open port 21/tcp on 190.8.176.106
Discovered open port 443/tcp on 190.8.176.106
Discovered open port 80/tcp on 190.8.176.106
Discovered open port 26/tcp on 190.8.176.106
Discovered open port 465/tcp on 190.8.176.106
Completed SYN Stealth Scan at 12:05, 1.92s elapsed (100 total ports)
Initiating Service scan at 12:05
Scanning 13 services on aaron.colombiahosting.com.co (190.8.176.106)
Completed Service scan at 12:07, 136.32s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against aaron.colombiahosting.com.co
(190.8.176.106)
Retrying OS detection (try #2) against aaron.colombiahosting.com.co
(190.8.176.106)
NSE: Script scanning 190.8.176.106.
```

[+] Nmap scan report for aaron.colombiahosting.com.co (190.8.176.106)

```
Host is up (0.12s latency).
Not shown: 80 filtered ports
```

PORT	STATE	SERVICE VERSION
21/tcp	open	ftp Pure-FTPd
25/tcp	open	smtp?
26/tcp	open	smtp Exim smtpd 4.87
53/tcp	open	domain
80/tcp	open	http Apache httpd 2.2.27 ((UNIX) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
110/tcp	open	pop3 Dovecot pop3d
143/tcp	open	imap Dovecot imapd
443/tcp	open	ssl/http Apache httpd 2.2.27 ((UNIX) mod_ssl/2.2.27 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
465/tcp	open	ssl/smtp Exim smtpd 4.87
587/tcp	open	smtp Exim smtpd 4.87
993/tcp	open	ssl/imap Dovecot imapd
995/tcp	open	ssl/pop3 Dovecot pop3d
3306/tcp	open	mysql MySQL 5.5.32-cll-lve
32768/tcp	closed	filenet-tms
49152/tcp	closed	unknown
49153/tcp	closed	unknown
49154/tcp	closed	unknown
49155/tcp	closed	unknown
49156/tcp	closed	unknown
49157/tcp	closed	unknown

```
Device type: general purpose|WAP|firewall
```

```
Running (JUST GUESSING): Linux 3.X|2.6.X|2.4.X (94%), Fortinet Linux
2.6.X (85%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:linux:kernel:3 cpe:/o:linux:kernel:2.6.32
cpe:/o:linux:kernel:2.4 cpe:/o:fortinet:linux:2.6
cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Linux 3.0 (94%), Linux 2.6.32 - 2.6.35 (92%),
Linux 2.6.32 - 2.6.38 (92%), Linux 2.6.38 (91%), Linux 2.6.39 (90%),
Linux 2.6.34 (88%), Linux 2.6.18 (88%), Linux 2.6.32 - 2.6.33

No exact OS matches for host (test conditions non-ideal).
Uptime guess: 22.509 days (since Sun Sep 4 23:54:16 2016)
TCP Sequence Prediction: Difficulty=248 (Good luck!)
IP ID Sequence Generation: All zeros

OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/

Nmap done: 1 IP address (1 host up) scanned in 143.39 seconds
Raw packets sent: 248 (14.524KB) | Rcvd: 54 (3.414KB)
```

Según los resultados del escaneo al host de la empresa Panavias S.A. se puede observar lo siguiente:

- Puertos y Servicios: Se observa gran vulnerabilidad por puertos abiertos importantes como lo son el puerto 21, que corresponde al servicio FTP, el servicio SMTP para transferencia de correo en los puertos 25 y 26, el servicio IMAP que permite el acceso a mensajes en un servidor en el puerto 143 y el puerto 3306 que corresponde al servicio de bases de datos del host, el servicio MySql. Por encontrase abiertos, puede representar una amenaza al momento que un tercero los explote. Otros puertos abiertos que se encontraron durante el escaneo son el puerto 53 correspondiente al servicio de nombres DNS, el puerto 80 que corresponde el servicio http, donde se ejecuta la página web de la empresa Panavias S.A. (http://panavias.com), el servicio POP3 en el puerto 110 que también es utilizado para transferencia de mensajes de correo electrónico al servidor y los puertos 993 y 995 que son también protocolos de transferencia que van cifrados con un servicio SSL.

- Fingerprinting: se observa que los servidores donde se aloja el host que corresponden a ColombiaHosting, trabajan bajo Fortinent Linux 3.0. Seguramente ColombiaHosting utiliza esta distribución para ejecutar los servicios SSL. También utiliza FreeBSD que es un sistema operativo libre

compatible con Linux. Además se observa que los servidores de ColombiaHosting cuentan con firewall, con seguridad WAP.

7.3.2.2. Identificación de vulnerabilidades con Zenmap

Zenmap es una herramienta que permite ejecutar nmap de manera gráfica, realizando escaneos detallados, como también la graficas de topologías y trazas.

En primer lugar se realiza un escaneo al host, ejecutando el siguiente comando en Zenmap:

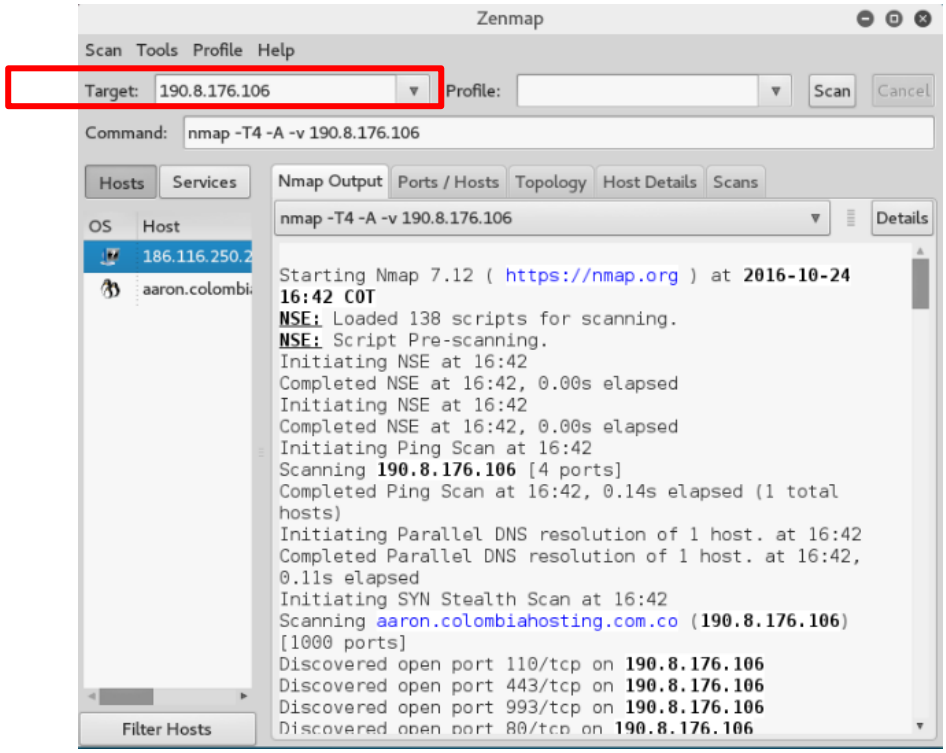
```
nmap –T4 –A -v 190.8.176.106
```

Dónde:

- –T4 acelera el proceso de consulta.
- -A consulta por los puertos y servicios, fingerprinting y traceroute.
- -v consulta por las versiones de los servicios e información adicional.

La siguiente figura muestra la ejecución en la herramienta Zenmap donde en el recuadro se introduce la dirección ip del host:

Figura 17. Escaneo del host en Zenmap



Fuente: Autor

Se obtiene la siguiente información tras el escaneo con Zenmap:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-24 16:42 COT
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:42
Completed NSE at 16:42, 0.00s elapsed
Initiating NSE at 16:42
Completed NSE at 16:42, 0.00s elapsed
Initiating Ping Scan at 16:42
Scanning 190.8.176.106 [4 ports]
Completed Ping Scan at 16:42, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:42
Completed Parallel DNS resolution of 1 host. at 16:42, 0.11s elapsed
Initiating SYN Stealth Scan at 16:42
Scanning aaron.colombiahosting.com.co (190.8.176.106) [1000 ports]
Discovered open port 110/tcp on 190.8.176.106
Discovered open port 443/tcp on 190.8.176.106
Discovered open port 993/tcp on 190.8.176.106
Discovered open port 80/tcp on 190.8.176.106
```

```
Discovered open port 53/tcp on 190.8.176.106
Discovered open port 25/tcp on 190.8.176.106
Discovered open port 995/tcp on 190.8.176.106
Discovered open port 21/tcp on 190.8.176.106
Discovered open port 3306/tcp on 190.8.176.106
Discovered open port 143/tcp on 190.8.176.106
Discovered open port 587/tcp on 190.8.176.106
Discovered open port 26/tcp on 190.8.176.106
Discovered open port 465/tcp on 190.8.176.106
Discovered open port 34572/tcp on 190.8.176.106
Discovered open port 34571/tcp on 190.8.176.106
Discovered open port 34573/tcp on 190.8.176.106
Completed SYN Stealth Scan at 16:42, 9.85s elapsed (1000 total ports)
Initiating Service scan at 16:42
Scanning 16 services on aaron.colombiahosting.com.co (190.8.176.106)
Completed Service scan at 16:45, 151.94s elapsed (16 services on 1 host)
Initiating OS detection (try #1) against aaron.colombiahosting.com.co
(190.8.176.106)
Initiating Traceroute at 16:45
Completed Traceroute at 16:45, 3.03s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 16:45
Completed Parallel DNS resolution of 8 hosts. at 16:45, 0.54s elapsed
NSE: Script scanning 190.8.176.106.
Initiating NSE at 16:45
Completed NSE at 16:46, 69.08s elapsed
Initiating NSE at 16:46
Completed NSE at 16:46, 1.18s elapsed
Nmap scan report for aaron.colombiahosting.com.co (190.8.176.106)
Host is up (0.11s latency).
Not shown: 928 filtered ports, 56 closed ports
PORT        STATE SERVICE     VERSION
21/tcp      open  ftp         Pure-FTPd
| ssl-cert: Subject: commonName=*.colombiahosting.com.co
| Issuer: commonName=AlphaSSL CA - SHA256 -
G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-21T12:33:08
| Not valid after:  2017-10-22T12:33:08
| MD5:   8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
|_SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a
|_ssl-date: 2016-10-24T21:45:11+00:00; -32s from scanner time.
25/tcp      open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
26/tcp      open  smtp        Exim smtpd 4.87
| smtp-commands: aaron.colombiahosting.com.co Hello
aaron.colombiahosting.com.co [181.55.78.163], SIZE 52428800, 8BITMIME,
PIPELINING, AUTH PLAIN LOGIN, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT
RSET HELP
| ssl-cert: Subject: commonName=*.colombiahosting.com.co
| Issuer: commonName=AlphaSSL CA - SHA256 -
G2/organizationName=GlobalSign nv-sa/countryName=BE
```

```
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-21T12:33:08
| Not valid after:  2017-10-22T12:33:08
| MD5:   8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
|_SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a
|_ssl-date: 2016-10-24T21:45:09+00:00; -32s from scanner time.
53/tcp      open  domain
| dns-nsid:
|_  bind.version: 9.8.2rc1-RedHat-9.8.2-0.47.rc1.el6_8.2
80/tcp      open  http        Apache httpd 2.2.27 ((Unix) mod_ssl/2.2.27
OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
| http-methods:
|   Supported Methods: OPTIONS GET HEAD POST TRACE
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3          Dovecot pop3d
|_pop3-capabilities: TOP SASL(PLAIN LOGIN) PIPELINING CAPA UIDL STLS USER
AUTH-RESP-CODE RESP-CODES
| ssl-cert: Subject: commonName=*.colombiahosting.com.co
| Issuer: commonName=AlphaSSL CA - SHA256 -
G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-21T12:33:08
| Not valid after:  2017-10-22T12:33:08
| MD5:   8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
|_SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a
|_ssl-date: 2016-10-24T21:45:09+00:00; -32s from scanner time.
143/tcp   open  imap          Dovecot imapd
|_imap-capabilities: ENABLE LITERAL+ SASL-IR IDLE IMAP4rev1 post-login
LOGIN-REFERRALS AUTH=PLAIN NAMESPACE STARTTLS ID more have
AUTH=LOGINA0001 listed capabilities Pre-login OK
| ssl-cert: Subject: commonName=*.colombiahosting.com.co
| Issuer: commonName=AlphaSSL CA - SHA256 -
G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-21T12:33:08
| Not valid after:  2017-10-22T12:33:08
| MD5:   8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
|_SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a
|_ssl-date: 2016-10-24T21:45:12+00:00; -32s from scanner time.
443/tcp   open  ssl/http      Apache httpd 2.2.27 ((Unix) mod_ssl/2.2.27
OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1e-
fips mod_bwlimited/1.4
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=pruebas.casalimpia.co
```

```
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's
Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-24T07:29:00
| Not valid after:  2017-01-22T07:29:00
| MD5:   7cee f4bb 8946 5fc0 ebe8 1eea 399b 2c22
|_SHA-1: 015c a84a 03c0 67f6 f164 5d1b e9ba 2b3b 1303 1cdc
|_ssl-date: 2016-10-24T21:45:12+00:00; -31s from scanner time.
465/tcp   open  ssl/smtp      Exim smtpd 4.87
| smtp-commands: aaron.colombiahosting.com.co Hello
aaron.colombiahosting.com.co [181.55.78.163], SIZE 52428800, 8BITMIME,
PIPELINING, AUTH PLAIN LOGIN, HELP,
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
|_ssl-date: 2016-10-24T21:45:08+00:00; -33s from scanner time.
587/tcp   open  smtp          Exim smtpd 4.87
| smtp-commands: aaron.colombiahosting.com.co Hello
aaron.colombiahosting.com.co [181.55.78.163], SIZE 52428800, 8BITMIME,
PIPELINING, AUTH PLAIN LOGIN, STARTTLS, HELP,
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT
RSET HELP
| ssl-cert: Subject: commonName=*.colombiahosting.com.co
| Issuer: commonName=AlphaSSL CA - SHA256 -
G2/organizationName=GlobalSign nv-sa/countryName=BE
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-21T12:33:08
| Not valid after:  2017-10-22T12:33:08
| MD5:   8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
|_SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a
|_ssl-date: 2016-10-24T21:45:11+00:00; -32s from scanner time.
993/tcp   open  ssl/imap      Dovecot imapd
|_imap-capabilities: ENABLE AUTH=LOGINA0001 SASL-IR IDLE IMAP4rev1 post-
login LOGIN-REFERRALS AUTH=PLAIN NAMESPACE have ID more OK listed
capabilities LITERAL+ Pre-login
|_ssl-date: 2016-10-24T21:45:09+00:00; -32s from scanner time.
995/tcp   open  ssl/pop3      Dovecot pop3d
|_pop3-capabilities: UIDL USER SASL(PLAIN LOGIN) PIPELINING AUTH-RESP-
CODE CAPA RESP-CODES TOP
|_ssl-date: 2016-10-24T21:45:13+00:00; -32s from scanner time.
3306/tcp  open  mysql         MySQL 5.5.32-cll-lve
| mysql-info:
|   Protocol: 53
|   Version: .5.32-cll-lve
|   Thread ID: 33538852
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, InteractiveClient,
Support41Auth, IgnoreSpaceBeforeParenthesis, FoundRows,
SupportsTransactions, LongPassword, SupportsLoadDataLocal,
IgnoreSigpipes, Speaks41ProtocolNew, ODBCClient,
DontAllowDatabaseTableColumn, LongColumnFlag, SupportsCompression,
ConnectWithDatabase
```

```
|   Status: Autocommit
|_  Salt: <p?)M*).IfGmqnVA$.[^
34571/tcp open  unknown
34572/tcp open  http          Adaptec Storage Manager Agent httpd
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: %APPLICATION%
34573/tcp open  ssl/unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 0.325 days (since Mon Oct 24 08:58:26 2016)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
```

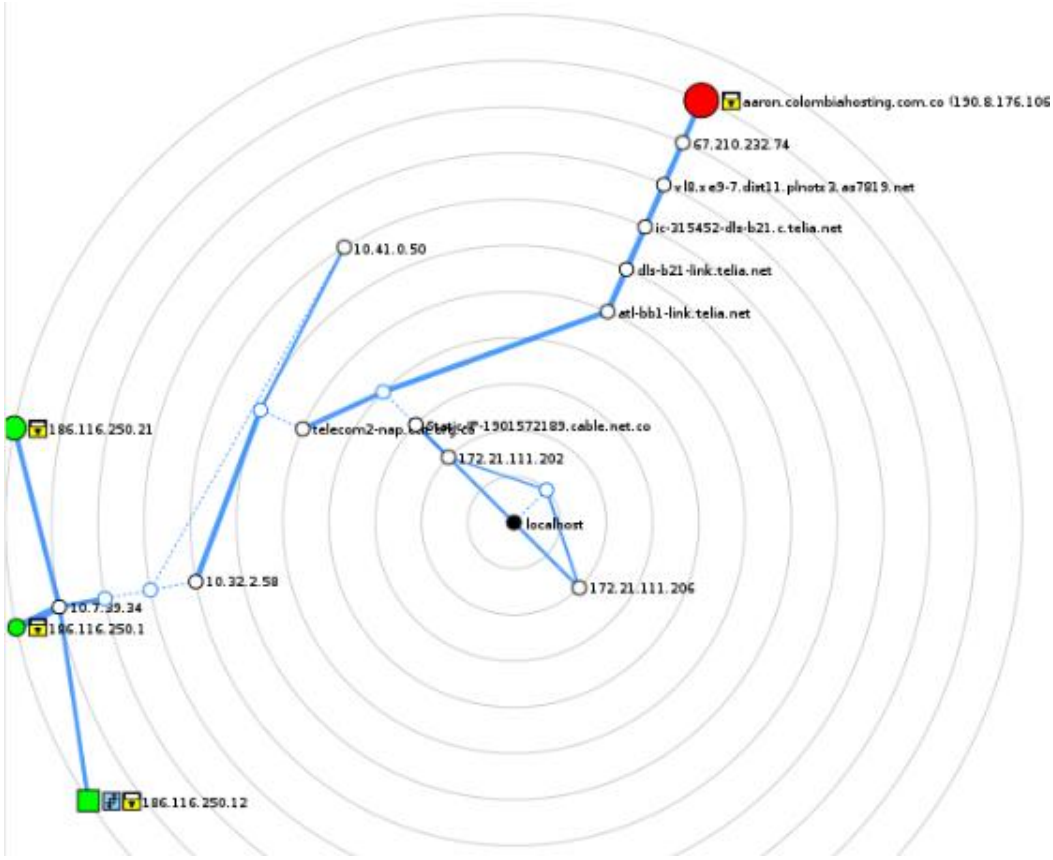
En los resultados se observa que en los puertos 21 (FTP), 26 (SMTP), 110 (POP3), 143 (IMAP), 443 (SSL) y 587 (SMTP) muestra datos encriptados en MD5 y SHA-1 que podrían corresponder a usuarios o contraseñas para acceso a los servicios. Los datos encontrados son:

- MD5: 8053 5b46 361a b1ef 8baa 9189 15dd 3a0f
  SHA-1: e220 8278 64c0 1721 a2f4 822f 8d19 1d25 d840 4f6a

- MD5: 7cee f4bb 8946 5fc0 ebe8 1eea 399b 2c22
  SHA-1: 015c a84a 03c0 67f6 f164 5d1b e9ba 2b3b 1303 1cdc

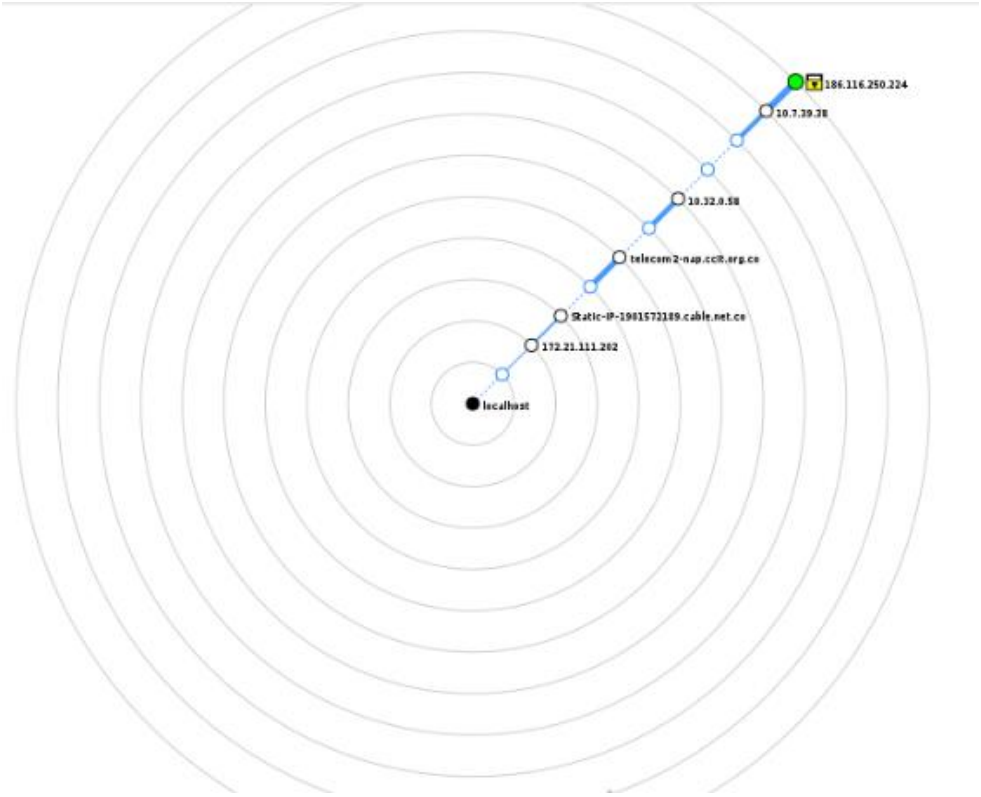
De igual manera, se procede a realizar las trazas en Zenmap, referente a las rutas que siguieron los paquetes hasta alcanzar los objetivos, estos se muestran en la figura 18 la traza para el host con la dirección 190.8.176.106 el cual consiguió 13 trazas hasta llegar al servidor aaron.colombiahosting.com.co donde se encuentra alojado el host de panavias correspondiente al servicio web (http://panavias.com) y en la figura 19 para la red local con la dirección 186.116.250.224, el cual la traza ya se había realizado en el escaneo de nmap, el cual consiguió 6 trazas hasta llegar al objetivo.

Figura 18. Topología de enrutamiento para el host



Fuente: Autor

Figura 19. Topología de enrutamiento para la red local



Fuente: Autor

7.3.3. Análisis de Vulnerabilidades

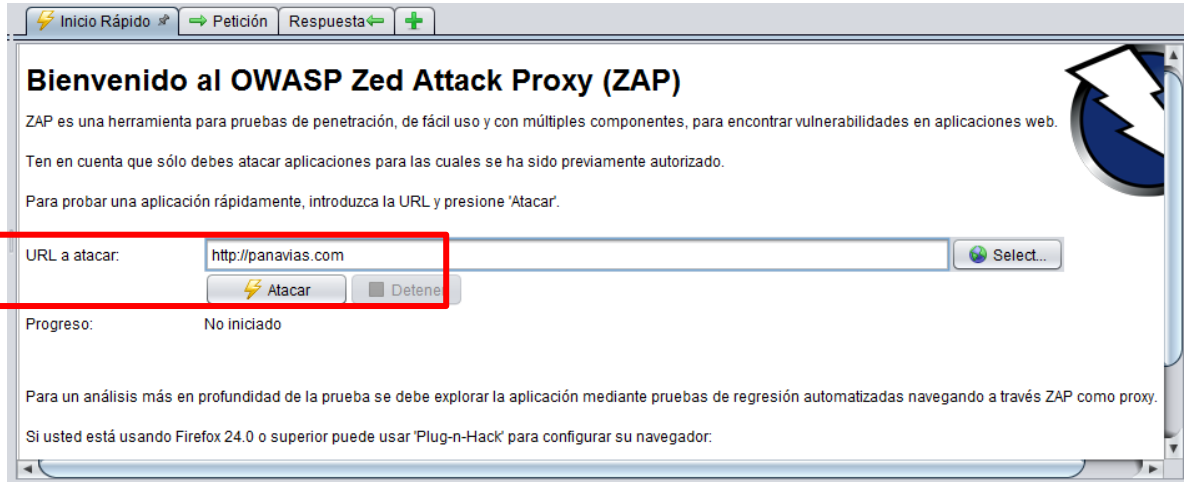
Se ejecutan herramientas para escanear vulnerabilidades y determinar el nivel de riesgo que poseen estas. Se procede a realizar estas pruebas en el host, donde las herramientas son idóneas ya que analizan vulnerabilidades en aplicaciones web y en la red local, con herramientas que puedan aplicar en este punto.

7.3.3.1. Análisis de vulnerabilidades con OWASP-ZAP

La herramienta OWASP-ZAP permite identificar y analizar vulnerabilidades a través de varias herramientas como lo es el escaneo de spider que analiza los directorios ocultos en la aplicación web y el Escaneo Activo que permite identificar y analizar vulnerabilidades encontradas en esta.

Se procede a realizar en análisis en OWASP-ZAP, introduciendo la dirección url del sitio web de la empresa que corresponde a http://panavias.com, como se muestra en la siguiente imagen:

Figura 20. Inicio del análisis en OWASP-ZAP

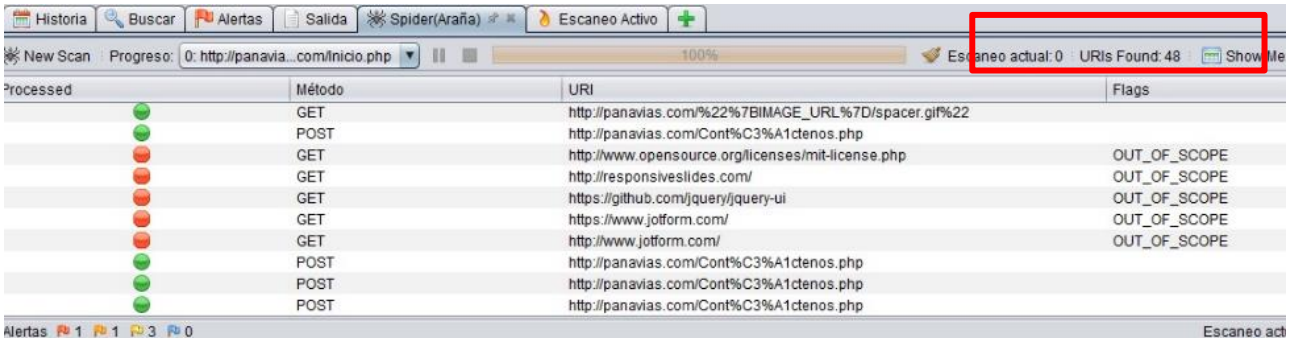


Fuente: Autor

- **Analizando directorios con Spider (Araña)**

La herramienta Spider de OWASP-ZAP, permite identificar directorios ocultos en la aplicación web a analizar, realizando un listado de todas las url del sitio, llamados “direcciones semillas”.

Figura 21. Ejecución de Spider en OWASP-ZAP



Fuente: Autor

De acuerdo al recuadro de la figura 21, se encontraron 48 direcciones url en la aplicación web de Panavias (http://panavias.com). Las urls ocultas de la página se muestran en la siguiente tabla:

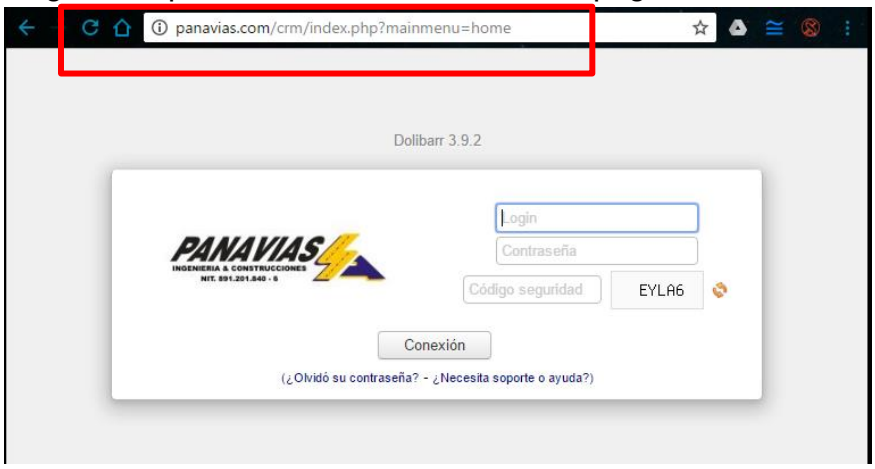
Tabla 10. Directorios y direcciones ocultas

Directories	HTTP Code	HTTP Reason	Link
/images/	403	Forbidden	http://panavias.com//images/
/2/	200	OK	http://panavias.com//2/
/media/	200	OK	http://panavias.com//media/
/etc/	501	Method Not Implemented	http://panavias.com//etc/
/js/	403	Forbidden	http://panavias.com//js/
/crm/	200	OK	http://panavias.com//crm/
/scripts/	403	Forbidden	http://panavias.com//scripts/
/index/	200	OK	http://panavias.com//index/
/home/	200	OK	http://panavias.com//home/
/documents/	403	Forbidden	http://panavias.com//documents/
/cgi-bin/	403	Forbidden	http://panavias.com//cgi-bin/

Fuente: Autor

De acuerdo a los resultados, se observa que hay uno en particular y corresponde a la dirección http://panavias.com//crm/ del directorio /crm/ escaneado por Spider, el cual corresponde al login o ingreso al panel de administración de la página web de Panavias S.A. esto se muestra en la siguiente imagen con la introducción del link en el navegador para verificar:

Figura 22. Ingreso al panel de administración de la página web de Panavias S.A.

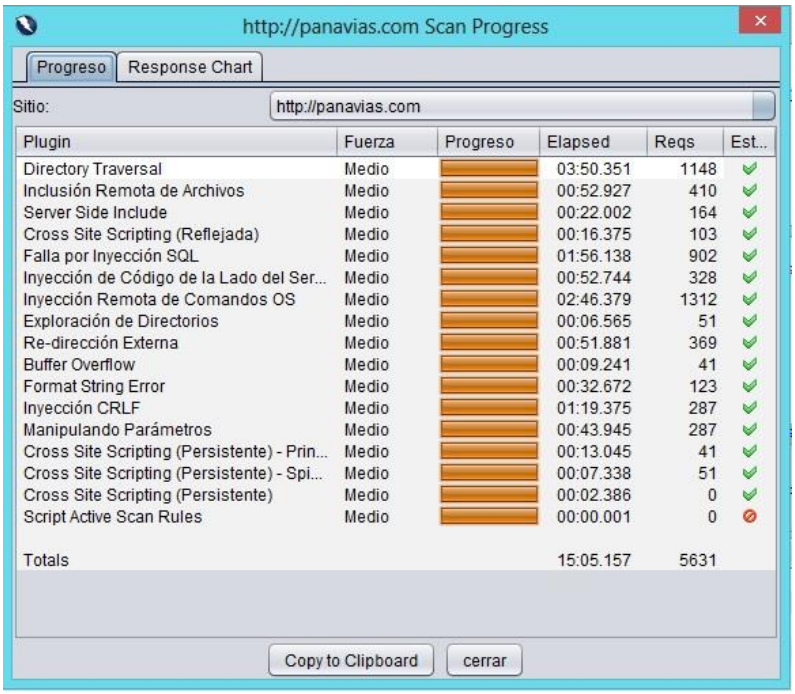


Fuente: Autor

- **Análisis de vulnerabilidades con OWASP-ZAP**

OWASP-ZAP inicia, luego de analizar los directorios de la página, el escaneo activo que permite evaluar, de acuerdo al listado de amenazas informáticas que este tiene, a cuál de ellas la página es vulnerable. El listado del escaneo activo de amenazas se muestra en la siguiente imagen:

Figura 23. Escaneo Activo de amenazas de OWASP-ZAP



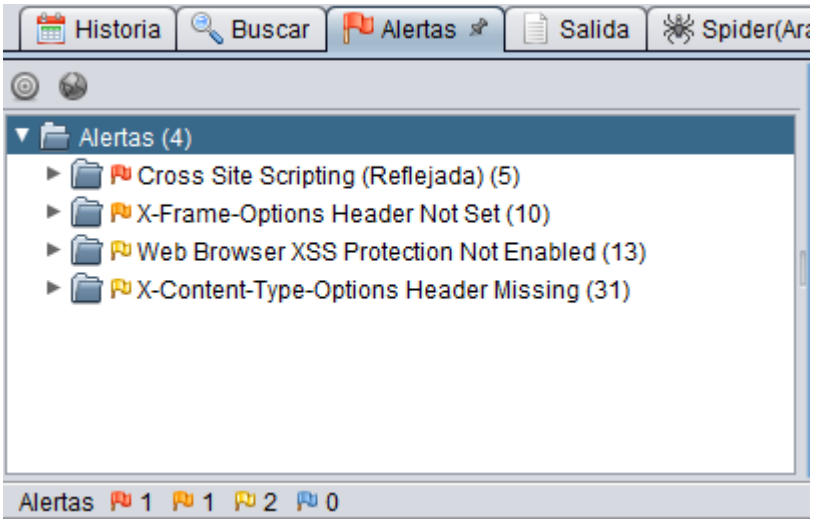
Fuente: Autor

Posteriormente, luego del escaneo activo, OWASP-ZAP clasifica las vulnerabilidades encontradas de acuerdo a la siguiente escala:

- Bandera Roja: Riesgo Alto
- Bandera Amarrilla Oscura: Riesgo Medio
- Bandera Amarilla Clara: Riesgo Bajo

Según los resultados del escaneo activo de amenazas, que se reportan en la pestaña “Alertas” se obtuvo una vulnerabilidad de riesgo alto, una vulnerabilidad de riesgo medio y dos de riesgo bajo. Esto se muestra en la siguiente imagen:

Figura 24. Listado de Alertas de OWASP-ZAP



Fuente: Autor

De las cuatro alertas dadas por OWASP-ZAP la vulnerabilidad por Cross Site Scripting (Reflejada) es la que se clasifica como de Riesgo Alto con cinco instancias. En el reporte generado por OWASP-ZAP se muestran la descripción de la vulnerabilidad, la solución ante esto y las instancias o urls comprometidas.

Tabla 11. Descripción de vulnerabilidad por CSS Reflejado

Cross Site Scripting	Riesgo: Alto
Descripción	Vulnerabilidad que permite inyectar código malicioso de tipo JavaScript o VBScript en los “agujeros” o fallas de código en una aplicación web.

Tabla 11. Descripción de vulnerabilidad por CSS Reflejado (Continuación)

	Existen tres tipos de ataques con Cross Site Scripting: • Reflejado • Persistente • Basados en DOM La vulnerabilidad detectada por OWASP-ZAP se clasifica como un CSS Reflejado que consiste en modificar valores que en el código de la aplicación web utiliza como variables entre dos páginas.
Solución	De acuerdo al reporte de OWASP-ZAP, se debe implementar en la fase de Diseño y Arquitectura del desarrollo de la aplicación web, librerías o frameworks que permitan generar y validar líneas de código seguro como lo son Microsoft's Anti-XSS, el módulo de OWASP ESAPI Encoding, y Apache Wicket. Además de implementar pruebas de código en la fase de implementación que permitan detectar estas fallas acertadamente.
Instancias	Son las urls afectadas o vectores de ataque. Se detectaron 5 instancias las cuales son: • url: http://panavias.com/Cont%C3%A1ctenos.php parámetro: textbox0 • url: http://panavias.com/Cont%C3%A1ctenos.php parámetro: textbox1 • url: http://panavias.com/Cont%C3%A1ctenos.php parámetro: textbox2 • url: http://panavias.com/Cont%C3%A1ctenos.php parámetro: textbox7 • url: http://panavias.com/Cont%C3%A1ctenos.php parámetro: textbox12

Fuente. Autor

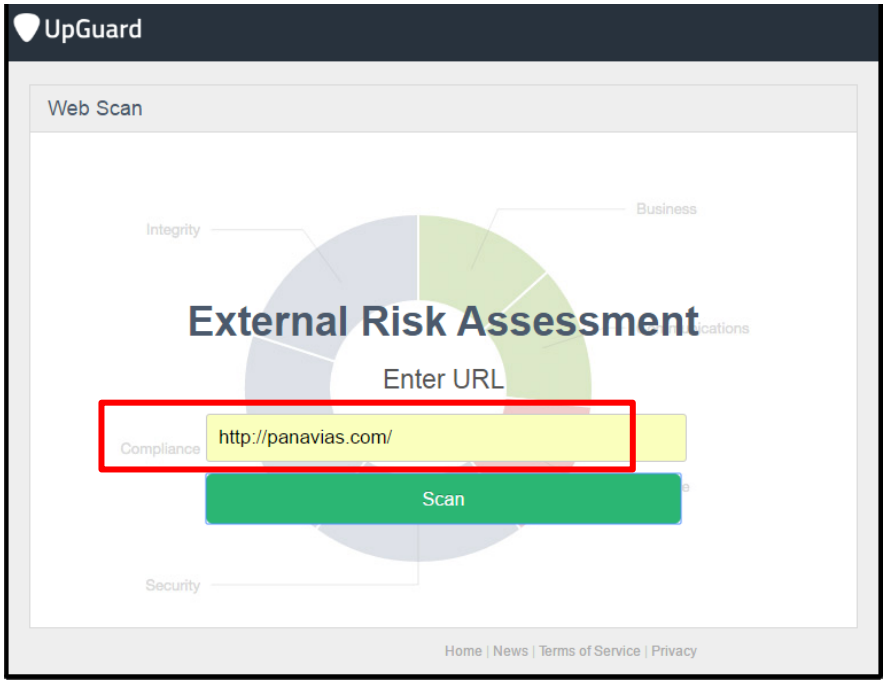
El reporte html completo del testeo de la aplicación web correspondiente a la dirección http://panavias.com/ generado por OWASP-ZAP denominado “Panavias-OWASP-ZAP.html” se encuentra en el Anexo G – Pruebas de Penetración, en este se evidencian las alertas encontradas durante el testeo que fueron 4; descripción de la vulnerabilidad, las instancias con las url’s y paramentos comprometidos, su solución, información adicional y referencias.

7.3.3.2. Análisis de vulnerabilidades con UpGuard

UpGuard es un escáner web que permite identificar vulnerabilidades a aplicaciones web realizando pruebas de pishing, presencia de malware, falsa autenticación directamente en la aplicación y en las comunicaciones como registro de servidores DNS, puertos, servicios, etc.

Se procede a realizar el escaneo de la página web que corresponde a la dirección url http://panavias.com/ en UpGuard, como se muestra en el recuadro de la siguiente imagen:

Figura 25. Escaneo de vulnerabilidades en UpGuard



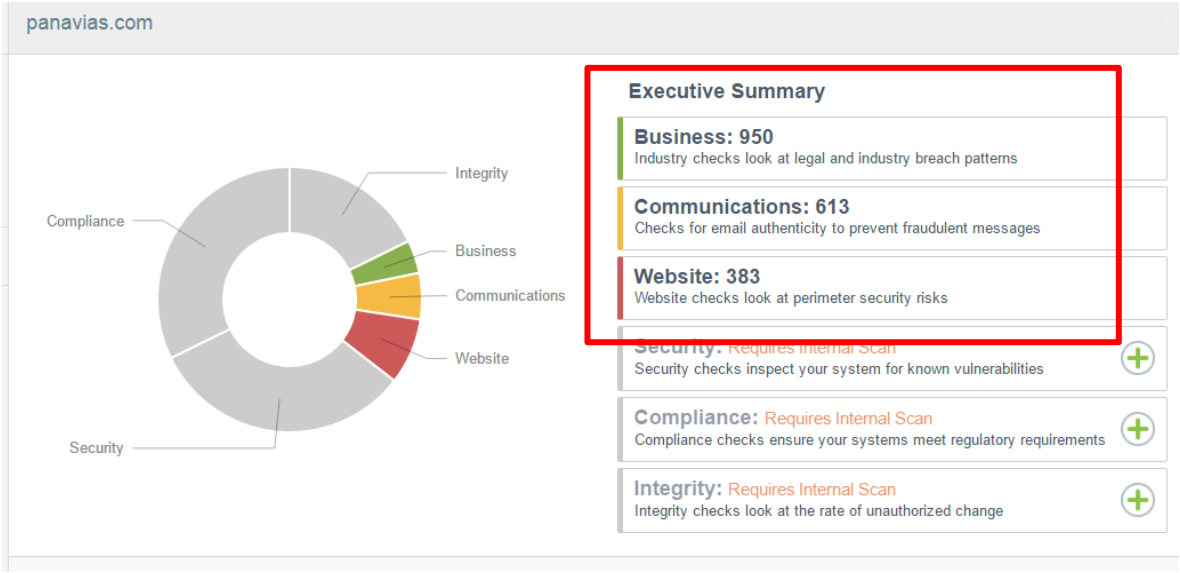
Fuente: Autor

Tras el escaneo, UpGuard, muestra gráficamente el total de advertencias encontradas durante el análisis, donde las evalúa de acuerdo a tres parámetros:

- Negocios: verifica patrones de violación legales.
- Comunicaciones: verifica los servicios de comunicación.
- Website: verifica riesgos de seguridad en la aplicación web.

Los resultados tras el escaneo del url http://panavias.com/ en UpGuard se muestran en la siguiente imagen:

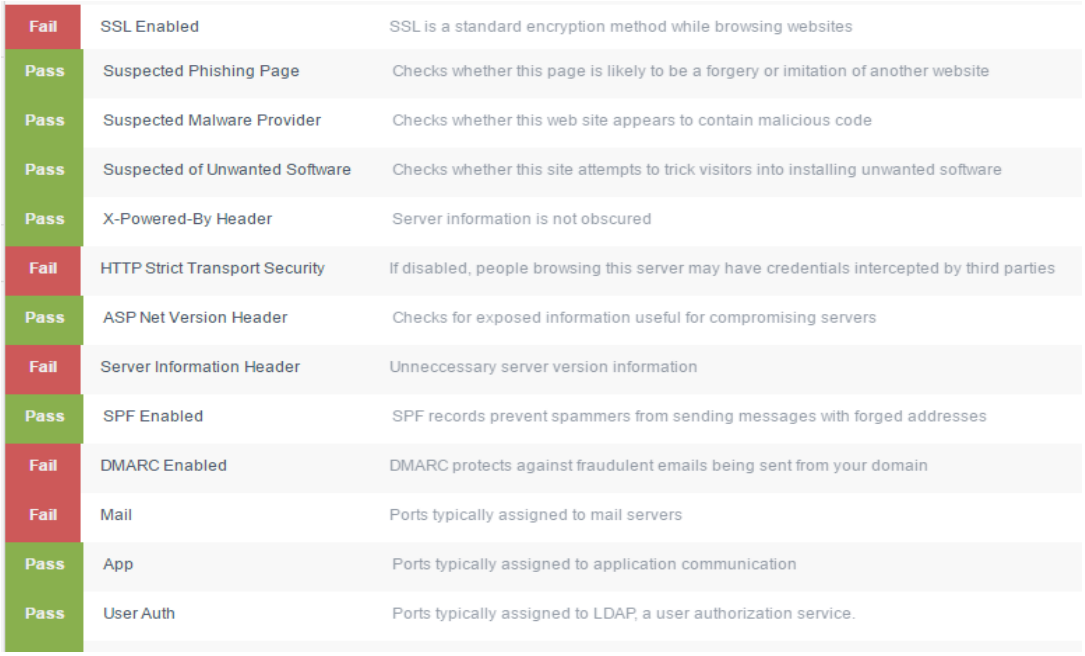
Figura 26. Gráfica del Escaneo en UpGuard



Fuente: Autor

De acuerdo al recuadro de la figura 26, se evaluaron para el paramento Negocios (Business) 950 procesos, del parámetro Comunicaciones (Communications) 613 procesos y del parámetro Sitio Web (WebSite) 383 procesos.

Figura 27. Ítems evaluados en el primer test



Fail	SSL Enabled	SSL is a standard encryption method while browsing websites
Pass	Suspected Phishing Page	Checks whether this page is likely to be a forgery or imitation of another website
Pass	Suspected Malware Provider	Checks whether this web site appears to contain malicious code
Pass	Suspected of Unwanted Software	Checks whether this site attempts to trick visitors into installing unwanted software
Pass	X-Powered-By Header	Server information is not obscured
Fail	HTTP Strict Transport Security	If disabled, people browsing this server may have credentials intercepted by third parties
Pass	ASP Net Version Header	Checks for exposed information useful for compromising servers
Fail	Server Information Header	Unneccessary server version information
Pass	SPF Enabled	SPF records prevent spammers from sending messages with forged addresses
Fail	DMARC Enabled	DMARC protects against fraudulent emails being sent from your domain
Fail	Mail	Ports typically assigned to mail servers
Pass	App	Ports typically assigned to application communication
Pass	User Auth	Ports typically assigned to LDAP, a user authorization service.

Fuente: Autor

Se evaluaron 27 items en dos partes. La primera, como se muestra en la figura 27, las pruebas que fallaron, que son las que se muestran en rojo, fueron las siguientes:

- SSL Enabled: A pesar de que el host cuenta con el servicio SSL, UpGuard determina que no lo tiene habilitado.
- HTTP Strict Transport Security: Ausencia de la cabecera HTTPS para trafico seguro de la información.
- Server Information Header: Información sensible de los servidores expuesta.
- DMARC Enabled: El host no cuenta con el servicio DMARC para proteger de mensajes fraudulentos y phising.
- Mail: información de cuentas de correo electrónico expuestas.

Figura 28. Ítems evaluados en el segundo test

Pass	File Sharing	Ports typically assigned to file sharing services
Pass	Voice	Ports typically assigned to voice over IP services
Pass	Administration	Ports typically assigned to services that provide access to workstations
Fail	Database	Ports typically assigned to database communication
Fail	DNSSEC Enabled	DNSSEC records prevent third parties from forging the records that guarantee a domain's identity
N/A	SSL Expiry	Certificate does not expire within 30 days
N/A	SSL Strength	Industry standard SHA256 encryption in use
N/A	Domain Expiry	Domain does not expire within 30 days
N/A	HttpOnly Cookies	Helps mitigate the risk of client side script attacks
N/A	Secure Cookies	Checks that third parties cannot copy identity information and use it on another computer
N/A	CEO Approval Rating	CEO approval rating according to employee reviews
N/A	Employee Company Rating	Employee company rating
N/A	Breaches	Known breaches that have been recorded against the company
N/A	Exposed Emails	Known email accounts that have been exposed in breaches

Fuente: Autor

En la segunda entrega, como se muestra en la figura 28, dos pruebas fallaron la verificación, además de nueve pruebas que no aplicaron. Las pruebas que fallaron el test fueron las siguientes:

- Database: puertos de bases de datos expuestos. Como se vio anteriormente en otras pruebas, esto hace referencia al puerto 3306 de MySql que se encuentra abierto.
- DNSSEC Enabled: no se tiene activado este servicio para ocultar los registros de los servidores DNS del host.

El reporte html completo del testeo de la aplicación web correspondiente a la dirección http://panavias.com/ realizado en UpGuard, que se denomina “Panavias-UpGuard.html” se encuentra en el Anexo G – Pruebas de Penetración, en este se evidencian todos los ítems evaluados con las recomendaciones para su solución y los procesos evaluados en los parámetros Comunicaciones y Website.

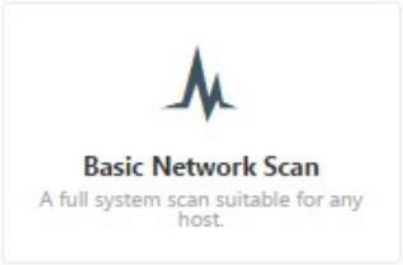
7.3.3.3. Análisis de vulnerabilidades con Nessus

Nessus scanner es una herramienta de la empresa Tenable Network Security, que permite identificar y analizar vulnerabilidades mediante varias opciones evaluando cada infraestructura de red. Entre sus opciones se encuentran escaneos para encontrar vulnerabilidades a redes, escaneos a host y aplicaciones web, como también escaneos a servicios en la nube. Para esta prueba, se procede a realizar dos escaneos con Nessus, uno para la red local de Panavias y el otro escaneo para su host.

- **Escaneo con Nessus a la red local de Panavias**

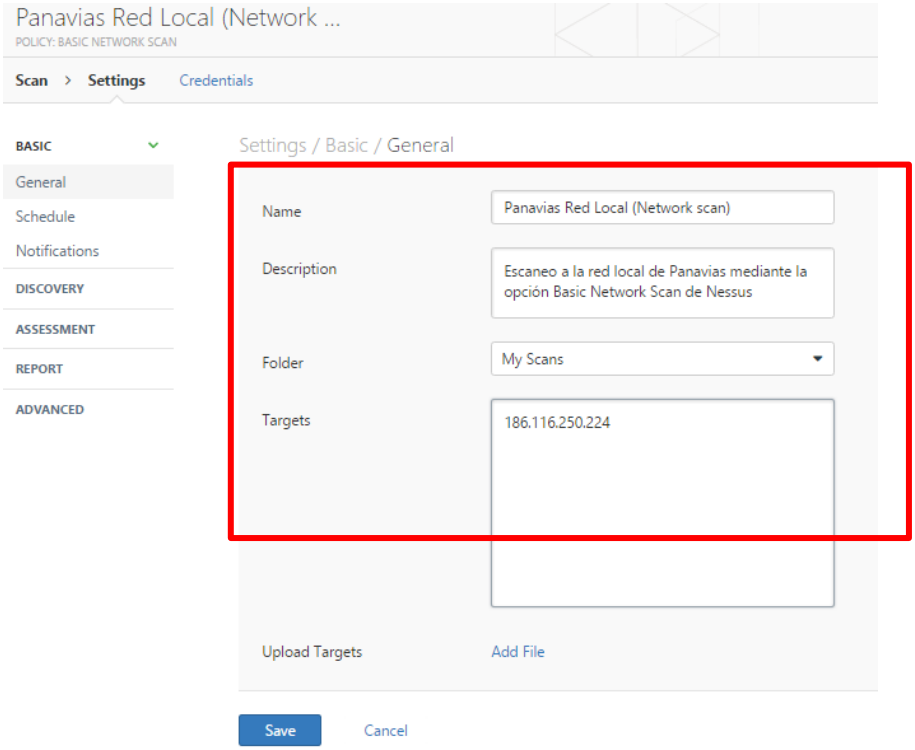
Para realizar el escaneo a la red local de la empresa Panavias S.A., que corresponde a la dirección IP 186.116.250.224, se procede a escoger la opción Basic Network Scan de Nessus (figura 29) y posteriormente se configura el escaneo como se muestra en la figura 30:

Figura 29. Opción Basic Network Scan de Nessus



Fuente: Autor

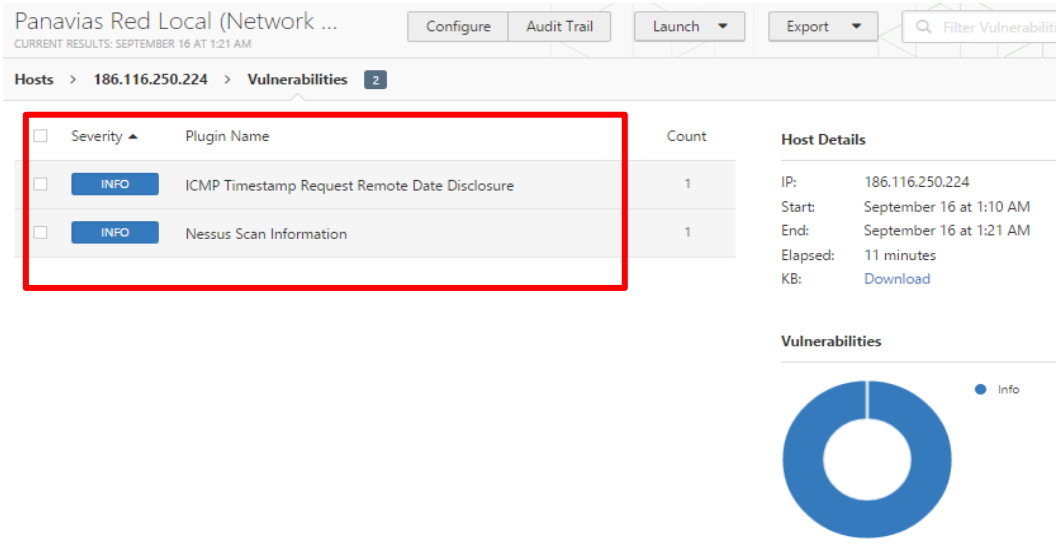
Figura 30. Configuración de escaneo a la red local en Nessus



Fuente: Autor

De acuerdo a los resultados tras el escaneo con Nessus a la red local, se encontraron dos vulnerabilidades como se muestra en la siguiente imagen:

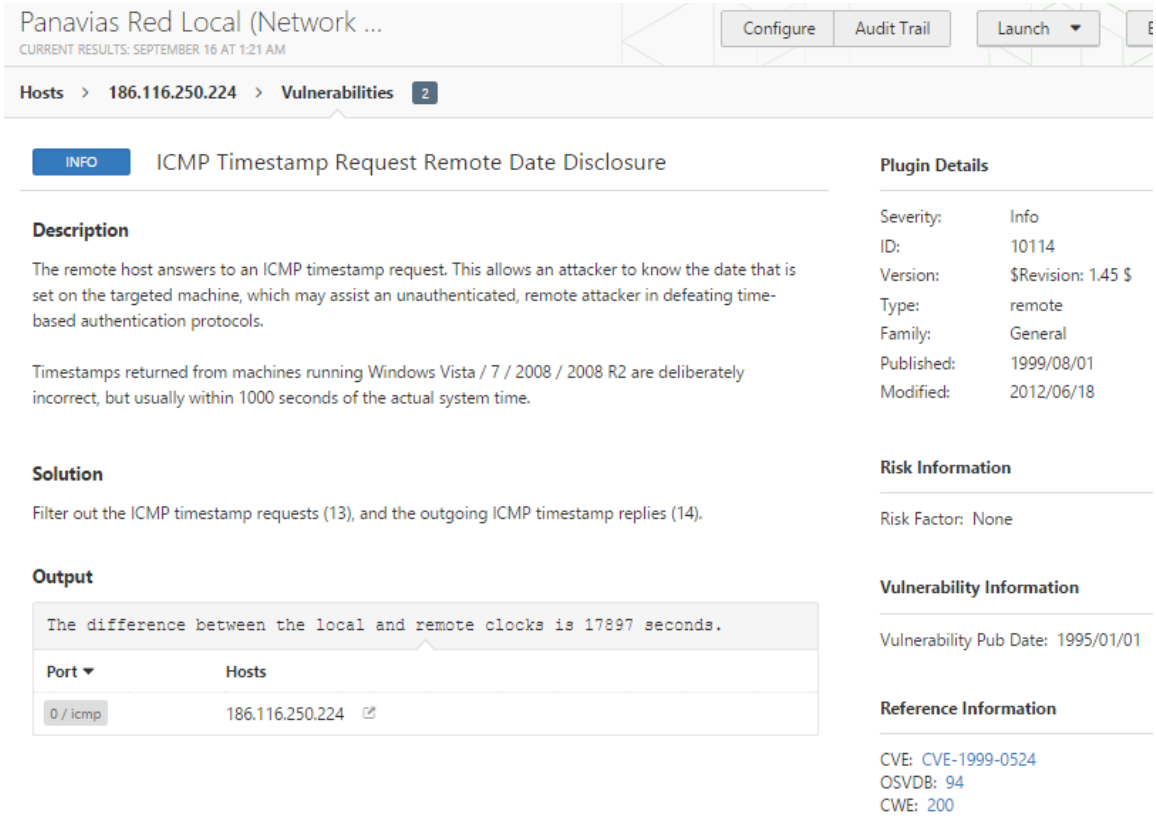
Figura 31. Vulnerabilidades encontradas en la red local con Nessus



Fuente: Autor

La vulnerabilidad más relevante corresponde al Protocolo de Mensajes de Control de Internet (ICMP), donde hay una solicitud de marca de tiempo en la respuesta al protocolo. Esto permite al atacante conocer las configuraciones de la maquina objetivo y burlar los sistemas de autenticación. La solución para esto, de acuerdo al reporte de Nessus es filtrar las solicitudes que se realicen al protocolo ICMP. Esta vulnerabilidad está registrada en el National Vulnerability Database bajo el código CVE-1999-0524. Los resultados de esta vulnerabilidad en Nessus se muestran en la siguiente imagen:

Figura 32. Reporte de vulnerabilidad por solicitudes ICMP en Nessus



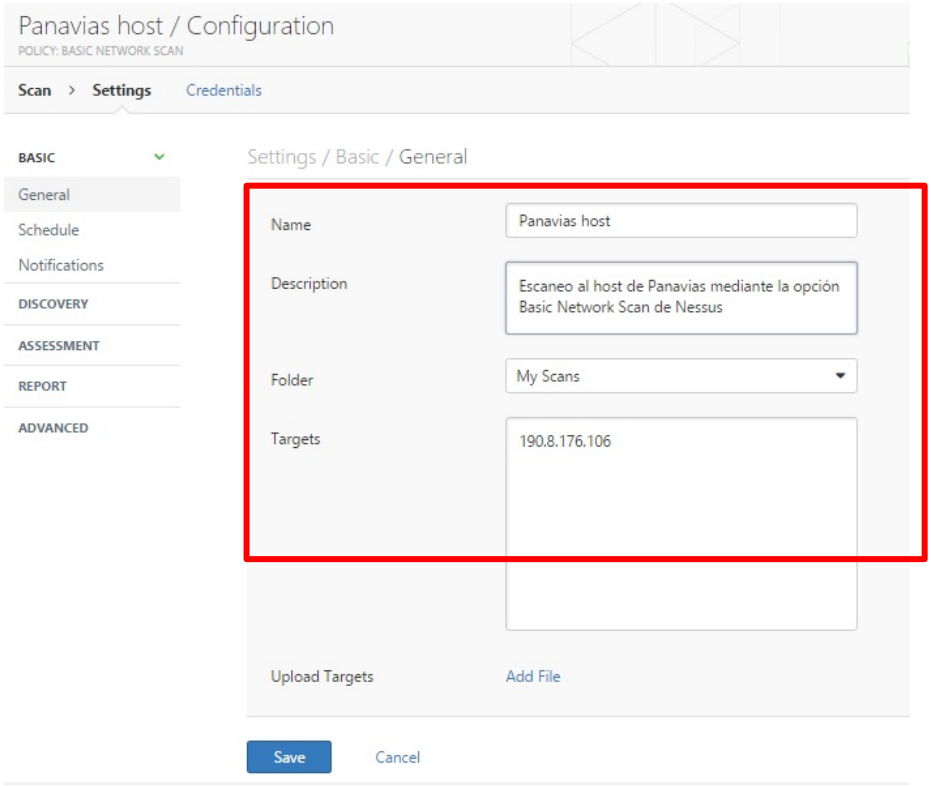
Fuente: Autor

El reporte html completo del testeo a la red local de Panavias S.A. correspondiente a la dirección IP 188.116.250.24 realizado en Nessus, que se denomina “Panavias_RedLocal-Nessus.html” se encuentra en el Anexo G – Pruebas de Penetración, en donde se muestran las vulnerabilidades encontradas con su clasificación, descripción y sus recomendaciones para su solución.

- **Escaneo con Nessus al Host de Panavias**

Para realizar el escaneo al host de la empresa Panavias S.A., que corresponde a la dirección IP 190.8.176.106, se procede a escoger la opción Basic Network Scan de Nessus y posteriormente se configura el escaneo como se muestra en la siguiente imagen:

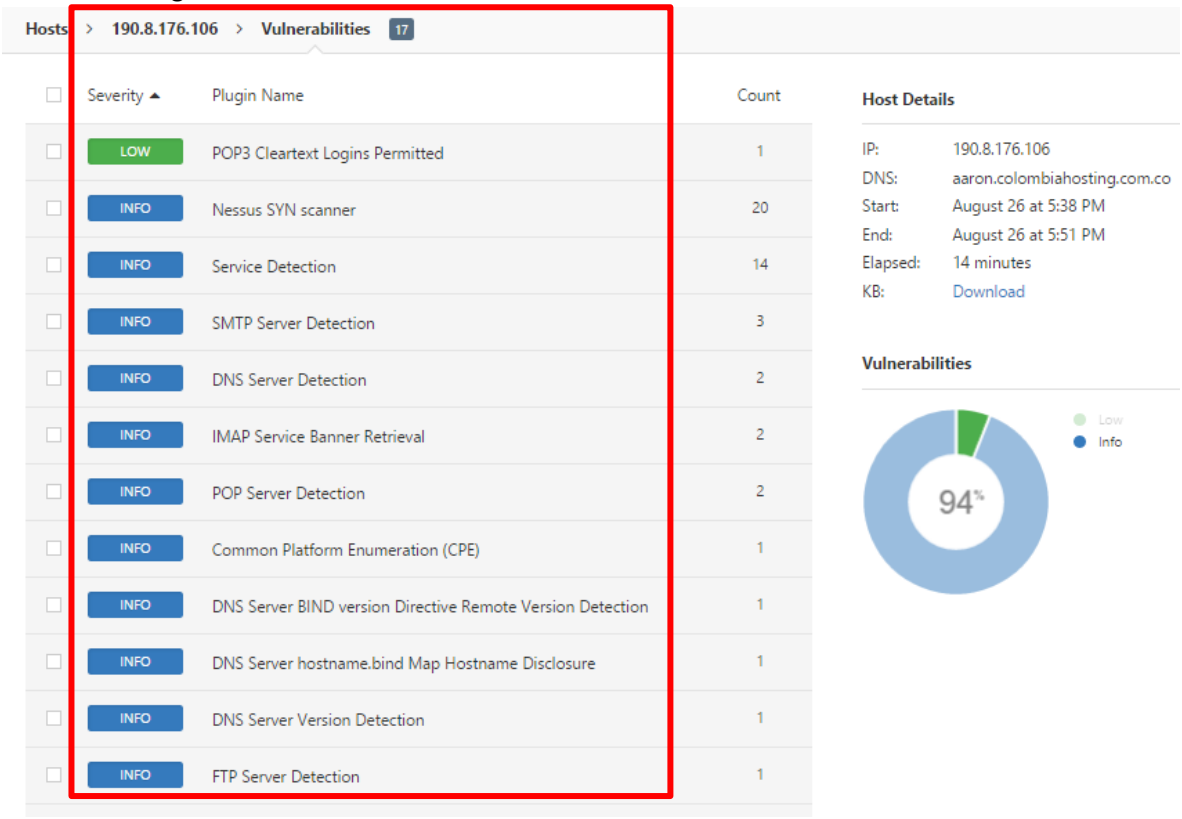
Figura 33. Configuración de escaneo a la red local en Nessus



Fuente: Autor

De acuerdo a los resultados tras el escaneo con Nessus al host, se encontraron 17 vulnerabilidades; una de ellas es la más relevante que corresponde al servicio POP3, el protocolo de oficina de correo, los demás son considerados de riesgo bajo, entre los cuales se muestran la detección de los servidores SMTP, POP, DNS, FTP, como también escaneo de puertos abiertos TCP/IP e información expuesta en el Traceroute. Los resultados se observan en la figura 32:

Figura 34. Vulnerabilidades encontradas en el host con Nessus

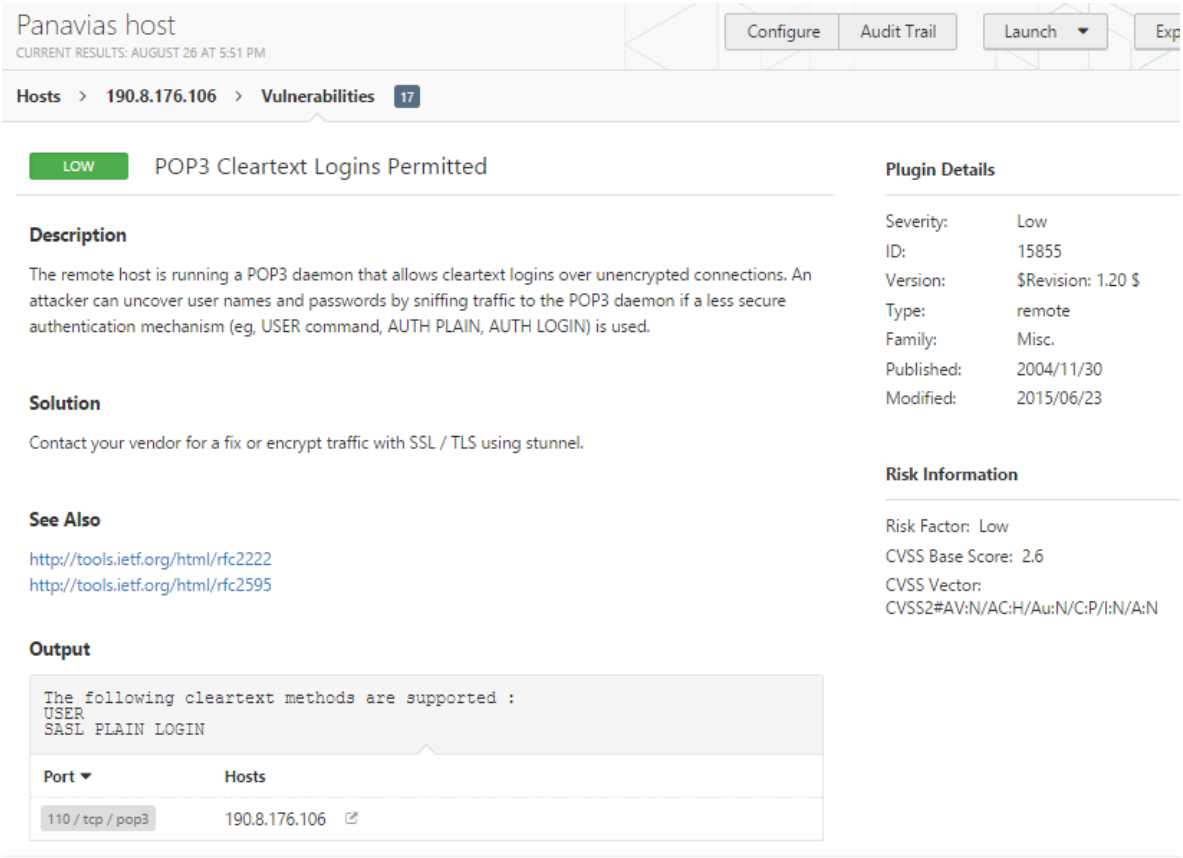


Fuente: Autor

En el recuadro de la figura 33 no se alcanza a observar todas las vulnerabilidades encontradas durante el escaneo, pero estas se podrán revisar a detalle en el reporte de Nessus.

La vulnerabilidad más relevante encontrada durante el escaneo corresponde al Protocolo de Oficina de Correo (POP3) en el puerto 110, donde Nessus reporta que este servicio está realizando conexiones sin encriptar. Un atacante, mediante sniffing, puede obtener cuentas de usuario y contraseñas. La solución para ello, de acuerdo a Nessus es que se debe contactar al proveedor para utilizar protocolos criptográficos como SSL/TLS. Se observó, de acuerdo a pruebas anteriores, que el servicio SSL se encuentra inactivo. Esta vulnerabilidad, de acuerdo a la puntuación dada por el National Vulnerability Database se evalúa con el vector CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N y se califica como 2.6, considerándose como riesgo bajo, pero debe mitigarse ya que fácilmente puede ser explotada. Los resultados de esta vulnerabilidad en Nessus se muestran en la siguiente imagen:

Figura 35. Reporte de vulnerabilidad del servicio POP3 en Nessus



Fuente: Autor

El reporte html completo del testeo al host de Panavias S.A. correspondiente a la dirección IP 190.8.176.106 realizado en Nessus, que se denomina “Panavias_Host-Nessus.html” se encuentra en el Anexo G – Pruebas de Penetración, en donde se muestran todas las vulnerabilidades encontradas durante el escaneo con su clasificación, descripción y sus recomendaciones para su solución.

7.3.3.4. Prueba a redes inalámbricas con JumpStart

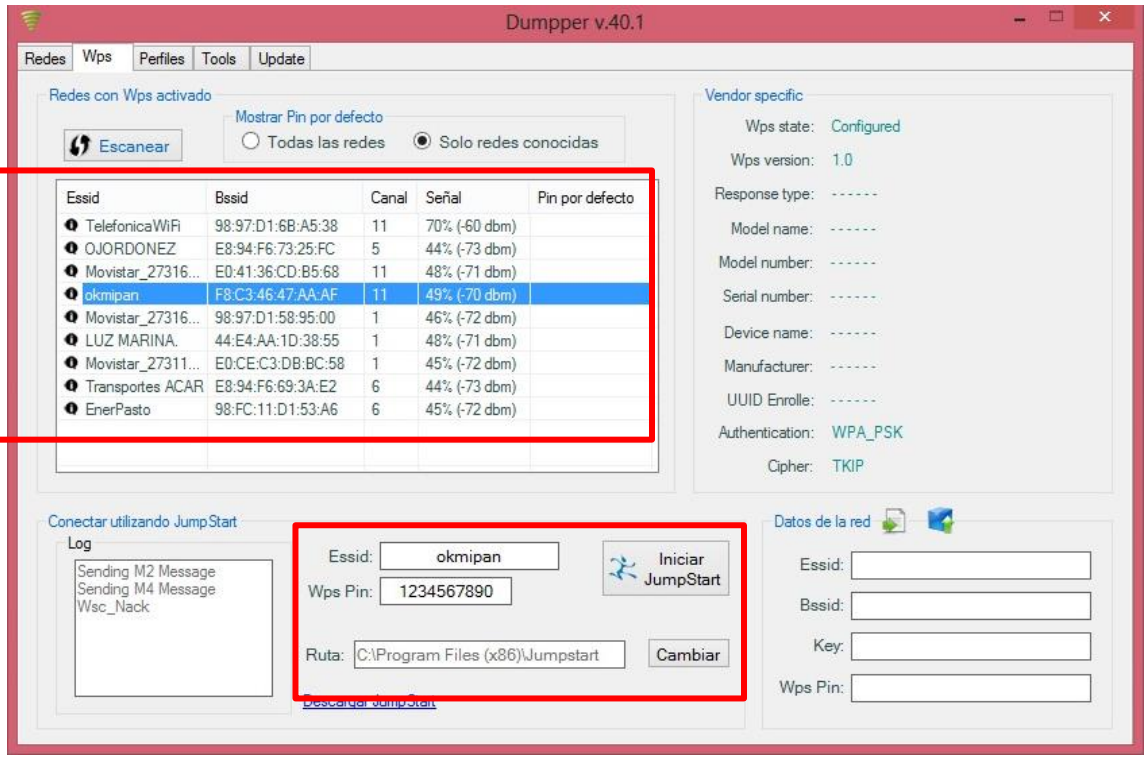
JumpStart es una herramienta que permite evaluar qué tipo de seguridad tienen una conexión inalámbrica (WiFi). Si una conexión, tiene activado el sistema WPS (WiFi Protected Setup), JumpStart, realiza un ataque por diccionario con el objetivo de conectarse a la red que está testeando. También realiza la evaluación a aquellas redes que contengan sistema WPA y WEP. Se procederá a evaluar la red inalámbrica WiFi de la empresa Panavias S.A.

Figura 36. Red inalámbrica Panavias S.A.

Fuente: Autor

Como se observa en la figura 35, se procede a seleccionar la red “okmipan” que corresponde a la conexión inalámbrica (WiFi) de la empresa Panavias S.A. Esta conexión tiene un cifrado WPA-PSK; WPA como el servidor de autenticación y PSK (Pre-Shared Key), el cual está diseñado para uso doméstico y redes de oficina, donde todos los equipos conectados a esta red, poseen la misma contraseña. WPA-PSK también es llamado WPA-Personal, y esta permite a la maquina asociarse a puntos de acceso utilizando codificación TKIP o AES. Con esta información, se procede a realizar la prueba a la red inalámbrica de la empresa Panavias S.A. con la extensión Dumpper de JumpStart, la cual al momento de solicitar el handshaking a la red objetivo, realiza un ataque de diccionario para autenticarse y poder conectarse posteriormente a la red.

Figura 37. Escaneo de redes vulnerables con Dumpper - JumpStart



Fuente: Autor

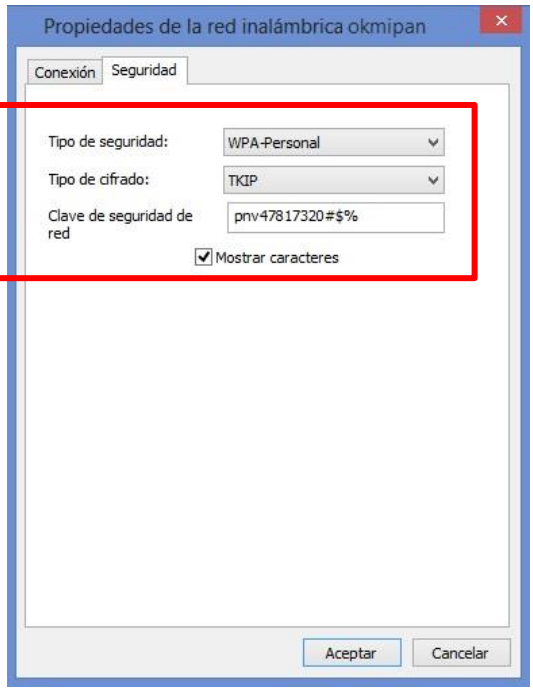
Como se observa en la figura 36, en el recuadro superior, se escanean las redes que tienen activado el sistema WPS y que pueden ser vulnerables a ataques de JumpStart o a otro tipo de ataques de fuerza bruta con diccionario para poder conectarse posteriormente. Se procede a seleccionar la red “okmipan”, que corresponde a la red inalámbrica de la empresa Panavias S.A. Luego, en el recuadro inferior, se observa la red seleccionada, la cual JumpStart tratara de conectarse por medio del WPS Pin 1234567890. JumpStar solicitara el handshaking a la red objetivo con este pin y luego tratara de realizar la posterior conexión. Esta herramienta permite también, almacenar los datos de una red luego de conectarse para luego poder ingresar. Una vez iniciado JumpStart, este selecciona automáticamente la red a escanear, de todas las posibles que se presentan y luego procede a conectarse tratando de autenticarse con el pin seleccionado. Si el intento es fallido, se puede ingresar manualmente otro WPS Pin y proceder nuevamente a intentar conectarse a una red. La interfaz de conexión con JumpStart a la red “okmipan” se observa en la siguiente imagen:

Figura 38. Conexión a red inalámbrica con JumpStart

Fuente: Autor

Luego de algunos minutos (el proceso de conexión, puede durar varios minutos), la conexión a la red “okmipan” se realiza con éxito, donde posteriormente se procede a revisar las propiedades de la red para verificar su contraseña la cual es pnv47817320#$% como se muestra en la figura 38. Con esto se demuestra que la red inalámbrica de Panavias S.A. es vulnerable a tipo de ataques de fuerza bruta con o sin diccionario.

Figura 39. Propiedades de la red inalámbrica okmipan



Fuente: Autor

7.4. APLICACION DE INSTRUMENTOS DE RECOLECCION DE INFORMACION

Se aplicaron los instrumentos para la recolección de la información, como lo fueron las entrevistas directas con el personal encargado de la oficina de sistemas y comunicaciones de Panavias S.A., con el objetivo de evaluar la seguridad física y lógica de la red, se aplicaron las listas de chequeo, estas tomadas directamente de la ISO/IEC 27002:2013 a los dominios directamente e indirectamente relacionados con la auditoria y se ejecutaron los cuestionarios de control, para establecer el nivel de riesgo de en cada proceso o dominio a evaluar.

7.4.1. Ejecución de Entrevistas

Se ejecutaron dos entrevistas, la primera para evaluar la seguridad física de la red y la otra para evaluar la seguridad lógica de la red de datos de la empresa Panavias S.A. realizadas directamente al encargado de la oficina de sistemas y comunicaciones con el objetivo de conocer acerca de la administración de esta.

Para evaluar la seguridad física de la red de la empresa Panavias S.A se tienen en cuenta los siguientes controles:

- Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados.
- Controles de utilización de los equipos de red y de comunicaciones, previniendo accesos inadecuados.
- Controles para la protección y tendido adecuado de cables y líneas de comunicaciones.
- Controles para perdida de la información y desastres.

De acuerdo a lo anterior, el formato de entrevista aplicado para evaluar la seguridad física de la red de datos de la empresa Panavias S.A. es el que se incluye en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Formato_EntrevistaSeguridadFisica”.

En la entrevista a la seguridad física de la red, se obtuvieron los siguientes hallazgos:

- No existen mecanismo de control de acceso al área de sistemas y cualquier funcionario de la empresa puede ingresar.

- El servidor no se encuentra en conjunto con los demás elementos de la red en la oficina de sistemas y comunicaciones, se encuentra entre la oficina financiera y el archivo.
- No existe inventario de los equipos de red.
- Se realiza mantenimiento a los equipos de red como al cableado y switches, pero no periódicamente. Esto lo realiza la empresa proveedora del servicio y lo hace en un plazo máximo de dos veces al año.
- No existen equipos para monitorización de la red en la empresa.
- El cableado UTP de la red no se encuentra protegido (blindado) ni etiquetado.
- El rack de comunicaciones no posee etiquetas para sus elementos y no se le ha organizado debidamente.
- Únicamente existen cámaras de vigilancia en el despacho y en la oficina de la gerencia de la empresa. Lo que los equipos de cómputo y de red son vulnerables a robo.
- No existen planes de contingencia en cuanto a fallas en las telecomunicaciones, lo que puede afectar la continuidad del negocio, ya que la mayoría de los procesos de la empresa, dependen del servicio de internet.
- Los equipos de cómputo y de red no se encuentran protegidos en su totalidad sobre posibles amenazas físicas y ambientales.

El formato diligenciado sobre la entrevista para evaluar la seguridad física de la red de datos en la empresa Panavias S.A. se encuentra en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Entrevista_SeguridadFisica”.

Para evaluar la seguridad lógica de la red en la empresa Panavias S.A se tienen en cuenta los siguientes controles:

- Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red.
- Control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas.
- Controles para asegurar que las transmisiones van solamente a usuarios autorizados.
- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.
- Controles de Seguridad en la Red.

De acuerdo a lo anterior, el formato de entrevista aplicado para evaluar la seguridad lógica de la red de datos de la empresa Panavias S.A. es el que se incluye en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Formato_EntrevistaSeguridadLogica”.

En la entrevista aplicada a la seguridad lógica de la red, se obtuvieron los siguientes hallazgos:

- No existen controles de errores para detectar fallas de transmisión en la red ya que no hay monitorización de esta.
- No existen controles para asegurar que las transmisiones van solamente a usuarios autorizados.
- No existen ni se utilizan herramientas para mapeo de redes, monitorear tráfico de red y herramientas para administrar la seguridad de los servicios de red.
- Nunca se han ejecutado herramientas que permitan identificar vulnerabilidades en la red ya que nunca se han realizado auditorias de seguridad informática.
- No existen ni se utilizan herramientas de criptografía para el cifrado de datos.
- Existen controles de seguridad en la red como firewalls, estos son los que vienen por defecto configurados en los routers, pero son vulnerables a cualquier intrusión. Esto se demostró en la fase de ejecución de pruebas de penetración, en donde se logró escanear toda la subred de datos de la empresa.

El formato diligenciado sobre la entrevista para evaluar la seguridad lógica de la red de datos en la empresa Panavias S.A. se encuentra en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Entrevista_SeguridadLogica”

7.4.2. Evaluación de dominios directamente relacionados

Los dominios directamente relacionados, son aquellos que ayudan a consecución directa del objetivo planteado para el desarrollo de la auditoria. Los dominios directamente relacionados son A9. Control de Acceso y A13. Seguridad en las Telecomunicaciones, donde se verifican los subdominios o controles existentes en la red de la empresa a través de la ejecución de listas de chequeo diseñadas directamente de la ISO/IEC 27002:2013, cuestionarios de control, para determinar el porcentaje de riesgo a la que está sometido el dominio evaluado y por último se realiza el análisis de riesgos de acuerdo a los hallazgos encontrados durante la auditoria.

7.4.2.1. Evaluación del Dominio A9. Control de Acceso

Se procede a evaluar el primer dominio directamente relacionado, que corresponde al dominio A9. Control de Acceso, el cual tiene por objetivo verificar los controles A9.1.2 de “Control de Acceso a las Redes y Servicios Asociados”, y A9.4.1 de Restricción de Acceso a la Información según la norma NTC/ISO/IEC 27002:2013. Para esto, se ejecutaran Listas de Chuequeo con cada uno de los subdominios a evaluar, cuestionarios de control y se realizara el análisis de riesgos con los hallazgos obtenidos.

7.4.2.1.1. Ejecución de listas de chequeo del dominio A9. Control de Acceso

Para el primer dominio directamente relacionado, el cual es el A9. Control de Acceso, se evalúan los siguientes subdominios:

- A9.1.2. Control de Acceso a las Redes y Servicios Asociados
- A9.4.1 Restricción de Acceso a la Información

El formato para la lista de chequeo para verificar los controles del dominio A9. Control de Acceso y sus subdominios, es el que se incluye en el Anexo D – A9. Control de Accesos, donde se denomina “Formato_ListadeChequeoA9”.

Tras la ejecución de la lista de chequeo para verificar los controles del primer dominio A9. Control de Acceso, en la red de datos de la empresa Panavias S.A, se obtienen los siguientes resultados:

- No existen procedimientos de autorización para determinar a quien se permiten acceder a las redes y servicios de red.
- No existen controles y procedimientos de gestión para proteger el acceso a la red y los servicios de red.
- No existen medios usados para acceder a las redes y servicios de red como VPN.
- No existe monitoreo del uso de los servicios de red.
- No existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos y sistemas críticos.

Se hace referencia al software Helysa GW en el cumplimiento de los controles de menús para controlar el acceso a la funcionalidad de aplicaciones y controles de los datos a los que puede tener un usuario particular.

El formato diligenciado sobre la lista de chequeo para para verificar los controles del dominio A9. Control de Acceso y sus subdominios de la red de datos en la empresa Panavias S.A. se encuentra en el Anexo D – Control de Acceso, el cual se denomina “ListadeChequeoA9”

7.4.2.1.2. Ejecución de cuestionarios de control del dominio A9. Control de Acceso

Estos cuestionarios cuantitativos, se realizan en conjunto con el encargado de la oficina de sistemas y comunicaciones de la empresa Panavias S.A, donde se da una calificación numérica, el cual va en una escala de menor a mayor, de 1 a 5 a los procesos para determinar su nivel de vulnerabilidad, donde 1 significa que no es importante tener el control y 5 significa que es importante que se tenga este.

Se aplica el cuestionario de control al primer dominio directamente relacionado, que corresponde a A9. Control de Acceso, donde se evalúa cuantitativamente los hallazgos obtenidos en la lista de chequeo. En conjunto se evalúan los procesos que corresponden a sus subdominios los cuales son A9.1.2. Control de acceso a las redes y servicios asociados y A9.4.1. Restricción de acceso a la información. El resumen del cuestionario de control se encuentra en la siguiente tabla:

Tabla 12. Resultados del cuestionario en el dominio A9. Control de Acceso

Pregunta	Si	No	N/A	Observaciones
¿Las redes y servicios de red solo tiene el acceso el usuario autorizado?	3			Los servicios de red solo accede el encargado pero al área de red accede cualquier funcionario.
¿Existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red?		4		No existen controles para determinar quién accede al área de red.
¿Existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?		4		No existen controles para proteger el acceso al área de red.
¿Existen medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		3		No existen medios de acceso a la red como VPN pero si existe la red inalámbrica.
¿Existen requisitos de autenticación de usuarios para acceder a diversos servicios de red?	2			Si existen requisitos de autenticación para acceder a la red.
¿Existe monitoreo del uso de los servicios de red?		5		No existe monitoreo de los servicios de red para detectar fallas.
¿Existen menús para controlar acceso a la funcionalidad de las aplicaciones?	1			Si existen control de accesos en relación al software Helysa GW
¿Existe control de los datos a los que puede tener acceso un usuario particular?	1			Si existe control de los datos en relación al software Helysa GW
¿Existe control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?	1			Si existen estos controles en relación al software Helysa GW y a la red. Solo el

Tabla 12. Resultados del cuestionario en el dominio A9. Control de Acceso (Continuación)

				usuario autorizado puede realizar estas acciones.
¿Existe control de los derechos de acceso de otras aplicaciones?	1			Si existen controles de acceso basados en roles, tanto para el software Helysa GW como para la red.
¿Existe limitación de la información contenida en las salidas?	3			Controles de salida mínimos del software Helysa e inexistentes en la red
¿Existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?		5		No existen controles para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.
TOTALES	**12**	**21**		
PUNTAJE TOTAL	**33**			

Fuente: Autor

Con los resultados, se procede a obtener el porcentaje del riesgo, que corresponde al cuestionario del dominio A9. Control de Acceso, donde se aplica el siguiente proceso:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

De acuerdo a los resultados, se procede a realizar el respectivo cálculo:

Porcentaje de riesgo parcial = (12 * 100) / 33 = 36.36
Porcentaje de riesgo = 100 – 36.36 = 63.64

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

De acuerdo a los resultados, se obtiene la siguiente información final respecto al cálculo del porcentaje y nivel de riesgo del dominio A9. Control de Acceso, según el cuestionario aplicado:

- Porcentaje de riesgo parcial = 36,36%
- Porcentaje de riesgo = **63,64%**
- Impacto según relevancia del proceso: **Riesgo Medio**

El formato diligenciado sobre el cuestionario de control para evaluar los controles del dominio A9. Control de Acceso y sus procesos seleccionados para la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. se encuentra en el Anexo D – A9. Control de Acceso, el cual se denomina “CuestionarioControlA9”.

7.4.2.1.3. Análisis de riesgos del dominio A9. Control de Acceso

Se procede a realizar el análisis de riesgos correspondiente al dominio A9. Control de Acceso, con los hallazgos encontrados en las listas de chequeo y la evaluación obtenida de los cuestionaros de control. De acuerdo al porcentaje de riesgos evaluado en los cuestionarios del presente dominio, este se clasifica de Riesgo Medio.

- **Listado de vulnerabilidades para el dominio A9. Control de Acceso**

El listado de vulnerabilidades se obtiene al verificar la ausencia o no cumplimiento de los controles realizados en las listas de chequeo y los cuestionarios de control. Para el dominio A9. Control de Acceso, se identificaron las siguientes vulnerabilidades:

Tabla 13. Listado de vulnerabilidades del dominio A9. Control de Acceso

Ítem	Vulnerabilidad
R001	No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.
R002	No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.
R003	No existen medios usados para acceder a las redes y servicios de red como el uso de VPN.
R004	No existe monitoreo del uso de los servicios de red
R005	No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.

Fuente: Autor

- **Calculo de análisis de riesgo para el dominio A9. Control de Acceso**

De acuerdo a las vulnerabilidades encontradas en el dominio A9. Control de Acceso, se procede a hacer una valoración estimando la probabilidad por el impacto acerca de las consecuencias que podrían traer y la probabilidad de ocurrencia. El cálculo del análisis de riesgo para cada una de las vulnerabilidades encontradas en el dominio A9. Control de Acceso, se muestra en la siguiente tabla:

Tabla 14. Calculo de análisis de riesgo del dominio A9. Control de Acceso

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R001	No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.	3	2	**6**
R002	No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.	3	2	**6**
R003	No existen medios usados para acceder a las redes y servicios de red como el uso de VPN.	4	3	**12**

Tabla 14. Calculo de análisis de riesgo del dominio A9. Control de Acceso (Continuación)

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R004	No existe monitoreo del uso de los servicios de red	4	4	**16**
R005	No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.	4	4	**16**

Fuente: Autor

- **Matriz de riesgos para el dominio A9. Control de Acceso**

Se trasladan los resultados obtenidos en el cálculo del análisis de riesgos del dominio A9. Control de Acceso a una matriz para poder observar fácilmente los resultados obtenidos, donde se asigna con colores para cada una de la celdas asociadas a la escala (Verde=Riesgo Bajo, Amarillo=Riesgo Medio, Rojo=Riesgo Alto) y de esta manera poder dictaminar el tratamiento para los riesgos evaluados. La matriz de riesgo para el dominio A9. Control de Acceso con sus riesgos evaluados se muestra en la siguiente tabla:

Tabla 15. Matriz de riesgos del dominio A9. Control de Acceso

PROBABILIDAD	**4**				**R004, R005**
	3			**R003**	
	2			**R001, R002**	
	1				
		1	**2**	**3**	**4**
	IMPACTO				

Fuente: Autor

De acuerdo a la matriz de riesgo evaluada, los riesgos que necesitan mayor tratamiento son los que corresponde al R004 (No existe monitoreo del uso de los servicios de red) y R005 (No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes). Estos son los que se encuentran a mayor escala y se deben tratar inmediatamente. El R003 (No existen medios usados para acceder a las redes y servicios de red como el uso de VPN), también debe tratarse, ya que de acuerdo a la escala se considera de riesgo alto, pero en menor grado a los dos anteriores. Los riesgos R001 Y R002 se clasifican como riesgo medio, de igual manera se deben establecer controles para que su probabilidad de ocurrencia no se incremente y generen un impacto mayor.

7.4.2.2. Evaluación del dominio A13. Seguridad en las Telecomunicaciones

Se procede a evaluar el segundo dominio directamente relacionado, que corresponde al dominio A13. Seguridad en las Telecomunicaciones, el cual tiene por objetivo verificar los controles A13.1.1 de “Control de Redes”, A13.1.2 de “Seguridad de los Servicios de Red”, y A13.1.3 de “Separación en las Redes” según la norma NTC/ISO/IEC 27002:2013. Para esto, se ejecutaran Listas de Chuequeo con cada uno de los subdominios a evaluar, cuestionarios de control y se realizara el análisis de riesgos con los hallazgos obtenidos.

7.4.2.2.1. Ejecución de listas de chequeo del dominio A13. Seguridad en las Telecomunicaciones

Para el segundo dominio directamente relacionado, el cual es el A13. Seguridad en las Telecomunicaciones, se evalúan los siguientes subdominios:

- Subdominio A13.1.1 Controles de Redes
- Subdominio A13.1.2 Seguridad de los Servicios de Red
- Subdominio A13.1.3 Separación en las Redes

El formato para la lista de chequeo para verificar los controles del dominio A13. Seguridad en las Telecomunicaciones y sus subdominios, es el que se incluye en el Anexo F – A13. Seguridad en las Telecomunicaciones, donde se denomina “Formato_ListadeChequeoA13”.

Tras la ejecución de la lista de chequeo para verificar los controles del segundo dominio directamente relacionado A13. Seguridad en las Telecomunicaciones, en la red de datos de la empresa Panavias S.A, se obtienen los siguientes resultados:

- No se establecen responsabilidades y procedimientos para la gestión de los equipos de redes.
- No se separa la responsabilidad operacional de las operaciones de cómputo en las redes.
- No existen controles para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas.
- No existen controles para proteger los sistemas y aplicaciones conectados.
- No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- No se cuenta con un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información.
- No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.
- No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.
- No existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad.
- No existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.
- La red se no encuentra dividida en dominios de red separados ósea que no se encuentra segmentada.

En el subdominio A13.1.3. Separación de las Redes, tres controles no aplicaron ya que la red, como su primer control lo verifica, no se encuentra segmentada o separada por dominios.

El formato diligenciado sobre la lista de chequeo para para verificar los controles del dominio A13. Seguridad en las Telecomunicaciones y sus subdominios seleccionados para la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. se encuentra en el Anexo F – Seguridad en las Telecomunicaciones, el cual se denomina “ListadeChequeoA13”.

7.4.2.2.2. Ejecución de cuestionarios de control del dominio A13. Seguridad en las Telecomunicaciones

Estos cuestionarios cuantitativos, se realizan en conjunto con el encargado de la oficina de sistemas y comunicaciones de la empresa Panavias S.A, donde se da una calificación numérica, el cual va en una escala de menor a mayor, de 1 a 5 a los procesos para determinar su nivel de vulnerabilidad, donde 1 significa que no es importante tener el control y 5 significa que es importante que se tenga este.

Los resultados arrojados en la aplicación del cuestionario de control al segundo dominio directamente relacionado, que corresponde a A13. Seguridad en las Telecomunicaciones, arrojan los hallazgos más críticos, debido a la gran ausencia de controles de seguridad en la red. Se evalúan los procesos que corresponden a sus subdominios A13.1.1. Controles de redes, A13.1.2. Seguridad de los servicios de red y A13.1.3. Separación en las redes. El resumen de los resultados del cuestionario de control aplicado se encuentra en la siguiente tabla:

Tabla 16. Resultados del cuestionario en el dominio A13. Seguridad en las Telecomunicaciones

Pregunta	Si	No	N/A	Observaciones
¿Se establecen responsabilidades y procedimientos para la gestión de equipos de redes?		3		Se establecen responsabilidades pero no hay procedimientos para la gestión de los equipos de redes.
¿Se separa la responsabilidad operacional por las redes, de las operaciones de cómputo?		4		No se incluye el desarrollo de los procedimientos de operación apropiados para la red
¿Existen controles para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?		5		No existen controles para salvaguardar los servicios de seguridad informática en la red.

Tabla 16. Resultados del cuestionario en el dominio A13. Seguridad en las Telecomunicaciones (Continuación)

Pregunta	Si	No	N/A	Observaciones
¿Existen controles para proteger los sistemas y aplicaciones conectados?		4		No existen este tipo de controles para la red de la empresa.
¿Se cuenta con controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados?		4		No existen este tipo de controles para la red de la empresa.
¿Se cuenta con un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?		5		No existe este tipo de control ya que no se monitorean los servicios de la red.
¿Se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?		5		No se coordinan actividades para la seguridad informática de la red ya que la gerencia no ha establecido procedimientos.
Los sistemas en la red, ¿se autentican?	2			Los sistemas de red si se autentican (aplicación web y servidor) lo mismo que el software Helysa GW, pero se debería reforzar su seguridad.
¿Se restringe la conexión a dispositivos no autorizados a los sistemas a la red?		3		No hay controles de administración de dispositivos conectados a la red
¿Existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red?		3		No existe tecnología relacionada con criptografía. El host tiene desactivad los servicios de cifrado.

Tabla 16. Resultados del cuestionario en el dominio A13. Seguridad en las Telecomunicaciones (Continuación)

Pregunta	Si	No	N/A	Observaciones
¿Existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red?		4		No existen controles para asegurar la conexión segura a la red
¿Existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red?		3		No existen este tipo de procedimientos.
¿La red se encuentra dividida en dominios de red separados?		5		La red no se encuentra segmentada.
¿Se permite el acceso entre dominios de redes controlando el acceso utilizando firewalls o enrutado de filtrado?				Este control no aplica porque la red no se encuentra segmentada.
¿Las redes inalámbricas (redes externas) se encuentran separadas a las redes internas?				Este control no aplica porque la red no se encuentra segmentada.
¿Se emplean mecanismos de autenticación, criptografía y tecnologías de control de accesos de redes entre las redes?				Este control no aplica porque la red no se encuentra segmentada.
TOTALES	**2**	**48**		
PUNTAJE TOTAL	**50**			

Fuente: Autor

Con los resultados, se procede a obtener el porcentaje del riesgo, que corresponde al cuestionario del dominio A13. Seguridad en las Telecomunicaciones, donde se aplica el siguiente proceso:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

De acuerdo a los resultados, se procede a realizar el respectivo cálculo:

Porcentaje de riesgo parcial = (2*100) / 50 = 4
Porcentaje de riesgo = 100 – 4 = 96

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

De acuerdo a los resultados, se obtiene la siguiente información final respecto al cálculo del porcentaje y nivel de riesgo del dominio A13. Seguridad en las Telecomunicaciones, según el cuestionario aplicado:

- Porcentaje de riesgo parcial = 4 %
- Porcentaje de riesgo = **96 %**
- Impacto según relevancia del proceso: **Riesgo Alto**

Los resultados muestran que en este dominio se precisa elaborar controles correctivos ya que su porcentaje de riesgo es Alto. El formato diligenciado sobre el cuestionario de control para evaluar los controles del dominio A13. Seguridad en las Telecomunicaciones y sus procesos seleccionados para la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. se encuentra en el Anexo F – A13. Seguridad en las Telecomunicaciones, el cual se denomina “CuestionarioControlA13”.

7.4.2.2.3. Análisis de riesgos del dominio A13. Seguridad en las Telecomunicaciones

Se procede a realizar el análisis de riesgos correspondiente al dominio A13. Seguridad en las Telecomunicaciones, con los hallazgos encontrados en las listas de chequeo y la evaluación obtenida de los cuestionaros de control. Debido a la gran ausencia critica de controles en la red, el porcentaje de riesgos evaluado en los cuestionarios del presente dominio, este se clasifica de Riesgo Alto y es que le requiere mayor gestión.

- **Listado de vulnerabilidades para el dominio A13. Seguridad en las Telecomunicaciones**

El listado de vulnerabilidades se obtiene al verificar la ausencia o no cumplimiento de los controles realizados en las listas de chequeo y los cuestionarios de control. Para el dominio A13. Seguridad en las Telecomunicaciones, se identificaron las siguientes vulnerabilidades:

Tabla 17. Listado de vulnerabilidades del dominio A13. Seguridad en las Telecomunicaciones

Ítem	Vulnerabilidad
R006	No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.
R007	No se incluye el desarrollo de los procedimientos de operación apropiados para la red.
R008	No existen controles para salvaguardar los servicios de seguridad informática en la red.
R009	No existen controles para proteger los sistemas y aplicaciones conectados.
R010	No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
R011	No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.
R012	No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.
R013	No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.
R014	No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.
R015	No existen controles para asegurar la conexión segura a la red.
R016	No existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.
R017	La red se no se encuentra dividida en dominios de red separados o segmentada.
R018	Vulnerabilidad por puertos sensibles abiertos y expuestos.

Fuente: Autor

- **Calculo de análisis de riesgo para el dominio A13. Seguridad en las Telecomunicaciones**

De acuerdo a las vulnerabilidades encontradas en el dominio A13. Seguridad en las Telecomunicaciones, se procede a hacer una valoración estimando la probabilidad por el impacto acerca de las consecuencias que podrían traer y la probabilidad de ocurrencia. El cálculo del análisis de riesgo para cada una de las vulnerabilidades encontradas en el dominio A13. Seguridad en las Telecomunicaciones, se muestra en la tabla 22.

Tabla 18. Calculo de análisis de riesgo del dominio A13. Seguridad en las Telecomunicaciones

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R006	No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.	4	3	**12**
R007	No se incluye el desarrollo de los procedimientos de operación apropiados para la red.	3	4	**12**
R008	No existen controles para salvaguardar los servicios de seguridad informática en la red.	4	4	**16**
R009	No existen controles para proteger los sistemas y aplicaciones conectados.	4	4	**16**
R010	No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.	4	3	**12**
R011	No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.	4	3	**12**

Tabla 18. Calculo de análisis de riesgo del dominio A13. Seguridad en las Telecomunicaciones (Continuación)

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R012	No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.	3	4	**12**
R013	No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.	3	3	**9**
R014	No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.	2	3	**6**
R015	No existen controles para asegurar la conexión segura a la red.	3	3	**9**
R016	No existen procedimientos del uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.	3	3	**9**
R017	La red se no se encuentra dividida en dominios de red separados o segmentada.	4	3	**12**
R018	Vulnerabilidad por puertos sensibles abiertos y expuestos.	4	4	**16**

Fuente: Autor

- **Matriz de riesgo para el dominio A13. Seguridad en las Telecomunicaciones**

Se trasladan los resultados obtenidos en el cálculo del análisis de riesgos del dominio A13. Seguridad en las Telecomunicaciones a una matriz para poder

observar fácilmente los resultados obtenidos, donde se asigna con colores para cada una de la celdas asociadas a la escala (Verde=Riesgo Bajo, Amarillo=Riesgo Medio, Rojo=Riesgo Alto) y de esta manera poder dictaminar el tratamiento para los riesgos evaluados. La matriz de riesgo para el dominio A13. Seguridad en las Telecomunicaciones con sus riesgos evaluados se muestra en la siguiente tabla:

Tabla 19. Matriz de riesgos del dominio A13. Seguridad en las Telecomunicaciones

PROBABILIDAD	**4**			**R006, R010, R011, R017**	**R008, R009 R018**
	3			**R013, R015, R016**	**R012, R007**
	2			**R014**	
	1				
		1	**2**	**3**	**4**
	IMPACTO				

Fuente: Autor

De acuerdo a la matriz de riesgo evaluada para este dominio, se muestran resultados críticos en relación a la gran ausencia de controles presentes en la red de datos de la empresa Panavias S.A. Los riesgos de mayor criticidad y que necesitan mitigación inmediata, son los que corresponden a R008 (No existen controles para salvaguardar los servicios de seguridad informática en la red), R009 (No existen controles para proteger los sistemas y aplicaciones conectados) y R018 (Vulnerabilidad por puertos sensibles abiertos y expuestos). En la escala se muestran riesgos de clasificación alta en menor grado pero que también se deben implementar controles como lo son R006 (No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red), R010 (No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados), R017 (No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red), R017 (La red se no se encuentra dividida en dominios de red separados o segmentada) y R012 (No se coordinan actividades de gestión para optimizar el servicio de la

organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información). Todos estos riesgos mencionados, se debe considerar tratar inmediatamente. Se encontraron de igual manera riesgos de clasificación alta pero de menor probabilidad como lo son R007, R013, R015, R016. Los riesgos de clasificación alta están asociados con planes de actuación correctivas. Los riesgos de clasificación media, son aquellos que necesitan investigación y determinar el tipo de tratamiento. Estos están asociados con planes de actuación preventivas.

7.4.3. Evaluación de dominios indirectamente relacionados

Los dominios indirectamente relacionados son aquellos, que aunque no estén implicados con el desarrollo del objetivo de la auditoria, es preciso revisarlos para verificar su cumplimiento y funcionamiento dentro de la empresa. Estos dominios corresponden al A5. Políticas de Seguridad de la Información, A6. Organización de la Seguridad de la Información y A11. Seguridad Física y del Entorno donde se verifican los subdominios o controles existentes en la red de la empresa a través de la ejecución de listas de chequeo diseñadas directamente de la ISO/IEC 27002:2013, cuestionarios de control, para determinar el porcentaje de riesgo a la que está sometido el dominio evaluado y por último se realiza el análisis de riesgos de acuerdo a los hallazgos encontrados durante la auditoria.

7.4.3.2. Evaluación del Dominio A5. Políticas de Seguridad de la Información

Se procede a evaluar el primer dominio indirectamente relacionado, que corresponde al dominio A5. Políticas de Seguridad de la Información, el cual tiene por objetivo verificar los controles A5.1.1. “Políticas para la Seguridad de la Información” y A5.1.2. “Revisión de las Políticas para la Seguridad de la Información”, según la norma NTC/ISO/IEC 27002:2013. Para esto, se ejecutaran Listas de Chuequeo con cada uno de los subdominios a evaluar, cuestionarios de control y se realizara el análisis de riesgos con los hallazgos obtenidos.

7.4.3.2.1. Ejecución de listas de chequeo del dominio A5. Políticas de Seguridad de la Información

Para el dominio A5. Políticas de Seguridad de la Información, se evalúan los siguientes subdominios:

- Subdominio A5.1.1. Políticas para la Seguridad de la Información
- Subdominio A5.1.2. Revisión de las Políticas para la Seguridad de la Información

De acuerdo a lo anterior, el formato para la lista de chequeo para verificar los controles del dominio A5. Políticas de Seguridad de la Información, es el que incluye en el Anexo B – A5. Políticas de Seguridad de la Información, donde se denomina “Formato_ListadeChequeoA5”.

Al implementar la lista de chequeo para evaluar el presente dominio, se encuentra que la empresa Panavias S.A. nunca ha establecido directrices para la creación de políticas de seguridad de la información, por lo tanto, la lista de chequeo que corresponde al dominio A5. Políticas de Seguridad de la Información, no se ejecutó. Para esto, se debe formular recomendaciones donde se deben implementar estas políticas en la empresa.

En la lista de chequeo, los controles establecidos para su verificación no aplicaron ya que no existen políticas de seguridad en la empresa. Por lo tanto se establece que tampoco hay controles establecidos para la red de datos. El formato de lista de chequeo del dominio A5. Políticas de Seguridad de la Información, se encuentra en el Anexo B – Políticas de Seguridad de la Información, el cual se denomina “ListadeChequeoA5” donde se establece que no aplicaron los controles y por lo tanto no se ejecutó dicho formato ya que no existen políticas en la empresa.

7.4.3.2.2. Ejecución de cuestionarios de control del dominio A5. Políticas de Seguridad de la Información

Al no aplicarse las listas de chequeo en la verificación de los controles del dominio A5. Políticas de Seguridad de la Información, debido a que no existe documentación en referencia a políticas de seguridad en la empresa Panavias S.A. no se aplican los cuestionarios de control cuantitativos para determinar el porcentaje de riesgo de los hallazgos a los que están expuestos en este dominio.

7.4.3.2.3. Análisis de riesgos del dominio A5. Políticas de Seguridad de la Información

Al no aplicarse las listas de chequeo y los cuestionarios de control en este dominio, debido a la ausencia de documentación en referencia a políticas de

seguridad, no se encuentran hallazgos en la auditoria, por lo tanto no se realiza el análisis de riesgos. Se realiza la recomendación de implementar esta documentación, en relación a los controles de establecimiento de documentación referente a políticas de seguridad de la información y la revisión de las mismas, de acuerdo a la normatividad.

7.4.3.3. Evaluación del Dominio A6. Organización de la Seguridad de la Información

Se procede a evaluar el segundo dominio indirectamente relacionado, que corresponde al dominio A6. Organización de la Seguridad de la Información, el cual tiene por objetivo verificar los controles A6.1.1 de “Roles y Responsabilidades para la Seguridad de la Información”, según la norma NTC/ISO/IEC 27002:2013.. Para esto, se ejecutaran listas de chequeo con cada uno de los subdominios a evaluar, cuestionarios de control y se realizara el análisis de riesgos con los hallazgos obtenidos.

7.4.3.3.1. Ejecución de listas de chequeo del dominio A6. Organización de la Seguridad de la Información

Para el segundo dominio indirectamente relacionado, el cual es el A6. Organización de la Seguridad de la Información, se evalúan los siguientes subdominios:

- A6.1.1 Roles y Responsabilidades para la Seguridad de la Información

El formato de lista de chequeo para verificar los controles del presente dominio, es el que se incluye en el Anexo C – A6. Organización de la Seguridad de la Información, donde se denomina “Formato_ListadeChequeoA6”.

Al no existir políticas de seguridad en la empresa Panavias S.A. tampoco se han establecido directrices en relación a la organización de la seguridad de la información, como lo son el establecimiento de roles y responsabilidades para la gestión de los activos y procesos relacionados. Esto se establece en el segundo dominio indirecto a verificar, el A6. Organización de la Seguridad de la Información, donde al no existir estos controles, no aplicaron.

El formato de lista de chequeo del dominio A6. Organización de la Seguridad de la Información, se encuentra en el Anexo C – Organización de la Seguridad de la

Información, el cual se denomina “ListadeChequeoA6” donde se establece que los controles no aplicaron, al igual que el anterior dominio y por lo tanto no se ejecutó dicho formato ya que no existen políticas en la empresa.

7.4.3.3.2. Ejecución de cuestionarios de control del dominio A6. Organización de la Seguridad de la Información

Al no aplicarse las listas de chequeo en la verificación de los controles del dominio A6. Organización de la Seguridad de la Información, debido a que no existe documentación en referencia a políticas de seguridad y su organización en la empresa Panavias S.A. no se aplican los cuestionarios de control cuantitativos para determinar el porcentaje de riesgo de los hallazgos a los que están expuestos en este dominio.

7.4.3.3.3. Análisis de riesgos del dominio A6. Organización de la Seguridad de la Información

Al no aplicarse las listas de chequeo y los cuestionarios de control en este dominio, debido a la ausencia de documentación en referencia a políticas de seguridad, no se encuentran hallazgos en la auditoria, por lo tanto no se realiza el análisis de riesgos. Se realiza la recomendación de implementar esta documentación, en relación a los controles de establecimiento de documentación referente a roles y responsabilidades de la seguridad de la información, de acuerdo a la normatividad.

7.4.3.4. Evaluación del Dominio A11. Seguridad Física y del Entorno

Se procede a evaluar el tercer dominio indirectamente relacionado, que corresponde al dominio A11. Seguridad Física y del Entorno, el cual tiene por objetivo verificar los controles A11.2.1 de “Ubicación y Protección de los Equipos” y A11.2.3 de “Seguridad del Cableado”, según la norma NTC/ISO/IEC 27002:2013. Para esto, se ejecutaran Listas de Chuequeo con cada uno de los subdominios a evaluar, cuestionarios de control y se realizara el análisis de riesgos con los hallazgos obtenidos.

7.4.3.4.1. Ejecución de listas de chequeo del dominio A11. Seguridad Física y del Entorno

Para el último dominio indirectamente relacionado, el cual es el A11. Seguridad Física y del Entorno, se evalúan los siguientes subdominios:

- Subdominio A11.2.1 Ubicación y Protección de los Equipos
- Subdominio A11.2.3 Seguridad del Cableado

El formato de lista de chequeo para verificar los controles del dominio A11. Seguridad Física y del Entorno es el que se incluyen en el Anexo E – A11. Seguridad Física y del Entorno, donde se denomina "Formato_ListadeChequeoA11".

El tercer dominio indirectamente relacionado es el A11. Seguridad Física y del Entorno, donde se verifican el cumplimiento de dos subdominios o controles existentes en la empresa, se obtienen los siguientes resultados:

- Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas.
- No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo. Existen cámaras de vigilancia y alarmas contra incendio pero estas no abarcan toda el área de la empresa.
- Las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información no o cuentan con protección.

El formato diligenciado sobre la lista de chequeo para para verificar los controles del dominio A11. Seguridad Física y del Entorno y sus subdominios seleccionados para la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. se encuentra en el Anexo E – Seguridad Física y del Entorno, el cual se denomina "ListadeChequeoA11".

7.4.3.4.2. Ejecución de cuestionarios del dominio A11. Seguridad Física y del Entorno

Estos cuestionarios cuantitativos, se realizan en conjunto con el encargado de la oficina de sistemas y comunicaciones de la empresa Panavias S.A, donde se da una calificación numérica, el cual va en una escala de menor a mayor, de 1 a 5 a los procesos para determinar su nivel de vulnerabilidad, donde 1 significa que no es importante tener el control y 5 significa que es importante que se tenga este.
De los dominios indirectamente relacionados, el único que arrojo hallazgos en su verificación es el dominio A11. Seguridad Física y del Entorno donde se procede a evaluar evalúa cuantitativamente sus resultados. En conjunto se evalúan los procesos que corresponde a los subdominios A11.2.1. Ubicación y protección de los equipos y A11.2.3. Seguridad del cableado. El resumen de los resultados del cuestionario de control se muestra en la siguiente tabla:

Tabla 20. Resultados del cuestionario en el dominio A11. Seguridad Física y del Entorno

Pregunta	Si	No	N/A	Observaciones
¿Las instalaciones de procesamiento de información y de redes están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas?		5		Los equipos de red no están ubicados en su lugar idóneo. No hay ordenamiento del rack y el servidor no se encuentra en el área de red.
¿Se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo?		4		Existen cámaras de vigilancia y alarmas contra incendio, pero estas no abarcan toda la empresa, por lo que son vulnerables y el cableado UTP es de cobre y este es vulnerable a interferencias.

Tabla 20. Resultados del cuestionario en el dominio A11. Seguridad Física y del Entorno (Continuación)

Pregunta	Si	No	N/A	Observaciones
¿Se hace seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información y de redes?	4			El seguimiento lo hace la empresa proveedora, pero no lo realiza periódicamente. Es preciso que esto se gestione con el personal de la misma empresa.
Las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información, ¿son subterráneas o cuentan con otra protección alternativa?		5		El cableado UTP de cobre no cuenta con protección de blindaje.
¿Los cables de energía eléctrica se encuentran separados de los cables de telecomunicaciones para evitar interferencias?	3			El cableado si se encuentra separado, pero existen inferencias por ser cableado de cobre. Es necesario cambiar a fibra óptica.
¿Existen controles para inspecciones físicas al cableado?	4			El seguimiento lo hace la empresa proveedora, pero no lo realiza periódicamente. Es preciso que esto se gestione con el personal de la misma empresa.
TOTALES	**11**	**14**		
PUNTAJE TOTAL	**25**			

Fuente: Autor

Con los resultados, se procede a obtener el porcentaje del riesgo, que corresponde al cuestionario del dominio A11. Seguridad Física y del Entorno, donde se aplica el siguiente proceso:

Porcentaje de riesgo parcial = (Total SI * 100) / Total
Porcentaje de riesgo = 100 - Porcentaje de riesgo parcial

De acuerdo a los resultados, se procede a realizar el respectivo cálculo:

Porcentaje de riesgo parcial = (11 * 100) / 25 = 44
Porcentaje de riesgo = 100 – 44 = 56

Para determinar el nivel de riesgo total, se tiene en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo
31% - 70% = Riesgo Medio
71% - 100% = Riesgo Alto

De acuerdo a los resultados, se obtiene la siguiente información final respecto al cálculo del porcentaje y nivel de riesgo del dominio A11. Seguridad Física y del Entorno, según el cuestionario aplicado:

- Porcentaje de riesgo parcial = 44%
- Porcentaje de riesgo = **56 %**
- Impacto según relevancia del proceso: **Riesgo Medio**

El formato diligenciado sobre el cuestionario de control para evaluar los controles del dominio A11. Seguridad Física y del Entorno y sus procesos seleccionados para la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. se encuentra en el Anexo E – A11. Seguridad Física y del Entorno, el cual se denomina “CuestionarioControlA11”.

7.4.3.4.3. Análisis de riesgos del dominio A11. Seguridad Física y del Entorno

Se procede a realizar el análisis de riesgos correspondiente al dominio A11. Seguridad Física y del Entorno, con los hallazgos encontrados en las listas de chequeo y la evaluación obtenida de los cuestionaros de control. De acuerdo al

porcentaje de riesgos evaluado en los cuestionarios del presente dominio, este se clasifica de Riesgo Medio.

- **Listado de vulnerabilidades para el dominio A11. Seguridad Física y del Entorno**

El listado de vulnerabilidades se obtiene al verificar la ausencia o no cumplimiento de los controles realizados en las listas de chequeo y los cuestionarios de control. Para el dominio A11. Seguridad Física y del Entorno, se identificaron las siguientes vulnerabilidades:

Tabla 21. Listado de vulnerabilidades del dominio A11. Seguridad Física y del Entorno

Ítem	Vulnerabilidad
R019	Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas
R020	No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo
R021	El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.
R022	Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.

Fuente: Autor

- **Calculo de análisis de riesgo para dominio A11. Seguridad Física y del Entorno**

De acuerdo a las vulnerabilidades encontradas en el dominio A11. Seguridad Física y del Entorno, se procede a hacer una valoración estimando la probabilidad por el impacto acerca de las consecuencias que podrían traer y la probabilidad de ocurrencia. El cálculo del análisis de riesgo para cada una de las vulnerabilidades

encontradas en el dominio A11. Seguridad Física y del Entorno, se muestra en la siguiente tabla:

Tabla 22. Calculo de análisis de riesgo del dominio A11. Seguridad Física y del Entorno

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R019	Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas	4	3	**12**
R020	No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo	2	4	**8**
R021	El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.	4	2	**8**

Tabla 22. Calculo de análisis de riesgo del dominio A11. Seguridad Física y del Entorno

No	Vulnerabilidad	Probabilidad	Impacto	Evaluación del Riesgo
R022	Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.	4	3	**12**

Fuente: Autor

- **Matriz de riesgo para dominio A11. Seguridad Física y del Entorno**

Se trasladan los resultados obtenidos en el cálculo del análisis de riesgos del dominio A11. Seguridad Física y del Entorno a una matriz para poder observar fácilmente los resultados obtenidos, donde se asigna con colores para cada una de la celdas asociadas a la escala (Verde=Riesgo Bajo, Amarillo=Riesgo Medio, Rojo=Riesgo Alto) y de esta manera poder dictaminar el tratamiento para los riesgos evaluados. La matriz de riesgo para el dominio A11. Seguridad Física y del Entorno con sus riesgos evaluados se muestra en la tabla 30.

Tabla 23. Matriz de riesgos del dominio A11. Seguridad Física y del Entorno

PROBABILIDAD	**4**		**R021**	**R019, R022**	
	3				
	2				**R020**
	1				
		1	**2**	**3**	**4**
	IMPACTO				

Fuente: Autor

De acuerdo a la matriz de riesgo evaluada para este dominio, los riesgos que se debe realizar el tratamiento inmediato, son los que corresponden a R019 (Las instalaciones de procesamiento de información y de redes no están ubicadas

cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas), R022 (El seguimiento y mantenimiento de las instalaciones de redes no lo realiza el personal encargado de la misma empresa) y R023 (Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa). Se identifican otros dos riesgos de clasificación alta, como lo son R021 y R020, que a pesar son de menor grado, también se debe realizar el tratamiento respectivo. Todos los riesgos evaluados en el dominio A11. Seguridad Física y del Entorno, se clasifican como Riesgo Alto y se debe realizar el plan de actuación correctiva correspondiente.

7.5. RESULTADOS DE LA AUDITORIA

Una vez concluida la fase de ejecución, se organizan los papeles de trabajo de la auditoria que corresponden a los instrumentos de recolección de la información como lo son los resultados de las entrevistas, listas de chequeo, cuestionarios de control, como también los resultados del análisis de riesgos realizado a cada proceso dominio auditado.

7.5.1. Dictamen de Auditoria y Guías de Hallazgo

Se procede a documentar y organizar los resultados de la auditoria, realizadas durante la fase de ejecución, en las guías de hallazgo de la auditoria. Estas contienen la descripción del hallazgo, la evaluación del riesgo realizada con sus causas y posibles efectos o amenazas que se pueden presentar. Los efectos se identifican de acuerdo al catálogo de amenazas del libro de Magerit V3. En las guías de hallazgo también se documentan las recomendaciones para corregir dicho riesgo y las evidencias del hallazgo, donde se documenta en que prueba o instrumento se encontró el riesgo.

7.5.1.1. Hallazgos del dominio A9. Control de Acceso

A continuación se documentan los hallazgos, con mayor relevancia obtenidos durante el análisis de riesgos y a los que se les debe mitigar de forma inmediata.

El primero corresponde al riesgo denominado R004 (No existe monitoreo del uso de los servicios de red), donde se documenta el hallazgo y las recomendaciones en la siguiente tabla:

Tabla 24. Guía de hallazgos para el riesgo R004

Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Riesgo	R004 - No existe monitoreo del uso de los servicios de red.
Descripción del Hallazgo	
No existe un monitoreo acerca del uso de los servicios de red, el cual permita establecer un seguimiento de la actividad de la red de la empresa. No existen herramientas que permitan el mapeo de redes, revisar el tráfico de red y también el uso de herramientas aplicadas a los servicios de red como el uso activo de protocolos criptográficos para el cifrado de la información.	

Tabla 24. Guía de hallazgos para el riesgo R004 (Continuación)

Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: No se han establecido controles para realizar el registro de la actividad de la red en la empresa. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.7] Deficiencias en la organización [E.24] Caída del sistema por agotamiento de recursos **[A] Ataques deliberados** [A.8] Difusión de software dañino [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.24] Denegación de servicio
Recomendaciones – Acciones Correctivas
El administrador de red es el encargado de gestionar y controlar los servicios de red que permitan el correcto funcionamiento de la infraestructura telemática. Además, está a cargo de implementar medidas de protección adecuadas, supervisar los registros y actividades que permitan salvaguardar la red tanto en

Tabla 24. Guía de hallazgos para el riesgo R004 (Continuación)

su parte física, como lógica. También implementar herramientas que permitan gestionar y controlar todos los procesos de los servicios de red, como lo son: 1. Herramientas para el mapeo de redes: permiten identificar y gestionar los procesos y servicios de la red y subredes. La herramienta más utilizada para escaneo de redes es Nmap. 2. Herramientas para el escaneo de vulnerabilidades en la red: permiten identificar y explotar vulnerabilidades presentes en la red, esto después de un proceso de pentesting o Auditoria de Seguridad Informática a la red. Existen muchas herramientas, entre las más conocidas se encuentran OWASP-ZAP, Nessus, UpGuard, OpenVAS, Maltego, etc. 3. Herramientas para administrar el tráfico de la red: permiten administrar los paquetes de red y observar (sniffing) lo que está circulando por ella. La herramienta más conocida para tráfico de red es Wireshark. Herramientas para monitorización de la red: permiten una gestión total de los procesos y servicios de red; para llevar registro y prevenir fallas en esta. Entre las herramientas más conocidas se encuentran Solarwinds, Pandora FMS, Zenoss, Microsoft Network Monitor, etc
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red de datos - Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013. - Pruebas de penetración con UpGuard y Nessus donde se identifican que los protocolos para cifrado de la información están inactivos.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-004”.

El segundo hallazgo en el dominio auditado y el cual se le consideran realizar las respectivas acciones correctivas, es el riesgo denominado R005 (No existen

controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes), donde se documenta el hallazgo y las recomendaciones en la siguiente tabla:

Tabla 25. Guía de hallazgos para el riesgo R005

Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.4.1. Restricción de Acceso a la Información
Riesgo	R005 - No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.
Descripción del Hallazgo	
No existen controles para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes. No se han establecido controles para asegurar los servicios de seguridad informática en los sistemas de información y redes.	
Riesgo – Nivel de Riesgo (Causas / Efectos)	
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles de acceso físico o lógico para asegurar los servicios de seguridad informática dentro de la empresa. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.7] Deficiencias en la organización [E.14] Fugas de información [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información **[A] Ataques deliberados** [A.4] Manipulación de la configuración	

Tabla 25. Guía de hallazgos para el riesgo R005 (Continuación)

[A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información
Recomendaciones – Acciones Correctivas
En el manual de políticas de seguridad de la información, en donde se definen las políticas de control de acceso, se debe definir un control de claves y nombres de usuario, donde se debe declarar el uso de contraseñas seguras y el cambio periódica de estas, tanto para el acceso de los servicios de red, entre ellos el software Helysa GW, en el cual se almacenan la mayoría de los activos de información de la empresa como también para el ingreso de los equipos de cómputo, con el objetivo de fortalecer la integridad de la información de la empresa.
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red de datos - Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-005”.

De igual manera se encontraron otros riesgos durante la auditoria del dominio y el análisis de riesgos, con una evaluación de riesgo menor, que merecen acciones correctivas inmediatas, como lo es el riesgo R003 (No existen medios usados para acceder a las redes y servicios de red como el uso de VPN), como también riesgos. Los riesgos R001 Y R002 se clasifican como riesgo medio, de igual manera se deben establecer controles para que su probabilidad de ocurrencia no se incremente y generen un impacto mayor. Todas las recomendaciones de los riesgos encontrados durante el dominio A9. Control de Acceso se encuentran

documentas en el Anexo H – Guías de Hallazgo, estas se denominan de acuerdo a la siguiente tabla:

Tabla 26. Guías de Hallazgo para el dominio A9. Control de Acceso

Item	Riesgo	Guía de Hallazgo
R001	No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.	AP-GH-001
R002	No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.	AP-GH-002
R003	No existen medios usados para acceder a las redes y servicios de red como el uso de VPN.	AP-GH-003
R004	No existe monitoreo del uso de los servicios de red	AP-GH-004
R005	No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.	AP-GH-005

Fuente: Autor

7.5.1.2. Hallazgos del dominio A13. Seguridad en las Telecomunicaciones

En el presente dominio auditado, se encontraron gran cantidad de riesgos, el cual se deben implementar acciones correctivas inmediatas. A continuación se muestran algunos de los hallazgos auditados en el dominio A13. Seguridad de las Telecomunicaciones.

El primero corresponde al riesgo denominado R006 (No se establecen procedimientos para la gestión de equipos de redes), donde se documenta el hallazgo y las recomendaciones en la siguiente tabla:

Tabla 27. Guía de hallazgos para el riesgo R006

Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes

Tabla 27. Guía de hallazgos para el riesgo R006 (Continuación)

Riesgo	R006 - No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.
Descripción del Hallazgo	
No existen procedimientos para gestionar adecuadamente el equipo de red en la empresa Panavias S.A. La utilización de los equipos de red no es idónea, ya que se encuentra mal distribuido, por ejemplo el rack donde los switches no poseen un orden y el cableado no se encuentra etiquetado como también el servidor no se encuentra en el área de red. Además, de no existir un inventario sobre los dispositivos de red. El mantenimiento del equipo de la red no se realiza periódicamente y no se hace dentro de la empresa, lo hace el proveedor.	
Riesgo – Nivel de Riesgo (Causas / Efectos)	
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles para la utilización y gestión de los equipos de red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[I] De origen industrial** [I.8] Fallo de servicios de comunicaciones [I.10] Degradación de los soportes de almacenamiento de la información **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.7] Deficiencias en la organización	
Recomendaciones – Acciones Correctivas	
Implementar controles en cuanto a la gestión de los equipos de redes, como lo son: - Ordenar el equipo de red, como lo son servidores, switches, routers, cableado, en un armario metálico o rack de comunicaciones. - El servidor principal se debe encontrar ya sea dentro del rack de comunicaciones o en la oficina de comunicaciones y sistemas de la empresa. - El cableado debe estar debidamente etiquetado.	

Tabla 27. Guía de hallazgos para el riesgo R006 (Continuación)

- Elaborar un inventario con los activos informáticos de red, tanto en su parte física, como lógica. - Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.
Evidencias del Hallazgo
- Visitas técnicas al área de red de la empresa Panavias S.A. - Entrevista para evaluar la seguridad física de la red de datos - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-006”.

El siguiente hallazgo en el dominio auditado y en el cual se le consideran realizar las respectivas acciones correctivas, es el riesgo denominado R007 (No se incluye el desarrollo de los procedimientos de operación apropiados para la red), donde se documenta el hallazgo y sus recomendaciones en la siguiente tabla:

Tabla 28. Guía de hallazgos para el riesgo R007

Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R007 - No se incluye el desarrollo de los procedimientos de operación apropiados para la red.
Descripción del Hallazgo	
No se establece el desarrollo de procedimientos de operación apropiados para la red como lo son el establecimiento de manuales de instrucciones apropiadas de operación y procedimientos de respuesta ante fallas de la infraestructura de red y la implementación de manuales de políticas de seguridad de la información en la empresa Panavias S.A.	
Riesgo – Nivel de Riesgo (Causas / Efectos)	
Evaluación del riesgo = 12 **(Riesgo Alto)**	

Tabla 28. Guía de hallazgos para el riesgo R007 (Continuación)

Causas: La gerencia no ha establecido controles en cuanto a la creación de manuales de procedimientos y de políticas de seguridad para la red.

Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas:

[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.24] Caída del sistema por agotamiento de recursos
[E.28] Indisponibilidad del personal

Recomendaciones – Acciones Correctivas

1. Elaborar e implementar un manual de políticas de seguridad de la información para el área de sistemas y comunicaciones de la empresa Panavias S.A. que contenga:

- Políticas de seguridad de la información.
    - Objetivos de la organización.
    - Alcance.
    - Definiciones.
- Políticas de seguridad de la información en el recurso humano y responsabilidades
- Políticas de control de accesos.
    - Categorías y niveles de acceso
    - Control de claves y nombres de usuario
- Políticas de seguridad para la administración de sistemas y comunicaciones
    - Políticas de uso de programas dentro de la empresa.
    - Políticas de uso de los dispositivos dentro de la empresa.
    - Políticas de uso de los puntos de red de datos.
    - Políticas de seguridad para el centro de datos y del centro del cableado.
    - Políticas sobre copias de seguridad.
- Políticas de seguridad física y del entorno.
    - Políticas de seguridad de los equipos.

Tabla 28. Guía de hallazgos para el riesgo R007 (Continuación)

2. Elaborar e implementar un manual de procedimientos y operaciones para la red de datos de la empresa, que contenga: - Objetivos de la empresa - Alcance - Responsabilidades y funciones - Inventario y valoración de los elementos de red (físico y lógico) - Controles de acceso de usuarios - Herramientas de gestión de la red (herramientas para mapeo de redes, control de tráfico y monitorización de la red) - Plan de respaldo en caso de incidentes
Evidencias del Hallazgo
- Visitas técnicas al área de red de la empresa Panavias S.A. donde se identificó que no se ha establecido o implementado un manual de procedimientos para la red ante posibles incidentes. - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-007”.

Otro hallazgo, el cual necesita planes de acciones correctivas es el riesgo R009 (No existen controles para proteger los sistemas y aplicaciones conectados), en donde se documenta el hallazgo y sus recomendaciones en la siguiente tabla:

Tabla 29. Guía de hallazgos para el riesgo R009

Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R009 - No existen controles para proteger los sistemas y aplicaciones conectados.
Descripción del Hallazgo	
No se han implementado controles de seguridad informática para proteger los sistemas de red, como la red local y el host; y aplicaciones de la empresa, como lo es el software Helysa GW, ante un incidente o ataque informático, ya sea	

Tabla 29. Guía de hallazgos para el riesgo R009 (Continuación)

interno o externo.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles para proteger los sistemas de red y aplicaciones en la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización **[A] Ataques deliberados** [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación de información [A.16] Introducción de falsa información [A.17] Corrupción de la información [A.18] Destrucción de la información [A.19] Divulgación de información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.26] Ataque destructivo [A.30] Ingeniería social
Recomendaciones – Acciones Correctivas
Se recomienda hacer uso de Sistemas de Seguridad Perimetrales para proteger los sistemas de red y aplicaciones en la empresa como son los siguientes: - Uso de cortafuegos o firewalls corporativos. - IDS- Sistemas detectores de intrusos e IPS. - Controles de contenidos (Listas negras y blancas). - Sistemas PROXY y controles de ancho de banda.

Tabla 29. Guía de hallazgos para el riesgo R009 (Continuación)

- Implementación de infraestructuras PKI. - Criptografía, Esteganografía y Certificados Digitales. - Implementación de redes VPN cliente-servidor y sitio a sitio. - Sistemas STORAGE-NAS, para almacenamiento masivo de datos - Sistemas HONEYPOT (Sistemas trampa para intrusos informáticos) - Sistemas Antimalware (Antivirus / Anti-SPAM) - Hardening (Aseguramiento) de telecomunicaciones de micro y macro cómputo
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red de datos - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Pruebas de penetración con nmap para identificar vulnerabilidades en la red y los servicios de red.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-009”.

También se documentaron los hallazgos, referente a la prueba de penetración sobre identificar vulnerabilidades a través de los puertos abiertos de red, el cual se denomina R018 (Vulnerabilidad por puertos sensibles abiertos y expuestos), en donde se documenta el hallazgo y sus recomendaciones en la siguiente tabla:

Tabla 30. Guía de hallazgos para el riesgo R018

Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	
Riesgo	R018 - Vulnerabilidad por puertos sensibles abiertos y expuestos.
Descripción del Hallazgo	
Tras el escaneo de red para identificar vulnerabilidades en la red local y el host de la empresa Panavias S.A., se muestra múltiples puertos sensibles expuestos que corren riesgo de ser explotados. También de información expuesta en algunos de ellos, como en el caso del host, donde se encontró datos encriptados que pueden corresponder a usuarios o contraseñas.	

Tabla 30. Guía de hallazgos para el riesgo R018 (Continuación)

Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: no se ha establecido controles para la seguridad de los servicios de red como es el caso de vulnerabilidad por puertos abiertos con riesgo a ser explotados. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.4] Errores de configuración [E.14] Fugas de información [E.20] Vulnerabilidades de los programas (software) **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.15] Modificación de información [A.17] Corrupción de la información [A.22] Manipulación de programas [A.24] Denegación de servicio [A.30] Ingeniería social
Recomendaciones – Acciones Correctivas
Durante la ejecución de pruebas de penetración, se encontró puertos con información sensible que pueden ser explotados, tanto en la dirección del host como de la red local. En el host, se muestran puertos abiertos de riesgo como lo son: - Puerto 21, servicio FTP - Puerto 26, servicio SMTP - Puerto 110, servicio POP3 - Puerto 143, servicio IMAP - Puerto 443, servicio ssl/http - Puerto 587, servicio smtp

Tabla 30. Guía de hallazgos para el riesgo R018 (Continuación)

- Puerto 993, servicio ssl/imap - Puerto 3306, servicio mysql Se recomienda cerrar los puertos a aquellos servicios de red que no se estén utilizando, además de la configuración de un firewall para los servicios del host. En el caso de la red local, se muestran puertos que se encuentran filtrados, con presencia de firewall configurado por defecto, pero este no resulta muy eficaz. Se recomienda configurar un firewall corporativo para gestionar los servicios de la red local de la empresa como lo es el software Helysa GW.
Evidencias del Hallazgo
- Prueba de penetración con nmap para identificar vulnerabilidades en la red y realizar acciones de escaneo de servicios, subred y fingerprinting. - Prueba de penetración con zenmap para recolectar información en el enrutamiento y la ejecución de scripts de nmap para recolocar información sensible en los puertos abiertos. - Pruebas de penetración con UpGuard y Nessus para identificar y analizar vulnerabilidades en la red.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-018”.

Los hallazgos encontrados durante la auditoria al dominio, se deben mitigar, ya que de acuerdo a la evaluación de riesgos, en su mayoría son clasificados como riesgo alto. Todas las recomendaciones de los riesgos encontrados durante el dominio A13. Seguridad en las Telecomunicaciones se encuentran documentas en el Anexo H – Guías de Hallazgo, estas se denominan de acuerdo a la siguiente tabla:

Tabla 31. Guías de Hallazgo para el dominio A13. Seguridad en las Telecomunicaciones

Ítem	Riesgo	Guía de Hallazgo
R006	No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.	AP-GH-006

Tabla 31. Guías de Hallazgo para el dominio A13. Seguridad en las Telecomunicaciones (Continuación)

Ítem	Riesgo	Guía de Hallazgo
R007	No se incluye el desarrollo de los procedimientos de operación apropiados para la red.	AP-GH-007
R008	No existen controles para salvaguardar los servicios de seguridad informática en la red.	AP-GH-008
R009	No existen controles para proteger los sistemas y aplicaciones conectados.	AP-GH-009
R010	No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.	AP-GH-010
R011	No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.	AP-GH-011
R012	No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.	AP-GH-012
R013	No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.	AP-GH-013
R014	No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.	AP-GH-014
R015	No existen controles para asegurar la conexión segura a la red.	AP-GH-015
R016	No existen procedimientos del uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.	AP-GH-016

Tabla 31. Guías de Hallazgo para el dominio A13. Seguridad en las Telecomunicaciones (Continuación)

Ítem	Riesgo	Guía de Hallazgo
R017	La red se no se encuentra dividida en dominios de red separados o segmentada.	AP-GH-017
R018	Vulnerabilidad por puertos sensibles abiertos y expuestos.	AP-GH-018

Fuente: Autor

7.5.1.3. Hallazgos del dominio A11. Seguridad Física y del Entorno

Los hallazgos o riesgos encontrados durante la auditoria del presenten dominio, también se clasifican como riesgo alto, algunos en escala menor, pero se deben mitigar. A continuación se muestran los hallazgos de mayor relevancia auditados en el dominio A13. Seguridad de las Telecomunicaciones.

El primero corresponde al riesgo denominado R019 (Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas), donde se documenta el hallazgo y las recomendaciones en la siguiente tabla:

Tabla 32. Guía de hallazgos para el riesgo R019

Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.1. Ubicación y Protección de los Equipos
Riesgo	R019 - Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas
Descripción del Hallazgo	
El área de red está encargada por un solo funcionario, pero no existen controles de acceso físico o lógico y cualquier funcionario de la empresa puede ingresar. La ubicación del equipo de red no es idónea, ya que se encuentra mal distribuido, por ejemplo el rack donde los switches no poseen un orden y el cableado no se encuentra etiquetado como también el servidor no se encuentra en el área de red, este se encuentra en la oficina financiera.	
Riesgo – Nivel de Riesgo (Causas / Efectos)	

Tabla 32. Guía de hallazgos para el riesgo R019 (Continuación)

Evaluación del riesgo = 12 **(Riesgo Alto)**

Causas: No se han establecido procedimientos para la ubicación de los equipos de red en la empresa Panavias S.A.

Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas:

[I] De origen industrial
[I.8] Fallo de servicios de comunicaciones
[I.10] Degradación de los soportes de almacenamiento de la información

[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.7] Deficiencias en la organización

[E] Errores y fallos no intencionados
[E.25] Pérdida de equipos

[A] Ataques deliberados
[A.25] Robo de equipos

Recomendaciones – Acciones Correctivas

Se recomienda establecer los siguientes controles:

- Establecer responsabilidades sobre quien tiene acceso al área de red y los equipos de red.
- Ordenar en el equipo de red en el área que corresponde. Se debe ordenar en un armario metálico o rack de comunicaciones con cada uno de sus elementos registrados en un inventario y su cableado debidamente etiquetado.
- Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.

Evidencias del Hallazgo

Tabla 32. Guía de hallazgos para el riesgo R019 (Continuación)

- Visitas técnicas al área de red de la empresa Panavias S.A. - Entrevista para evaluar la seguridad física de la red de datos - Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Fuente: Autor

La anterior guía se encuentra en el Anexo H – Guías de Hallazgo, el cual se denomina “AP-GH-019”.

El segundo hallazgo en el dominio auditado y el cual se le consideran realizar las respectivas acciones correctivas, es el riesgo denominado R022 (Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa), donde se documenta el hallazgo y las recomendaciones en la siguiente tabla:

Tabla 33. Guía de hallazgos para el riesgo R022

Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.3. Seguridad del Cableado
Riesgo	R022 - Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.
Descripción del Hallazgo	
El cableado UTP de cobre no cuenta con protección de blindaje y es vulnerable a interferencias. El cableado no posee ordenamiento ni etiquetado. No existen procedimientos contra interceptación daños al cableado de telecomunicaciones que transporta los datos o brinda soporte a los servicios de información de la empresa Panavias S.A.	
Riesgo – Nivel de Riesgo (Causas / Efectos)	
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: No se han establecido controles para la seguridad del cableado de telecomunicaciones de la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas:	

Tabla 33. Guía de hallazgos para el riesgo R022 (Continuación)

[I] De origen industrial [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización
Recomendaciones – Acciones Correctivas
Se recomienda realizar las siguientes acciones para la seguridad del cableado UTP: 1. En primer lugar, cambiar de empresa proveedora, ya que la actual utiliza cableado de cobre (UTP categoría 3), es preciso cambiar a cable de patch cord de fibra óptica para obtener mejoras en el rendimiento y disponibilidad de la red. 2. Si se mantiene con cableado de cobre, debe cumplir con especificaciones como: - Cableado UTP blindado de categoría 6. - Conductores de cobre solido de calibre entre 22 y 26 AWG. - Utilizar forro PVC. - El etiquetado del cableado debe contener: nombre del fabricante, tipo de cable, numero de pares, tipo y número de listado. 3. Si se cambia a cable patch cord de fibra óptica, se recomienda que este deba tener las siguientes especificaciones: - Deben ser probados para soportar velocidades hasta de 10 GB. - Debe ser compatible con todos los sistemas de cómputo y de red. - Debe ser cableado certificado para generar un desempeño óptimo de su función. - El cableado debe tener retardante de fuego y recubrimiento tipo Tight Buffer.
Evidencias del Hallazgo
- Visitas técnicas al área de red de la empresa Panavias S.A. - Entrevista para evaluar la seguridad física de la red de datos - Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Fuente: Autor

Los hallazgos encontrados durante la auditoria al dominio, se deben mitigar, ya que de acuerdo a la evaluación de riesgos, son clasificados como riesgo alto. Todas las recomendaciones de los riesgos encontrados durante el dominio A11. Seguridad Física y del Entorno se encuentran documentas en el Anexo H – Guías de Hallazgo, estas se denominan de acuerdo a la siguiente tabla:

Tabla 34. Guías de Hallazgo para el dominio A11. Seguridad Física y del Entorno

Ítem	Riesgo	Guía de Hallazgo
R019	Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas	AP-GH-019
R020	No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo	AP-GH-020
R021	El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.	AP-GH-021
R022	Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.	AP-GH-022

Fuente: Autor

7.5.2. Análisis de Brecha y Niveles de Madurez

Una vez organizados los papeles de trabajo de la auditoria, con las guías de hallazgos, donde se establecen sus recomendaciones, se procede a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala definida por la norma ISO/IEC 27001:2013 como se muestra en la tabla 40.

Tabla 35. Tabla de escala para ISO/IEC 27001:2013

Calificación		Descripción
N/A	No Aplica	No aplica.
0	Inexistente	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
20	Inicial	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.
40	Repetible	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
60	Definido	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.
80	Gestionado	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
100	Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: NTC/ISO/IEC 27001:2013

Para los cálculos totales del análisis de brecha, se determinó el promedio de valores asignados a cada control para obtener la calificación del objetivo de control al cual pertenecen según la normatividad, los cuales a su vez se promediaron para calcular el nivel de madurez de cada dominio

Tabla 36. Análisis de brecha a los dominios auditados

Dominio y subdominios	Descripción	% NM Objetivo de Control	Nivel de madurez	% NM Dominio y Controles
A5	**Políticas de Seguridad de la Información**			**20**
A5.1.1 Documento de política de seguridad de información	Política de seguridad de la información	40	Inicial	20
A5.1.2 Revisión de la política de seguridad de la información			Inicial	20
A6	**Organización de la Seguridad de la Información**			**10**
A6.1.1. Roles y responsabilidades para la seguridad de la información	Roles y responsabilidades	20	Inicial	20
A9	**Control de Acceso**			**30**
A9.1.2. Control de acceso a las redes y servicios asociados	Requisitos del negocio para el control de acceso	20	Inicial	20
A9.4.1. Restricción de acceso a la información	Control de acceso a las aplicaciones e información	40	Repetible	40

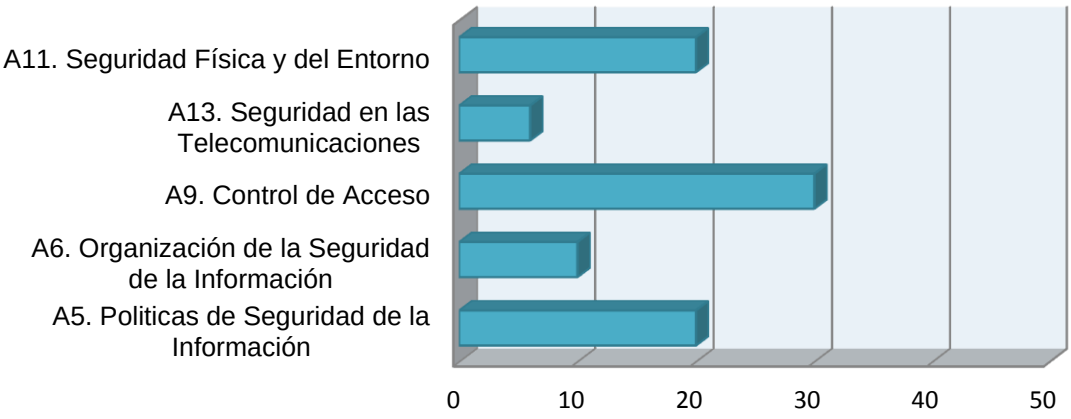
Tabla 36. Análisis de brecha a los dominios auditados (Continuación)

A13	**Seguridad en las Telecomunicaciones**			**6.66**
A13.1.1. Control de redes	Gestión de la seguridad en redes	13.33	Inicial	20
A13.1.2. Seguridad en los servicios de red			Inicial	20
A13.1.3. Separación de redes			Inexistente	0
A11	**Seguridad Física y del Entorno**			**20**
A11.2.1. Ubicación y protección de los equipos	Seguridad de los equipos	40	Inicial	20
A11.2.3. Seguridad del cableado			Inicial	20

Fuente: Autor

Una vez calculado y clasificado el nivel de madurez para cada de los dominios verificados durante la auditoria, se puede observar que la empresa Panavias S.A., en relación a la seguridad de su red de datos, se encuentra en un nivel de madurez inicial. Esto quiere decir que, la empresa ha reconocido que existe un problema y que hay que tratarlo, pero no se posee procesos estandarizados y controles que permitan corregir o mitigar cualquier fallo que se pueda presentar en su infraestructura de red, tanto en su parte física como lógica. Tampoco existe documentación relacionada con seguridad de la información, como lo son un manual de políticas y procedimientos, que es justo que la empresa implemente. Se puede observar los resultados de los niveles de madurez a los dominios verificados en la siguiente figura:

Figura 40. Niveles de Madurez



	A5. Politicas de Seguridad de la Información	A6. Organización de la Seguridad de la Información	A9. Control de Acceso	A13. Seguridad en las Telecomunicaciones	A11. Seguridad Física y del Entorno
Nivel de Madurez	20	10	30	6	20

Fuente: Autor

7.5.3. Declaración de Aplicabilidad

En la declaración de aplicabilidad, según la normatividad, es donde se listan los controles que se van a implementar. Para este caso, los controles se establecieron en las guías de hallazgo, para cada riesgo encontrado durante la auditoria a los dominios evaluados (Ver Anexo H- Guías de Hallazgos).

La declaración de aplicabilidad contiene los dominios y subdominios evaluados de acuerdo con el objetivo de la auditoria; contiene también las salvaguardas seleccionadas, las cuales se refieren a los controles existentes, siendo estas inexistentes en la empresa ya que no se han aplicado acciones correctivas y los controles que se van a implementar, según los procesos evaluados.

El documento que corresponde a la declaración de aplicabilidad que contienen los controles o recomendaciones planteadas para los riesgos o hallazgos encontrados durante la auditoria a la red de datos de la empresa Panavias S.A., se encuentran en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Panavias_DeclaracionAplicabilidad”.

8. DIVULGACIÓN

La divulgación de los resultados de la presente auditoria, se realizara a través del informe final de auditoria, el cual consiste en un informe ejecutivo que contiene, de manera general, los hallazgos obtenidos durante el proceso y las recomendaciones de estos. Cabe mencionar, que las recomendaciones técnicas, se encuentran en las guías de hallazgo, las cuales se entregaran directamente al encargado de la oficina asesora de comunicaciones y sistemas de la empresa Panavias S.A. para que se realicen las respectivas acciones correctivas. El informe final de auditoria se entregara al gerente general de la empresa Panavias S.A.

El documento que corresponde al informe final de auditoria, que se entrega directamente a la gerencia de la empresa, se encuentra en el Anexo A – Formatos y Documentación de la Auditoria, el cual se denomina “Panavias_InformeFinal”.

9. CONCLUSIONES

La auditoría finalizo cumpliendo cada una de las fases propuestas. A pesar de que en la primera fase, en la recolección de información de la empresa, no se realizó a tiempo ya que gran parte de la información solicitada no existía y no se han implementado procedimientos respecto a la gestión de la red de datos, se logró detectar las primeras falencias, respectivas a la auditoria. Las visitas técnicas, también aportaron gran cantidad de observaciones, respecto a identificar vulnerabilidades en la red, tanto en su parte física como lógica.

En la fase de planeación, se realizaron la elección respectiva a la normatividad y los dominios de esta que involucran únicamente con la evaluación a redes informáticas y con el objetivo de la auditoria. Una vez escogida la normatividad, se diseñaron los instrumentos de recolección de información, como lo fueron las entrevistas, las listas de chequeo, los cuestionarios de control cuantitativos y guías de hallazgos.

En la fase de ejecución de la auditoria, se aplicaron pruebas de penetración o testeo a la red de la empresa Panavias S.A. donde se identificaron vulnerabilidades a los que está expuesta la red de datos de la empresa Panavias S.A. Estas pruebas se aplicaron, tanto en la red local de la empresa, como en su servicio de host, su aplicación web. Una vez aplicados los instrumentos, como lo fueron entrevistas, listas de chequeo y cuestionarios de control, se procedió a realizar el análisis de riesgos, con los hallazgos obtenidos para determinar el nivel de criticidad de los riesgos encontrados tanto en las pruebas de penetración como en los instrumentos.

Una vez terminada la fase de ejecución, se procedió a organizar los papeles de trabajo de la auditoria en las guías de hallazgos, con el fin de organizar los resultados obtenidos, tanto de las pruebas de penetración, como de los instrumentos, y con ello, se realizó las respectivas recomendaciones y/o controles para mitigar los riesgos o hallazgos obtenidos durante la auditoria. Se determinó también los niveles de madurez de los dominios evaluados en la auditoria y se realizó la declaración de aplicabilidad, con los controles propuestos para realizar las respectivas acciones correctivas inmediatas de los riesgos o hallazgos encontrados durante la auditoria a la red de datos de la empresa Panavias S.A.

10. RECOMENDACIONES

Se recomienda hacer uso e implementar los controles propuestos en las guías de hallazgos como también en la declaración de aplicabilidad. De acuerdo al alto riesgo evaluado en el dominio A13. Seguridad en las Telecomunicaciones, se encuentran bastantes deficiencias tanto en la parte física como lógica de la red, lo cual se recomienda hacer las acciones correctivas inmediatas planteadas.

En primer lugar, se debería elaborar e implementar un manual de políticas de seguridad de la información en la empresa Panavias S.A. que contenga la gestión de los activos de información, los activos informáticos, respecto al equipo e cómputo y de red en la empresa y la delegación de responsabilidades para dichos activos y acciones. Para el área de sistemas y comunicaciones de la empresa, lugar donde se realizó la presente auditoria, se deben implementar políticas de control de acceso para la administración de sistemas y comunicaciones de red y políticas de seguridad física para los equipos de cómputo de red, como también, de la implementación de un manual de procedimientos y operaciones, que contenga las instrucciones sobre la gestión y control de la red de datos de la infraestructura tecnológica y de red en la empresa Panavias S.A.

Una vez implementada la documentación respectiva a las políticas de seguridad y el manual de procedimientos de la red de datos de la empresa Panavias S.A., se deben coordinar actividades de gestión, con el apoyo y aprobación de la gerencia de la empresa, para optimizar el servicio de red en la organización y que los controles se apliquen en forma coherente. Las políticas y controles ayudaran a la empresa a planificar, desarrollar e implementar soluciones respecto a su infraestructura tecnológica, como también garantizar los servicios de seguridad informática de los activos informáticos y de información.

En cuanto al control de acceso, se deben implementar controles respecto a procedimientos de autorización para determinar el personal que accede al área de red y los servicios de red, como también la protección del acceso a la red y servicios y medios seguros para acceder a las mismas. Estos controles se encuentras sustentado en las guías de hallazgo como también en la declaración de aplicabilidad, depende de la organización dar mitigación a estos procedimientos.

Para un monitoreo de los usos de los servicios de red, que permita realizar el seguimiento de la actividad de la red de la empresa, es preciso implementar

herramientas para gestionar el mapeo de redes, revisar el tráfico de red y también el uso de herramientas aplicadas a los servicios de red. Esto con el objetivo de implementar medidas de protección adecuadas, supervisar los registros y actividades que permitan salvaguardar la red tanto en su parte física, como lógica

La seguridad en telecomunicaciones en la empresa, de acuerdo a los parámetros evaluados, es el de mayor criticidad y se deben implementar controles o acciones correctivas inmediatas. Primero que todo, se deben implementar procedimientos para la gestión de los equipo de red, como lo son la elaboración de un inventario con los activos informáticos de red, tanto en su parte física, como lógica, como también el ordenamiento idóneo de todos los equipos de red en su área respectiva. También se deberían implementar controles para salvaguardar los servicios de seguridad informática en la red, como lo son la confidencialidad, disponibilidad e integridad de los activos de información e informáticos. Es preciso, hacer uso de Sistemas de Seguridad Perimetrales para proteger los sistemas de red y aplicaciones en la empresa, ya que se demostró, muchas falencias durante la realización de pruebas de penetración a la red de datos de la empresa Panavias S.A.

También se recomienda, utilizar controles relacionados con tecnología aplicada como lo son autenticación, protocolos criptográficos y controles para la conexión segura a la red. Estas recomendaciones para implementar estos controles, se encuentras sustentados en las guías de hallazgo como también en la declaración de aplicabilidad, depende de la organización dar un plan de acción correctiva o mitigar estos procedimientos.

La seguridad física de los equipos de cómputo y de red es de suma importancia, por lo que se deben establecer controles respecto al mantenimiento de los mismos, ya que actualmente lo realiza la empresa proveedora. Es preciso que estos procesos de mantenimiento los realice el personal encargado del área de sistemas y comunicaciones de la empresa. Como también, se deben implementar, y reforzar los que se tienen, controles para minimizar el riesgo de amenazas físicas y ambientales que se pueden presentar y que atenten contra los equipos de red y cómputo de la empresa Panavias S.A.

BIBLIOGRAFÍA

CÓDIGO PENAL. Ley 1273 de 2009 De la Protección de la Información y de los Datos. Colombia, 2009. Ministerio de la Información y las Comunicaciones de Colombia.

CÓDIGO PENAL. Ley 1581 de 2012 De la Protección de los Datos Personales, 2009. Congreso de Colombia.

ESTRADA, Alejandro. Seguridad en Redes. Estrategias de Seguridad en Redes. Madrid, España. 2016

FERRER, RODRIGO. Metodología de Análisis de Riesgo. Bogotá. Colombia, 2006. Empresa: SISTESEG.

ITURMENDI ACHA, Juan José. Auditoria Informática en la Empresa. Madrid, España. 1994.

MAGERIT Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de Elementos. Ministerio de Hacienda y Administraciones Públicas. España, 2012.

NTC-ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

NTC-ISO-IEC 27002:2013. Tecnología de la Información. Técnicas de Seguridad. Código de Practica para Controles de Seguridad de la Información.

PEREZ, Pablo Gonzales. GARCES, German. DE LA CAMARA, José Miguel. Pentesting con Kali. Madrid, España. 2013

POBLETE, Victoria. Procedimiento de Seguridad del Cableado. Ministerio de Salud. Santiago de Chile, 2013.

SOLARTE, Nicolás Javier. GUSTIN LOPEZ, Enith. HERNANDEZ, Ricardo Javier. Manual de Procedimientos para llevar a la Práctica la Auditoria Informática. San Juan de Pasto, Colombia. 2012.

TAPIADOR, Ángeles Sanz. Controles y Auditoria en Redes de Datos. Guía Práctica. Escuela Politécnica Superior. Facultad de Ingeniería Técnica en Informática de Gestión. Madrid, España. 2010.

VARGAS AVILES, Julio Rito. Conceptos sobre Auditoria Informática. Colombia, 2009. Universidad Nacional de ingeniería. Facultad de Ingeniería de Sistemas. Departamento de Ingeniería.

NORMA ISO/IEC 27000. Portal ISO 27000 en Español [en línea]. [Consultado el 26 de Agosto de 2016]. Disponible en: <http://www.iso27000.es/>

AUDITORIA INFORMÁTICA. Construcción de un concepto universal de auditoria [en línea]. [Consultado el 24 de Agosto de 2016] Disponible en: <http://fccea.unicauca.edu.co/old/tgarf/tgarfse1.html>

AUDITORIA INFORMÁTICA. Metodología de la Auditoria Informática [en línea]. [Consultado el 24 de Agosto de 2016]. Disponible en: <http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm#p2-1-1>

SEGURIDAD INFORMÁTICA. Capítulo 1. Estrategias de Seguridad [en línea]. [Consultado el 26 de Agosto de 2016]. Disponible en: <http://www.scoop.it/doc/download/cvdXLLFB5B3H35NMF97_qdw>

HELYSA. Software Administrativo y de Gestión [en línea]. [Consultado el 13 de Septiembre de 2016]. Disponible en: <helisa.com>

CENTRALOPS.NET. Utilidades avanzadas en internet [en línea]. [Consultado el 4 de Octubre de 2016]. Disponible en: <https://centralops.net/co/>

NMAP. Guía de referencia de Nmap (Pagina de manual) [en línea]. [Consultado el 5 de Octubre de 2016]. Disponible en: <https://nmap.org/man/es/>

ReYDeS. Realizar un spidering web utilizando OWASP-ZAP [en línea]. [Consultado el 5 de Octubre de 2016]. Disponible en: <http://www.reydes.com/d/?q=Realizar_un_Spidering_Web_utilizando_Zed_Attack_Proxy>

ReYDeS. Introducción a OWASP-ZAP [en línea]. [Consultado el 5 de Octubre de 2016]. Disponible en: <http://www.reydes.com/archivos/slides/eventos/OWASP_ZAP_Alonso_ReYDeS.pdf>

OWASP ZAP Zed Attack Proxy Project [en línea]. [Consultado el 7 de Octubre de 2016]. Disponible en: <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

UPGUARD. Web scanner vulnerabilty [en línea]. [Consultado el 11 de Octubre de 2016]. Disponible en: <https://www.upguard.com/>

NESSUS. Tenable Network Security [en línea]. [Consultado el 13 de Octubre de 2016]. <Disponible en: https://www.tenable.com/products/nessus-vulnerability-scanner>

NVD. National Vulnerability Database National Cyber Awareness System [en línea]. [Consultado el 25 de Octubre de 2016]. <Disponible en: https://nvd.nist.gov/>

NVD. National Vulnerability Database Common Vulnerability Scoring System Version 2 Calculator [en línea]. [Consultado el 25 de Octubre de 2016]. <Disponible en: https://nvd.nist.gov/CVSS/CVSS-v2-Calculator>

JUMPSTART. JumpStart WPS para Windows [en línea] [Consultado el 28 de Octubre de 2016]. <Disponible en: http://pokoxemo.blogspot.com.co/2014/06/descarga-jumpstart-wps-para-windows.html>

SGSI. Capítulo 3 Análisis de riesgos, identificación de amenazas. [en línea]. [Consultado el 10 de Noviembre de 2016]. <Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3231_identificacin_de_amenazas.html>

PORTAL ISO 27002. Control de Acceso [en línea]. [Consultado el 21 de Noviembre de 2016]. <Disponible en: http://www.iso27000.es/iso27002_9.html>

PORTAL ISO 27002. Seguridad en las Telecomunicaciones [en línea]. [Consultado el 21 de Noviembre de 2016]. <Disponible en: http://www.iso27000.es/iso27002_13.html>

PORTAL ISO 27002. Seguridad Física y del Entorno [en línea]. [Consultado el 21 de Noviembre de 2016]. <Disponible en: http://www.iso27000.es/iso27002_11.html>

ISO 27002 WIKI. Procedimientos y responsabilidades de operación [en línea]. [Consultado el 24 de Noviembre de 2016]. <Disponible en: https://iso27002.wiki.zoho.com/10-1-Procedimientos-y-responsabilidades-de-operaci%C3%B3n.html>

ISACA. La integridad de los datos [en línea]. [Consultado el 28 de Noviembre de 2016] <Disponible en: http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx?utm_referrer=>

ANEXOS

Nota:

Algunos datos no se muestran adjuntos en los anexos para preservar la confidencialidad de la información de la empresa Panavias S.A., como lo son los resultados de las pruebas de penetración (Anexo G - Pruebas de Penetración), los cuales se podrán visualizar por medio magnético adjunto a este documento.

Anexo A – Formatos y Documentación de la Auditoria: Formato_EntrevistaSeguridadFisica

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**			
Respondido por					

ÁREA
Red de datos de la empresa Panavias S.A.

ENTREVISTA PARA EVALUAR LA SEGURIDAD FISICA DE LA RED DE DATOS EN LA EMPRESA PANAVIAS S.A.
Objetivo:
Conocer acerca de la administración, en cuanto a su función y actividades de la red de datos de la empresa Panavias S.A. en su seguridad física

1.	**Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados**
1.1.	¿Cómo se resguarda el acceso al área de sistemas? Es decir, ¿solamente tiene acceso el personal de sistemas a esta área?
1.2.	¿El equipo de red y comunicaciones se mantiene en habitación cerrada con acceso únicamente del personal autorizado?
1.3.	¿Existen mecanismos para controlar el acceso al área de la red? Cuales
2.	**Controles de utilización de los equipos de red y de comunicaciones,**

2.1. ¿Cómo se encuentra distribuido el equipo de red? (cableado, routers, servidor, etc.
2.2. ¿Existe actualmente un inventario sobre los dispositivos del equipo de red?
2.3. ¿Se realiza un mantenimiento periódico de los equipos de red y de comunicaciones?, de ser afirmativo, ¿con que frecuencia se realiza el mantenimiento?
2.4. ¿Existen equipos de monitorización?, si existen, ¿se realiza el registro de tráfico de datos en la red?
3. Controles para la protección y tendido adecuado de cables y líneas de comunicaciones
3.1. ¿El cableado de red se encuentra debidamente protegido, etiquetado en las instalaciones adecuadas?
3.2. ¿Los armarios, distribuidores y terminaciones, se encuentran etiquetados?
3.3. ¿Se revisa periódicamente los cables y líneas de comunicaciones, buscando fallas o desgaste por su uso? de ser afirmativo, ¿con que frecuencia se realiza esta revisión?
3.4. ¿El cableado de datos va en un canal aparte del cableado eléctrico?

4. Controles para perdida de la información y desastres
4.1. En caso de pérdida de la información, ¿la organización cuenta con respaldos para esta en discos duros externos u otros dispositivos?, de ser afirmativo, ¿qué mecanismos utiliza la organización para realizar los respaldos de la información?
4.2. ¿Existen instalaciones de suministro adecuadas ante posibles cortes de luz ante posibles acontecimientos inesperados?, de ser afirmativo, ¿qué tipo de instalaciones utiliza la empresa?
4.3. ¿Los equipos de red se encuentran protegidos sobre posibles amenazas físicas y ambientales?
4.4. ¿Existen planes de contingencia para desastres que solo afecten a las comunicaciones?, como por ejemplo el fallo total de las comunicaciones en la organización.
5. Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados
5.1. ¿Cómo se resguarda el acceso al área de sistemas? Es decir, ¿solamente tiene acceso el personal de sistemas a esta área?
5.2. ¿El equipo de red y comunicaciones se mantiene en habitación cerrada con acceso únicamente del personal autorizado?
5.3. ¿Existen mecanismos para controlar el acceso al área de la red? Cuales

6. Controles de utilización de los equipos de red y de comunicaciones,
6.1. ¿Cómo se encuentra distribuido el equipo de red? (cableado, routers, servidor, etc.
6.2. ¿Existe actualmente un inventario sobre los dispositivos del equipo de red?
6.3. ¿Se realiza un mantenimiento periódico de los equipos de red y de comunicaciones?, de ser afirmativo, ¿con que frecuencia se realiza el mantenimiento?
6.4. ¿Existen equipos de monitorización?, si existen, ¿se realiza el registro de tráfico de datos en la red?
7. Controles para la protección y tendido adecuado de cables y líneas de comunicaciones
7.1. ¿El cableado de red se encuentra debidamente protegido, etiquetado en las instalaciones adecuadas?
7.2. ¿Los armarios, distribuidores y terminaciones, se encuentran etiquetados?
7.3. ¿Se revisa periódicamente los cables y líneas de comunicaciones, buscando fallas o desgaste por su uso? de ser afirmativo, ¿con que frecuencia se realiza esta revisión?
7.4. ¿El cableado de datos va en un canal aparte del cableado eléctrico?

8. Controles para perdida de la información y desastres
8.1. En caso de pérdida de la información, ¿la organización cuenta con respaldos para esta en discos duros externos u otros dispositivos?, de ser afirmativo, ¿qué mecanismos utiliza la organización para realizar los respaldos de la información?
8.2. ¿Existen instalaciones de suministro adecuadas ante posibles cortes de luz ante posibles acontecimientos inesperados?, de ser afirmativo, ¿qué tipo de instalaciones utiliza la empresa?
8.3. ¿Los equipos de red se encuentran protegidos sobre posibles amenazas físicas y ambientales?
8.4. ¿Existen planes de contingencia para desastres que solo afecten a las comunicaciones?, como por ejemplo el fallo total de las comunicaciones en la organización.

Anexo A – Formatos y Documentación de la Auditoria: Formato_EntrevistaSeguridadLogica

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**			
Respondido por					

ENTREVISTA PARA EVALUAR LA SEGURIDAD LÓGICA DE LA RED DE DATOS EN LA EMPRESA PANAVIAS S.A.
Objetivo:
Conocer acerca de la administración, en cuanto a su función y actividades de la red de datos de la empresa Panavias S.A. en su seguridad lógica.

1.	**Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red**
1.1.	¿El software de comunicaciones para permitir el acceso exige autenticación? (usuario y contraseña)
1.2.	¿Se inhabilita el usuario que sea incapaz de dar la contraseña erróneamente luego de un número determinado de intentos?
1.3.	¿Se obliga a los funcionarios a cambiar contraseñas regularmente?, de ser afirmativo, ¿Con que frecuencia se realiza el cambio de contraseñas?
2.	**Control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas**
2.1.	¿Se toman estadísticas que incluyan tasas de errores y de

retransmisión?, de ser afirmativo, ¿Con que frecuencia se toman estas estadísticas?
3. Controles para asegurar que las transmisiones van solamente a usuarios autorizados
3.1. ¿El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos o retrasados?
4. Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.
4.1. ¿Existen herramientas para mapear la red?, en caso afirmativo, ¿Que herramientas se utilizan?
4.2. ¿Existen herramientas para revisar el tráfico de la red?, en caso afirmativo, ¿Que herramientas se utilizan?
4.3. ¿Existen herramientas aplicadas para la seguridad de los servicios de red como lo son autenticación y controles de servicio de red? en caso afirmativo, ¿Que herramientas se utilizan?
5. Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.
5.1. ¿Existen técnicas de cifrado para los datos? en caso afirmativo, ¿Que técnicas de criptografía se utilizan?
5.2. ¿La transmisión de datos sensibles a través de redes abiertas, van cifrados?

6. Controles de Seguridad en la Red	
6.1.	¿Se han revisado controles en la seguridad de los módems como firewalls o cortafuegos para impedir el acceso de equipos foráneos a la red local de la organización?, de ser afirmativo, ¿Con que frecuencia se revisa estos controles?
6.2.	¿Existen políticas de prohibición de instalar programas o conectar equipos privados a la red local?, de ser afirmativo, ¿Qué políticas se han implementado?
6.3.	¿Periódicamente se ejecutan herramientas de ataques para descubrir vulnerabilidades?, de ser afirmativo, ¿los resultados se documentan y se corrigen las falencias encontradas?

Anexo A – Formatos y Documentación de la Auditoria: EntrevistaSeguridadFisica

PANAVIAS	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.	UNAD Versión 1.0

Elaborado por	Ing. Jesús G. Cortés	**Fecha**	24	OCT.	2016
Respondido por	Ing. Heimas Zuñiga				

ÁREA
Red de datos de la empresa Panavias S.A.

ENTREVISTA PARA EVALUAR LA SEGURIDAD FISICA DE LA RED DE DATOS EN LA EMPRESA PANAVIAS S.A.
Objetivo:
Conocer acerca de la administración, en cuanto a su función y actividades de la red de datos de la empresa Panavias S.A. en su seguridad física

1. Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados
1.1. ¿Cómo se resguarda el acceso al área de sistemas? Es decir, ¿solamente tiene acceso el personal de sistemas a esta área?
Existe Solo un encargado en la oficina de sistemas, pero no existen Controles de acceso y Cualquier funcionario puede ingresar.
1.2. ¿El equipo de red y comunicaciones se mantiene en habitación cerrada con acceso únicamente del personal autorizado?
El equipo de red y comunicaciones se encuentra en la oficina de sistemas, excepto el Servidor, que se encuentra entre la oficina financiera y el archivo.
1.3. ¿Existen mecanismos para controlar el acceso al área de la red? Cuales
No existen mecanismos de control de accesos a la oficina de Sistemas y comunicaciones.
2. Controles de utilización de los equipos de red y de comunicaciones,
2.1. ¿Cómo se encuentra distribuido el equipo de red? (cableado, routers, servidor, etc.
El rack de Comunicaciones contiene 2 Switches con cableado UTP de

sobre. Se cuenta con un Servidor Windows Sever 2003 y cuatro routers distribuidos. También se cuenta con el Software Administrativo Harpa GW.
2.2. ¿Existe actualmente un inventario sobre los dispositivos del equipo de red?
No existe inventario de los equipos de red
2.3. ¿Se realiza un mantenimiento periódico de los equipos de red y de comunicaciones?, de ser afirmativo, ¿con que frecuencia se realiza el mantenimiento?
El mantenimiento es encargado de realizarlo el proveedor, en este caso la empresa Movistar y este no se realiza Seguidamente. Máximo dos veces en el año.
2.4. ¿Existen equipos de monitorización?, si existen, ¿se realiza el registro de tráfico de datos en la red?
No existen equipos ni herramientas para monitorización de la red de la empresa.
3. Controles para la protección y tendido adecuado de cables y líneas de comunicaciones
3.1. ¿El cableado de red se encuentra debidamente protegido, etiquetado en las instalaciones adecuadas?
El cableado de red no se encuentra protegido (blindado) ni etiquetado para los equipos de la empresa.
3.2. ¿Los armarios, distribuidores y terminaciones, se encuentran etiquetados?
El rack de comunicaciones no posee etiquetados para su cableado y elementos.
3.3. ¿Se revisa periódicamente los cables y líneas de comunicaciones, buscando fallas o desgaste por su uso? de ser afirmativo, ¿con que frecuencia se realiza esta revisión?
Este mantenimiento también lo realiza la empresa proveedora, Movistar, lo realiza cuando se le solicita.
3.4. ¿El cableado de datos va en un canal aparte del cableado eléctrico?
Si existe separación del cableado de datos UTP con el cableado eléctrico, estos van por separado.
4. Controles para perdida de la información y desastres
4.1. En caso de pérdida de la información, ¿la organización cuenta con

respaldos para esta en discos duros externos u otros dispositivos?, de ser afirmativo, ¿qué mecanismos utiliza la organización para realizar los respaldos de la información?
Si existen copias de seguridad de los activos de información y, estos se almacenan en medios magnéticos como Cd's y también en memorias USB. El software Helysa, guarda sus datos en la Nube.
4.2. ¿Existen instalaciones de suministro adecuadas ante posibles cortes de luz ante posibles acontecimientos inesperados?, de ser afirmativo, ¿qué tipo de instalaciones utiliza la empresa?
La empresa Panorias S.A abarca todo el quinto piso del C.C. Valle de Atriz en Pasto, la cual cuenta con suministro de energía de fuente ante una eventual falla de luz.
4.3. ¿Los equipos de red se encuentran protegidos sobre posibles amenazas físicas y ambientales?
Existen cámaras de vigilancia en el despacho de la empresa, en la mayoría de las oficinas no, lo cual los equipos son vulnerables a robo. La empresa cuenta también con alarmas contra incendio.
4.4. ¿Existen planes de contingencia para desastres que solo afecten a las comunicaciones?, como por ejemplo el fallo total de las comunicaciones en la organización.
La mayoría de los procesos de la empresa Panorias S.A. dependen del Servicio de Internet. Esto depende de la conectividad al internet. No se han realizado planes de contingencia ante fallos en las Telecomunicaciones.

Anexo A – Formatos y Documentación de la Auditoria: EntrevistaSeguridadLogica

PANAVIAS	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**	24	oct.	2016
Respondido por	Ing. Holmes Zuñiga.				

ENTREVISTA PARA EVALUAR LA SEGURIDAD LÓGICA DE LA RED DE DATOS EN LA EMPRESA PANAVIAS S.A.

Objetivo:

Conocer acerca de la administración, en cuanto a su función y actividades de la red de datos de la empresa Panavias S.A. en su seguridad lógica.

1. Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red

1.1. ¿El software de comunicaciones para permitir el acceso exige autenticación? (usuario y contraseña)

Tanto el Servidor como el Gateway, el acceso cuenta con autenticación.

1.2. ¿Se inhabilita el usuario que sea incapaz de dar la contraseña erróneamente luego de un número determinado de intentos?

Tanto el Servidor como el Gateway permiten ilimitados numeros de intentos. El Software Helyso.GW, se bloquea luego de 3 intentos erróneos para acceso al Sistema.

1.3. ¿Se obliga a los funcionarios a cambiar contraseñas regularmente?, de ser afirmativo, ¿Con que frecuencia se realiza el cambio de contraseñas?

Se realiza cambio de contraseñas para el acceso del Software administrativo Helyso.GW cada 6 meses.

2. Control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas

2.1. ¿Se toman estadísticas que incluyan tasas de errores y de retransmisión?, de ser afirmativo, ¿Con que frecuencia se toman estas estadísticas?

No se toman este tipo de estadísticas ya que la empresa no cuenta con un sistema y proceso de monitorización a la red.

3. Controles para asegurar que las transmisiones van solamente a usuarios autorizados

3.1. ¿El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos o retrasados?

No existe este tipo de procedimiento ya que la empresa no cuenta con controles para la red de datos.

4. Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

4.1. ¿Existen herramientas para mapear la red?, en caso afirmativo, ¿Que herramientas se utilizan?

No se utilizan herramientas para mapeo de redes.

4.2. ¿Existen herramientas para revisar el tráfico de la red?, en caso afirmativo, ¿Que herramientas se utilizan?

No se utilizan herramientas para monitorear el tráfico de red.

4.3. ¿Existen herramientas aplicadas para la seguridad de los servicios de red como lo son autenticación y controles de servicio de red? en caso afirmativo, ¿Que herramientas se utilizan?

No se utilizan herramientas para administrar la seguridad de los Servicios de red.

5. Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.

5.1. ¿Existen técnicas de cifrado para los datos? en caso afirmativo, ¿Que técnicas de criptografía se utilizan?

No se utilizan herramientas de Criptografía para cifrar datos

5.2. ¿La transmisión de datos sensibles a través de redes abiertas, van cifrados?

No se utilizan herramientas de Criptografía para cifrar datos.

6. Controles de Seguridad en la Red
6.1. ¿Se han revisado controles en la seguridad de los módems como firewalls o cortafuegos para impedir el acceso de equipos foráneos a la red local de la organización?, de ser afirmativo, ¿Con que frecuencia se revisa estos controles?
Si existen firewalls para la red local, estos estan configurados en los routers, pero son firewalls básicos. El proveedor se encarga de revisar estos controles.
6.2. ¿Existen políticas de prohibición de instalar programas o conectar equipos privados a la red local?, de ser afirmativo, ¿Qué políticas se han implementado?
No se pueden instalar programas que afecten el ritmo de trabajo como juegos u otros programas de entretenimiento. Todo equipo ingresado a la empresa, debe ser registrado en recepción.
6.3. ¿Periódicamente se ejecutan herramientas de ataques para descubrir vulnerabilidades?, de ser afirmativo, ¿los resultados se documentan y se corrigen las falencias encontradas?
Nunca se han ejecutado este tipo de herramientas para identificar Vulnerabilidades en la red. Nunca se han realizado Auditorias de Seguridad Informática.

Anexo A – Formatos y Documentación de la Auditoria: Formato_CuestionarioControl

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-CC-000 Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**			
Respondido por					

Cuestionario de Control	
Dominio	
Proceso	
Objetivo del control	

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Pregunta	**Si**	**No**	**N/A**	**Observaciones**
TOTALES				
PUNTAJE TOTAL				

Anexo A – Formatos y Documentación de la Auditoria: Formato_GuiaHallazgos

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-000

Guía de Hallazgos	
Dominio/Proceso	
Subdominio	
Riesgo	

Descripción del Hallazgo
Riesgo – Nivel de Riesgo (Causa / Efecto)
Recomendaciones – Acciones Correctivas
Evidencias del Hallazgo

Anexo A – Formatos y Documentación de la Auditoria: Panavias_ProgramadeAuditoria

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.** **PROGRAMA DE AUDITORIA**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Objetivo: Desarrollar una auditoría a la seguridad de la red de datos que permita diseñar un sistema de gestión de seguridad informático que contenga los controles y procedimientos para la red en la empresa Panavias S.A.

Alcance: Para evaluar la seguridad de la red de datos de la empresa Panavias S.A. se tendrá en cuenta las siguientes etapas:

- Aplicación de instrumentos de recolección de la información.
- Aplicación de Pruebas de Penetración y Ethical Hacking.
- Realización de un Análisis y Gestión de riesgos informáticos.

Para la aplicación de los instrumentos de recolección de la información se tendrá en cuenta:

- Selección de la normatividad y dominios a aplicar.
- Diseño y aplicación de cuestionarios.
- Diseño y aplicación de listas de chequeo.

Para la aplicación de las pruebas de penetración, se tendrá en cuenta las fases del Pentesting (Ethical Hacking):

- Fase de recolección o reconocimiento.
- Fase de análisis de vulnerabilidades.

Para la realización del análisis y gestión de riesgos de los hallazgos y vulnerabilidades encontradas en los instrumentos de recolección de la información y las pruebas de penetración, se tendrá en cuenta:

- Análisis de riesgos de acuerdo a las vulnerabilidades encontradas
- Matriz de riesgos
- Gestión de riesgos

Responsabilidades:

Gerencia: Gerencia Panavias S.A.
Cargo encargado de la auditoria: Ingeniero Auditor, desarrollador del proyecto
Acompañamiento: Encargado del área de sistemas y comunicaciones de la empresa Panavias S.A. y un asistente de la misma empresa.

PROGRAMA DE AUDITORIA A LA SEGURIDAD DE LA RED DE DATOS PANAVIAS – AÑO 2017					
ACTIVIDAD	**RESPONSABLE**	**FECHA DE TERMINACIÓN**	**LUGAR**	**PROPOSITO**	**METODOLOGÍA**
Realización de visitas guiadas al área de red de la empresa	-Ingeniero Auditor -Encargado del área de sistemas -Asistente	19 – 30 de septiembre de 2016	Oficina de sistemas y comunicaciones. Empresa Panavias S.A	Conocer la red de datos de la empresa en su parte física y lógica.	Visitas técnicas guiadas mediante la observación directa
Recolección de documentación de la empresa, de la red y de la documentación propia de la auditoria.	Ingeniero Auditor	3 – 7 de octubre de 2016	Empresa Panavias S.A.	Recolección del archivo corriente y permanente de la auditoria	Metodología de la auditoria de sistemas: Recolección de información
Realización del Plan de auditoria, programa de auditoria y el plan de pruebas de penetración a la red de datos.	-Ingeniero Auditor -Encargado del área de sistemas -Gerencia de la empresa	10 – 14 de octubre de 2016	Empresa Panavias S.A.	Escoger la normatividad a aplicar en auditoria. Diseñar los instrumentos de la auditoria y	Metodología de la auditoria de sistemas: Planeación de la auditoria

				las pruebas de penetración a ejecutar	
Ejecución de los instrumentos de recolección de información de la auditoria	Ingeniero Auditor Encargado del área de sistemas	17 - 28 de octubre de 2016	Empresa Panavias S.A.	Ejecución de los instrumentos de recolección de información de la auditoria	Metodología de la auditoria de sistemas: Ejecución de instrumentos
Ejecución de pruebas de penetración en la red de datos de la empresa Panavias S.A.	Ingeniero Auditor	17 - 28 de octubre de 2016	Oficina de sistemas y comunicaciones. Empresa Panavias S.A	Ejecutar pruebas de penetración para identificar vulnerabilidades existentes en la red de datos de la empresa.	Penetration test y/o Ethical Hacking
Realización de la gestión de los riesgos encontrados durante la auditoria.	Ingeniero Auditor	1 – 4 de noviembre de 2016	Empresa Panavias S.A.	Realizar una gestión integral del riesgo con las no conformidades encontradas en la auditoria	Metodología de la auditoria de sistemas: Gestión integral del riesgo informático
Organización de los papeles de trabajo y no conformidades encontradas en la	Ingeniero Auditor	14 – 25 de noviembre de	Empresa Panavias S.A.	Establecer procedimientos, controles y/o	Metodología de la auditoria de sistemas: Dictamen final de la auditoria

auditoria, a través de las guías de hallazgo o informe técnico.		2016		recomendaciones para las no conformidades encontradas en la auditoria.	
Elaboración del análisis de brecha y los niveles de madurez, de acuerdo a los resultados de la auditoria. Elaboración de la Declaración de aplicabilidad	Ingeniero Auditor	28 de noviembre a 2 de diciembre de 2016	Empresa Panavias S.A.	Establecer el nivel de madurez en el que se encuentra la organización. Establecer un documento que contenga los controles propuestos	Calcular el análisis de breca y determinar el nivel de madurez de acuerdo a la escala de la normatividad. Elaboración de la declaración de aplicabilidad con los controles y procedimientos establecidos.
Elaboración y entrega del informe ejecutivo o informe final de auditoria.	Ingeniero Auditor	5 – 12 de diciembre de 2016	Empresa Panavias S.A.	Entrega del informe final de auditoria a la gerencia de la empresa Panavias S.A.	Entrega del informe final de auditoria.

_____

Responsable. Ingeniero Auditor
Ing. Jesús G. Cortes Camacho

_____

Aprobado por:
Gerencia Empresa Panavias S.A.

Anexo A – Formatos y Documentación de la Auditoria: Panavias_DeclaracionAplicabilidad

		Salvaguardas Seleccionadas	
Sección	**Controles evaluados ISO/IEC 27002:2013**	**Salvaguardas Existentes**	**Salvaguardas Planeadas (Controles)**
5	**Políticas de Seguridad**		
5.1.	**Políticas de seguridad de la información**		

5.1.1.	La gerencia debería aprobar y publicar un documento de la política de seguridad de la información y comunicarla a todos los empleados de la empresa Panavias S.A.	No existen salvaguardas ya que nunca se han empleado controles	Elaborar e implementar un manual de políticas de seguridad de la información para el área de sistemas y comunicaciones de la empresa Panavias S.A. que contenga:
			- Políticas de seguridad de la información.
			  - Objetivos de la organización.
			  - Alcance.
			  - Definiciones.
			- Políticas de seguridad de la información en el recurso humano y responsabilidades
			- Políticas de control de accesos.
			  - Categorías y niveles de acceso
			  - Control de claves y nombres de usuario
			- Políticas de seguridad para la administración de sistemas y comunicaciones
			  - Políticas de uso de programas dentro de la empresa.

			- Políticas de uso de los dispositivos dentro de la empresa. - Políticas de uso de los puntos de red de datos. - Políticas de seguridad para el centro de datos y del centro del cableado. - Políticas sobre copias de seguridad. - Políticas de seguridad física y del entorno. - Políticas de seguridad de los equipos.
5.1.2.	Una vez implementada la documentación de política de seguridad de la información, esta se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente.	No existen salvaguardas ya que nunca se han empleado controles	Cada política implementada, debe tener un propietario que tenga la responsabilidad aprobada por la gerencia de la empresa Panavias S.A., para el desarrollo, revisión y evaluación de las políticas.
6.	**Organización de la Seguridad de la Información**		
6.1.	**Roles y responsabilidades para la seguridad de la información**		
6.1.1.	Los miembros de la	No existen	En el documento “Políticas de

	gerencia de la empresa Panavias S.A. deberían respaldar activamente las iniciativas de seguridad, asignando y aprobando explícitamente las responsabilidades en la seguridad de la información dentro de la empresa.	salvaguardas ya que nunca se han empleado controles	Seguridad de la Información" se deben definir las Políticas de seguridad en el recurso humano y responsabilidades dentro de la empresa Panavias S.A.
9.	**Control de Acceso**		
9.1.	**Requisitos del negocio para el control de acceso**		
9.1.2.	*Control de acceso a las redes y servicios asociados.* Para cumplir con el objetivo de control de "Solo se debería permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente", se debe mitigar los riesgos a continuación.		Para cumplir con el objetivo del control, se debe dar mitigación a los riegos que se enumeran en 9.1.2.1, 9.1.2.2, 9.1.2.3 y 9.1.2.4
9.1.2.1.	No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.	No existen salvaguardas ya que nunca se han empleado controles	En el manual de políticas de seguridad de la información, en donde se definen las políticas de seguridad de la información en el recurso humano y responsabilidades, se debe definir quién o quiénes son los funcionarios

			autorizados para el ingreso al área de red, como la administración de los servicios mismos. Además, también se debe definir en la política de control de acceso, un control que mencione los niveles de acceso a los sistemas y servicio de red que deberían tener los usuarios en la empresa Panavias S.A. El manual de procedimientos para la gestión de la infraestructura tecnológica de la empresa Panavias S.A. deberá contener lo siguiente: - Objetivos de la empresa - Alcance - Responsabilidades y funciones - Inventario y valoración de los elementos de red (físico y lógico) - Controles de acceso de usuarios - Herramientas de gestión de la red (herramientas para mapeo de redes, control de tráfico y monitorización de la red) - Plan de respaldo en caso de incidentes
9.1.2.2.	No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda utilizar tanto controles de acceso físico a la oficina asesora de comunicaciones y sistemas, como controles de acceso lógico a la red de la empresa Panavias S.A. Las recomendaciones técnicas para

			realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-002.
9.1.2.3.	No existen medios usados para acceder a las redes y servicios de red como el uso de VPN.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda utilizar medios de seguridad perimetral como es el uso de redes virtuales privadas (VPN). Esto podría presentar una ventaja para la organización ya que permite crear una capa extra de seguridad dentro de la red local para proteger los activos de información, como lo es el uso del software Helysa GW, donde se almacena la gran mayoría de los activos de información de la empresa. Además, que la red VPN se basa en el “”protocolo túnel”, el cual cifra los datos que se transmiten dentro de la red privada.
9.1.2.4.	No existe monitoreo del uso de los servicios de red	No existen salvaguardas ya que nunca se han empleado controles	El administrador de red es el encargado de gestionar y controlar los servicios de red que permitan el correcto funcionamiento de la infraestructura telemática. Además, está a cargo de implementar medidas de protección adecuadas, supervisar los registros y actividades que permitan salvaguardar la red tanto en su parte física, como lógica. También implementar herramientas que permitan gestionar y controlar todos los procesos de los servicios de red. Se deben implementar herramientas para el mapeo de redes, análisis de tráfico, herramientas para identificar vulnerabilidades en la red y herramientas para monitoreo.

			Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-004.
9.4.	**Control de acceso a sistemas y aplicaciones**		
9.4.1.	*Restricción de acceso a la información.* Para cumplir con el objetivo de control de "El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso" se debe mitigar los riesgos a continuación.		Para cumplir con el objetivo del control, se debe dar mitigación al riego que se enumera en 9.4.1.1.
9.4.1.1.	No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.	No existen salvaguardas ya que nunca se han empleado controles	En el manual de políticas de seguridad de la información, en donde se definen las políticas de control de acceso, se debe definir un control de claves y nombres de usuario, donde se debe declarar el uso de contraseñas seguras y el cambio periódica de estas, tanto para el acceso de los servicios de red, entre ellos el software Helysa GW, en el cual se almacenan la mayoría delos activos de información de la empresa como también para el ingreso de los equipos de cómputo, con el objetivo de fortalecer la integridad de la información de la empresa.
13.	**Seguridad en las**		

	Telecomunicaciones		
13.1.	**Gestión de la Seguridad de las Redes**		
13.1.1.	*Control de Redes.* Para cumplir con el objetivo de control de "Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones" se debe mitigar los riesgos a continuación.		Para cumplir con el objetivo del control, se debe dar mitigación a los los riegos que se enumera en 13.1.1.1, 13.1.1.2, 13.1.1.3, 13.1.1.4, 13.1.1.5, 13.1.1.6, 13.1.1.7, 13.1.1.8, 13.1.1.9, 13.1.1.10, 13.1.1.11, 13.1.1.12 y 13.1.1.13.
13.1.1.1.	No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.	No existen salvaguardas ya que nunca se han empleado controles	Implementar controles en cuanto a la gestión de los equipos de redes, como lo son: - Ordenar el equipo de red, como lo son servidores, switches, routers, cableado, en un armario metálico o rack de comunicaciones. - El servidor principal se debe encontrar ya sea dentro del rack de comunicaciones o en la oficina de comunicaciones y sistemas de la empresa. - El cableado debe estar debidamente etiquetado. - Elaborar un inventario con los activos informáticos de red, tanto en su parte física, como lógica. - Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y

			coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.
13.1.1.2.	No se incluye el desarrollo de los procedimientos de operación apropiados para la red.	No existen salvaguardas ya que nunca se han empleado controles	Elaboración del documento de Políticas de Seguridad y el Manual de Procedimientos para la empresa Panavias S.A.
13.1.1.3.	No existen controles para salvaguardar los servicios de seguridad informática en la red.	No existen salvaguardas ya que nunca se han empleado controles	Establecer controles para salvaguardar los servicios de seguridad informática en la red, como lo son la confidencialidad, disponibilidad e integridad de los activos de informacion e informáticos. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-008.
13.1.1.4.	No existen controles para proteger los sistemas y aplicaciones conectados.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda hacer uso de Sistemas de Seguridad Perimetrales para proteger los sistemas de red y aplicaciones en la empresa. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-009.
13.1.1.5.	No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda el uso de un Sistema de Alimentación Ininterrumpida (UPS) en caso de un apagón eléctrico, el cual puede proporcionar energía para que la infraestructura de red y de cómputo pueda seguir funcionando y así no afectar su disponibilidad. Otra ventaja de estos sistemas es filtra

			las subidas y bajadas de tensión que llega a la carga eléctrica, evitando así un cortos en el flujo eléctrico en la empresa.
13.1.1.6.	No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda realizar un registro de todos los accesos (logged) para producir un rastro de referencia (Reference trail), como también la implementación de IDS, para detectar acciones que puedan afectar la red y los servicios de red en la empresa. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-011.
13.1.1.7.	No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.	No existen salvaguardas ya que nunca se han empleado controles	En primer lugar se debe implementar la documentación correspondiente a manual de políticas y manual de procedimientos, con el objetivo de realizar un seguimiento periódico al cumplimiento de estos controles. Las revisiones de estos controles, debe realizarse a manera de auditorías internas en la empresa, con el objetivo de verificar que estos procedimientos se cumplan y se puedan medir. Las políticas y controles ayudaran a la empresa a planificar, desarrollar e implementar soluciones respecto a su infraestructura tecnológica, como también garantizar los servicios de seguridad informática de los activos informáticos y de información.
13.1.1.8.	No se restringe la conexión a	No existen salvaguardas	Se debe crear un registro de todos los equipos y dispositivos que son

	dispositivos no autorizados a los sistemas a la red.	ya que nunca se han empleado controles	permitidos, conectados a la red de datos de la empresa Panavias S.A. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-013.
13.1.1.9.	No existen procedimientos del uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red	No existen salvaguardas ya que nunca se han empleado controles	En el manual de políticas de seguridad de la información, en donde se definen las políticas de control de acceso, se debe definir un control de claves y nombres de usuario, donde se debe declarar que el acceso a la información de la red y los servicios de red de la empresa, debe estar controlado. Corresponde a la oficina asesora de Comunicaciones y Sistemas, elaborar, mantener y publicar los documentos de servicios de red y procedimientos de administración de cuentas de usuario para el uso de servicios de red que ofrece la empresa Panavias S.A
13.1.2.	*Seguridad de los Servicios de Red.* Para cumplir con el objetivo de control de "Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya		Para cumplir con el objetivo del control, se debe dar mitigación a los riegos que se enumera en 13.1.2.1, 13.1.2.2 y 13.1.2.3

	sea que los servicios se presten internamente o se contraten externamente" se deben mitigar los riesgos a continuación.		
13.1.2.1.	No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda activar los protocolos criptográficos en el host, en caso de que se realicen transacciones o intercambio de información sensible online por medio de su servicio web como lo son por ejemplo, transacciones de pagos, autenticación de usuarios en la página, manejo de cuentas y facturas, intercambio de información con organizaciones externas. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-014.
13.1.2.2.	No existen controles para asegurar la conexión segura a la red.		Se recomienda implementar controles que permitan asegurar la conexión segura a la red de datos de la empresa. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-015.
13.1.2.3.	Vulnerabilidad por puertos sensibles abiertos y expuestos.		Durante la ejecución de pruebas de penetración, se encontró puertos con información sensible que pueden ser explotados, tanto en la dirección del host como de la red local.

			Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-018.
13.1.3.	*Separación de Redes.* Para cumplir con el objetivo de control de "Los grupos de servicios de la información, usuarios y sistemas de información se deberían separar en las redes" se deben mitigar los riesgos a continuación.		Para cumplir con el objetivo del control, se debe dar mitigación a los riegos que se enumera en 13.1.3.1.
13.1.3.1.	La red se no se encuentra dividida en dominios de red separados o segmentada.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda segmentar la red la empresa, con el objetivo de que al dividir la red en segmentos, aumenta su rendimiento y disponibilidad, esto para el caso de la red de la empresa que contiene muchos equipos y dispositivos conectados. Las recomendaciones técnicas para realizar las acciones correctivas correspondientes, se encuentran en la guía de hallazgos AP-GH-017.
11.	**Seguridad Física y del Entorno**		
11.2.	**Seguridad de los equipos**		
11.2.1.	*Ubicación y Protección de los Equipos.* Para cumplir con el objetivo de		Para cumplir con el objetivo del control, se debe dar mitigación a los riegos que se enumera en 11.2.1.1, 11.2.1.2 y 11.2.1.3.

	control de “Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado” se deben mitigar los riesgos a continuación.		
11.2.1.1.	Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda establecer los siguientes controles: - Establecer responsabilidades sobre quien tiene acceso al área de red y los equipos de red. - Ordenar en el equipo de red en el área que corresponde. Se debe ordenar en un armario metálico o rack de comunicaciones con cada uno de sus elementos registrados en un inventario y su cableado debidamente etiquetado. - Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.
11.2.1.2.	No se han adoptado controles para minimizar el riesgo de amenazas físicas y	No existen salvaguardas ya que nunca se han	Se recomienda utilizar cámaras de vigilancia para cada una de las áreas de la empresa para prevenir el posible robo de equipos.

	ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo	empleado controles	También, implementar las alarmas contra incendio en cada área de la empresa para prevenir posibles incendios o expansión de humo de este en caso de una eventualidad. Realizar revisiones periódicas, evaluar y controlar permanentemente la seguridad física para minimizar riesgos de amenazas físicas, ambientales y de origen industrial que se puedan presentar dentro de la empresa.
11.2.1.3.	El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.	No existen salvaguardas ya que nunca se han empleado controles	En el manual de políticas de seguridad de la información, en donde se definen las políticas de seguridad de la información en el recurso humano y responsabilidades, se debe definir, como parte de las obligaciones del encargado de la oficina asesora de comunicaciones y sistemas de la empresa, funciones que tienen que ver con el mantenimiento y seguimiento de las condiciones ambientales que puedan afectar las operaciones o las instalaciones de cómputo y de red. Estas deben ser revisadas periódicamente para prevenir cualquier eventualidad que puedan afectar la infraestructura de la empresa.
11.2.3.	*Seguridad del Cableado.* Para cumplir con el objetivo de control de “El cableado de		Para cumplir con el objetivo del control, se debe dar mitigación al riegos que se enumera en 11.2.2.1

	energía y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño" se deben mitigar los riesgos a continuación.		
11.2.2.1	Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.	No existen salvaguardas ya que nunca se han empleado controles	Se recomienda realizar las siguientes acciones establecidas en la guía de hallazgos AP-GH-022 para la seguridad del cableado

Anexo A – Formatos y Documentación de la Auditoria: Panavias_InformeFinal

San Juan de Pasto, 9 de diciembre de 2016

Ingeniero
LUIS ALBERTO CALDERON TORRES
Gerente
PANAVIAS S.A.

Cordial Saludo

Asunto: Informe Final de Auditoria

La presente, tiene como finalidad mostrar los resultados de la auditoria a la seguridad de la red de datos de la empresa Panavias S.A. realizada en el periodo comprendido entre agosto de 2016 a diciembre de 2016, donde se encontraron algunos procesos y procedimientos irregulares que se deben realizar acciones correctivas mediante la planeación y gestión de controles adecuados a la red de datos de la empresa.

Para llevar a cabo este proceso de auditoría, se utilizaron diversos medios como lo fue la ejecución de pruebas de penetración o testeo a la red, para identificar posibles amenazas o vulnerabilidades, como también medios de recolección de la información como lo fue la aplicación de entrevistas, listas de chequeo, cuestionarios de control, guías de hallazgos y la observación directa mediante visitas técnicas. El proceso de auditoria fue evaluado, de acuerdo a la normatividad ISO/IEC 27001:2013 e ISO/IEC 27002:2013, normas internacionales para la gestión de la seguridad de la información con los subdominios relacionados con el objetivo de la auditoria.

En algunos casos, se tuvo problemas con la recolección de la información documental, por lo cual genero retrasos en la organización de los resultados y la entrega del informe final.

A continuación se muestran los resultados obtenidos en la auditoria y recomendaciones generales de los procesos que fueron auditados, en donde se deberían realizar las respectivas acciones correctivas.

Riesgos Encontrados.

- No existe documentación relacionada con políticas de seguridad y/o manual de procedimientos para asegurar la infraestructura tecnológica de la empresa.
- No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.
- No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.
- No existen medios usados para acceder a las redes y servicios de red.
- No existe monitoreo del uso de los servicios de red
- No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.
- No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.
- No se incluye el desarrollo de los procedimientos de operación apropiados para la red.
- No existen controles para salvaguardar los servicios de seguridad informática en la red.
- No existen controles para proteger los sistemas y aplicaciones conectados.
- No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.
- No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.
- No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.
- No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.
- No existen controles para asegurar la conexión segura a la red.
- No existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.
- La red se no se encuentra dividida en dominios de red separados o segmentada.
- Vulnerabilidad por puertos sensibles abiertos y expuestos.

- Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas
- No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo
- El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.
- Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.

De acuerdo a los hallazgos encontrados, se hacen las siguientes recomendaciones, a nivel general para controlar y mejorar los procesos en cuanto a la red de datos de la empresa Panavias S.A. Se debe tener en cuenta, que las recomendaciones técnicas, propuestas en las guías de hallazgo, se entregan al encargado del área de sistemas y comunicaciones, el ingeniero Holmes Zuñiga, para que se hagan las respectivas acciones correctivas.

Recomendaciones.

- Elaborar la documentación respecto a las políticas de seguridad de la información y el manual de procedimientos para gestionar y asegurar la infraestructura tecnológica de la empresa Panavias S.A.

- En cuanto al control de acceso, se deben implementar controles respecto a procedimientos de autorización para determinar el personal que accede al área de red y los servicios de red, como también la protección del acceso a la red y servicios y medios seguros para acceder a las mismas.

- La seguridad en telecomunicaciones en la empresa, de acuerdo a los parámetros evaluados, es el de mayor criticidad y se deben implementar controles o acciones correctivas inmediatas. Entre ellos se encuentra la implementación de acciones de monitoreo de red, implementar controles

para salvaguardar los servicios de seguridad informática en la red, como lo son los activos de información e informáticos de la empresa, como también la implementación de Sistemas de Seguridad Perimetrales para proteger los sistemas de red y aplicaciones en la empresa.

- En cuanto a la seguridad física de los equipos de cómputo y de red, se deben establecer controles respecto al mantenimiento de los mismos, ya que actualmente lo realiza la empresa proveedora. Es preciso que estos procesos de mantenimiento los realice el personal encargado del área de sistemas y comunicaciones de la empresa. Como también, se deben implementar, y reforzar los que se tienen, controles para minimizar el riesgo de amenazas físicas y ambientales que se pueden presentar y que atenten contra los equipos de red y cómputo de la empresa Panavias S.A. También, el cambio de empresa proveedora que ofrezca una infraestructura física y lógica más robusta y que no afecte la disponibilidad de los servicios de red.

Con base a estas recomendaciones generales y las recomendaciones técnicas, propuestas en las guías de hallazgo, que se entregan al encargado del área, se debe poner en marcha planes de mejoramiento y de acción correctiva con miras a la adecuación y optimización de los servicios de red de la empresa.

Agradezco de antemano la atención prestada a la misma,

Cordialmente

_____

Ing. Jesús Germán Cortés Camacho
CC. 1085267906 Pasto
TP No. 52255-32887 NRÑ

Anexo B – A5. Políticas de Seguridad de la Información: Formato_ListadeChequeoA5

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	**Fecha**			

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A5. POLITICAS DE LA SEGURIDAD DE LA INFORMACION
Subdominio A5.1.1. Políticas para la Seguridad de la Información
Subdominio A5.1.2. Revisión de las Políticas para la Seguridad de la Información

Objetivo:

Verificar los controles A5.1.1. “Políticas para la Seguridad de la Información” y A5.1.2. “Revisión de las Políticas para la Seguridad de la Información”, según la norma NTC/ISO/IEC 27002:2013.

Control:

5.1.1. “Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.”

5.1.2. “Las políticas para la seguridad de la información se deberían revisar a intervalos planificados si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.”

La política de seguridad acerca de la “Políticas para la Seguridad de la Información” y “Revisión de las Políticas para la Seguridad de la Información “ según la normatividad, tienen las siguientes especificaciones:

Ítem	Si	No	N/A
A5.1.1. Políticas para la Seguridad de la Información			
¿Las políticas maneja la estrategia de negocios de acuerdo a los requisitos de la empresa?			
¿Las políticas manejan Reglamentaciones, legislación y			

contratos?			
¿Las políticas manejan el entorno actual y proyectado hacia las amenazas de la seguridad de la información?			
¿Las políticas contienen definición de la seguridad de la información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información?			
¿La políticas contienen la asignación de las responsabilidades, generales y específicas para la gestión de la seguridad de la información, a roles definidos?			
¿Las políticas contienen los procesos para manejar desviaciones y excepciones?			
Las políticas de seguridad contienen temas concernientes a:			
Control de acceso			
Clasificación de la información			
Seguridad física y del entorno			
Uso aceptable de los activos			
Políticas de escritorio y pantalla limpia			
Transferencia de información			
Dispositivos móviles y teletrabajo			
Restricciones sobre instalaciones y uso del software			
Copias de respaldo			
Transferencia de información			
Protección contra códigos maliciosos			
Gestión de las vulnerabilidades técnicas			
Controles criptográficos			
Seguridad de las comunicaciones			
Privacidad y protección de información de datos personales			
Relación con los proveedores			
A5.1.2. Revisión de las Políticas para la Seguridad de la Información			
¿Cada política tiene un propietario que tenga la responsabilidad aprobada por la dirección, para el desarrollo, revisión y evaluación de las políticas?			
Se realiza revisión periódica de las políticas de seguridad			

Anexo B – A5. Políticas de Seguridad de la Información: ListadeChequeoA5

PANAVIAS	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.	UNAD Versión 1.0.

Responsable	Ing. Jesús G. Cortés	Fecha	25	OCT.	2016

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013

Dominio A5. POLITICAS DE LA SEGURIDAD DE LA INFORMACION

Subdominio A5.1.1. Políticas para la Seguridad de la Información

Subdominio A5.1.2. Revisión de las Políticas para la Seguridad de la Información

Objetivo:

Verificar los controles A5.1.1. "Políticas para la Seguridad de la Información" y A5.1.2. "Revisión de las Políticas para la Seguridad de la Información", según la norma NTC/ISO/IEC 27002:2013.

Control:

5.1.1. "Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes."

5.1.2. "Las políticas para la seguridad de la información se deberían revisar a intervalos planificados si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas."

La política de seguridad acerca de la "Políticas para la Seguridad de la Información" y "Revisión de las Políticas para la Seguridad de la Información " según la normatividad, tienen las siguientes especificaciones:

Ítem	Si	No	N/A
A5.1.1. Políticas para la Seguridad de la Información			
¿Las políticas maneja la estrategia de negocios de acuerdo a los requisitos de la empresa?			X
¿Las políticas manejan Reglamentaciones, legislación y contratos?			X
¿Las políticas manejan el entorno actual y proyectado hacia las amenazas de la seguridad de la información?			X
¿Las políticas contienen definición de la seguridad de la			

información, objetivos y principios para orientar todas las actividades relacionadas con la seguridad de la información?			X
¿La políticas contienen la asignación de las responsabilidades, generales y específicas para la gestión de la seguridad de la información, a roles definidos?			X
¿Las políticas contienen los procesos para manejar desviaciones y excepciones?			X
Las políticas de seguridad contienen temas concernientes a:			
Control de acceso			X
Clasificación de la información			X
Seguridad física y del entorno			X
Uso aceptable de los activos			X
Políticas de escritorio y pantalla limpia			X
Transferencia de información			X
Dispositivos móviles y teletrabajo			X
Restricciones sobre instalaciones y uso del software			X
Copias de respaldo			X
Transferencia de información			X
Protección contra códigos maliciosos			X
Gestión de las vulnerabilidades técnicas			X
Controles criptográficos			X
Seguridad de las comunicaciones			X
Privacidad y protección de información de datos personales			X
Relación con los proveedores			X
A5.1.2. Revisión de las Políticas para la Seguridad de la Información			
¿Cada política tiene un propietario que tenga la responsabilidad aprobada por la dirección, para el desarrollo, revisión y evaluación de las políticas?			X
Se realiza revisión periódica de las políticas de seguridad			X
NOTA: No existen Políticas Para la Seguridad de la Información en la empresa.			

Anexo C – A6. Organización de la Seguridad de la Información: Formato_ListadeChequeoA6

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	**Fecha**			

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Subdominio A6.1.1 Roles y Responsabilidades para la Seguridad de la Información

Objetivo:

Verificar los controles A6.1.1 de "Roles y Responsabilidades para la Seguridad de la Información", según la norma NTC/ISO/IEC 27002:2013.

Controles:
6.1.1. "Se debería definir y asignar todas las responsabilidades de la seguridad de la información."

La política de seguridad acerca de "Roles y Responsabilidades de la Seguridad de la Información" tiene las siguientes especificaciones:

Ítem	Si	No	N/A
¿Se identifican y se definen los activos y los procesos de seguridad de la información?			
¿Se asignan la entidad responsable de cada activo o procesos de seguridad de la información y se documenta los detalles de esta responsabilidad?			
¿Se definen y documenta los niveles de autorización?			
Para tener la capacidad de cumplir las responsabilidades en el área de seguridad de la información el personal nombrados para estas funciones:			
¿Son competentes en el área?			
¿Se brinda oportunidades de mantenerse actualizados con los			

avances en este tema?			
¿Se identifica y documenta la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores?			

Anexo C – A6. Organización de la Seguridad de la Información: ListadeChequeoA6

PANAVIAS	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.	UNAD Versión 1.0.

Responsable	Ing. Jesús G. Cortés	Fecha	25	oct.	2016

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Subdominio A6.1.1 Roles y Responsabilidades para la Seguridad de la Información

Objetivo:

Verificar los controles A6.1.1 de "Roles y Responsabilidades para la Seguridad de la Información", según la norma NTC/ISO/IEC 27002:2013.

Controles:

6.1.1. "Se debería definir y asignar todas las responsabilidades de la seguridad de la información."

La política de seguridad acerca de "Roles y Responsabilidades de la Seguridad de la Información" tiene las siguientes especificaciones:

Ítem	Si	No	N/A
¿Se identifican y se definen los activos y los procesos de seguridad de la información?			X
¿Se asignan la entidad responsable de cada activo o procesos de seguridad de la información y se documenta los detalles de esta responsabilidad?			X
¿Se definen y documenta los niveles de autorización?			X
Para tener la capacidad de cumplir las responsabilidades en el área de seguridad de la información el personal nombrados para estas funciones:			
¿Son competentes en el área?			X
¿Se brinda oportunidades de mantenerse actualizados con los avances en este tema?			X
¿Se identifica y documenta la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores?			X

NOTA: No existen Procedimientos para la Seguridad de la información, por Consiguiente, no se pueden asignar Roles y Responsabilidades.

Anexo D – A9. Control de Acceso: Formato_ListadeChequeoA9

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	**Fecha**			

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A9. CONTROL DE ACCESO
Subdominio A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Subdominio A9.4.1 Restricción de Acceso a la Información

Objetivo:

Verificar los controles A9.1.2 de "Control de Acceso a las Redes y Servicios Asociados", y A9.4.1 de según la norma NTC/ISO/IEC 27002:2013.

Control:

9.1.2. "Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente."

9.4.1. "El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso."

Las políticas de seguridad acerca de "Control de Acceso a las Redes y Servicios Asociados" y "Restricción de Acceso a la Información" según la normatividad, tiene las siguientes especificaciones:

Ítem	Si	No	N/A
A9.1.2. Control de Acceso a las Redes y Servicios Asociados			
¿Las redes y servicios de red solo tiene el acceso el usuario autorizado?			
¿Existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red?			
¿Existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?			
¿Existen medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?			

¿Existen requisitos de autenticación de usuarios para acceder a diversos servicios de red?			
¿Existe monitoreo del uso de los servicios de red?			
A9.4.1 Restricción de Acceso a la Información			
¿Existen menús para controlar acceso a la funcionalidad de las aplicaciones?			
¿Existe control de los datos a los que puede tener acceso un usuario particular?			
¿Existe control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?			
¿Existe control de los derechos de acceso de otras aplicaciones?			
¿Existe limitación de la información contenida en las salidas?			
¿Existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?			

Anexo D – A9. Control de Acceso: ListadeChequeoA9

PANAVIAS	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	Fecha	25	oct.	2016

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A9. CONTROL DE ACCESO
Subdominio A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Subdominio A9.4.1 Restricción de Acceso a la Información

Objetivo:

Verificar los controles A9.1.2 de "Control de Acceso a las Redes y Servicios Asociados", y A9.4.1 de según la norma NTC/ISO/IEC 27002:2013.

Control:

9.1.2. "Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente."

9.4.1. "El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso."

Las políticas de seguridad acerca de "Control de Acceso a las Redes y Servicios Asociados" y "Restricción de Acceso a la Información" según la normatividad, tiene las siguientes especificaciones:

Item	Si	No	N/A
A9.1.2. Control de Acceso a las Redes y Servicios Asociados			
¿Las redes y servicios de red solo tiene el acceso el usuario autorizado?	X		
¿Existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red?		X	
¿Existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?		X	
¿Existen medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		X	
¿Existen requisitos de autenticación de usuarios para acceder a diversos servicios de red?	X		

¿Existe monitoreo del uso de los servicios de red?		X	
A9.4.1 Restricción de Acceso a la Información			
¿Existen menús para controlar acceso a la funcionalidad de las aplicaciones?	X		
¿Existe control de los datos a los que puede tener acceso un usuario particular?	X		
¿Existe control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?	X		
¿Existe control de los derechos de acceso de otras aplicaciones?	X		
¿Existe limitación de la información contenida en las salidas?	X		
¿Existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?		X	

Anexo D – A9. Control de Acceso: CuetionarioControlA9

PANAVIAS INGENIERÍA & CONSTRUCCIONES	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-CC-001 Versión 1.0.

Elaborado por	Ing. Jesús G. Cortés	**Fecha**	25	oct.	2016
Respondido por	Ing. Holmes Zuñiga.				

Cuestionario de Control	
Dominio	A9. CONTROL DE ACCESO
Proceso	A9.1.2. Control de Acceso a las Redes y Servicios Asociados A9.4.1 Restricción de Acceso a la Información
Objetivo del control	Verificar los controles A9.1.2 de "Control de Acceso a las Redes y Servicios Asociados", y A9.4.1 de según la norma NTC/ISO/IEC 27002:2013.

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Pregunta	Si	No	N/A	Observaciones
¿Las redes y servicios de red solo tiene el acceso el usuario autorizado?	3			Servicios de red solo accede el encargado área de red, cualquiera.
¿Existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red?		4		No existen controles para determinar quien accede al area de la red.
¿Existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red?		4		No existen controles para proteger el acceso al area de la red.
¿Existen medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas)?		3		No existe VPN si hay red inalambrica
¿Existen requisitos de autenticación de usuarios para acceder a diversos servicios de red?	2			si existen requisitos de autenticacion para los servicios de red.

¿Existe monitoreo del uso de los servicios de red?		5		No existe monitoreo de los servicios de red.
¿Existen menús para controlar acceso a la funcionalidad de las aplicaciones?	1			Si existe control de acceso. Software Hetysa GW.
¿Existe control de los datos a los que puede tener acceso un usuario particular?	1			Si existe control de los datos en relación al Software Hetysa GW.
¿Existe control de los derechos de acceso de los usuarios, por ejemplo, a leer, escribir, borrar y ejecutar?	1			Solo el USUARIO autorizado puede realizar estas acciones.
¿Existe control de los derechos de acceso de otras aplicaciones?	1			Si existen controles basados en roles.
¿Existe limitación de la información contenida en las salidas?	3			El Software Hetysa GW si posee, en la red estos son mínimos
¿Existen controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos?		5		No existen este tipo de controles para asegurar los datos en las aplicaciones y en la red.
TOTALES	12	21		
PUNTAJE TOTAL		33		

Anexo E – A11. Seguridad Física y del Entorno: Formato_ListadeChequeoA11

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	**Fecha**			

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio A11.2.1 Ubicación y Protección de los Equipos
Subdominio A11.2.3 Seguridad del Cableado

Objetivo:

Verificar los controles A11.2.1 de "Ubicación y Protección de los Equipos" y A11.2.3 de "Seguridad del Cableado", según la norma NTC/ISO/IEC 27002:2013.

Controles:

11.2.1. "Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado."

11.2.3. "El cableado de energía y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño."

Las políticas de seguridad acerca de "Ubicación y Protección de los Equipos" y "Seguridad del Cableado" según la normatividad, tienen las siguientes especificaciones:

Ítem	Si	No	N/A
A11.2.1 Ubicación y Protección de los Equipos			
¿Las instalaciones de procesamiento de información y de redes están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas?			
¿Se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos			

químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo?			
¿Se hace seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información y de redes?			
Subdominio A11.2.3 Seguridad del Cableado			
Las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información, ¿son subterráneas o cuentan con otra protección alternativa?			
¿Los cables de energía eléctrica se encuentran separados de los cables de telecomunicaciones para evitar interferencia?			
¿Existen controles para inspecciones físicas al cableado?			

Anexo E – A11. Seguridad Física y del Entorno: ListadeChequeoA11

PANAVIAS	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.	UNAD Versión 1.0

Responsable	Ing. Jesús G. Cortés	Fecha	25	Oct.	2016

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio A11.2.1 Ubicación y Protección de los Equipos
Subdominio A11.2.3 Seguridad del Cableado

Objetivo:

Verificar los controles A11.2.1 de "Ubicación y Protección de los Equipos" y A11.2.3 de "Seguridad del Cableado", según la norma NTC/ISO/IEC 27002:2013.

Controles:

11.2.1. "Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado."

11.2.3. "El cableado de energía y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño."

Las políticas de seguridad acerca de "Ubicación y Protección de los Equipos" y "Seguridad del Cableado" según la normatividad, tienen las siguientes especificaciones:

Ítem	Si	No	N/A
A11.2.1 Ubicación y Protección de los Equipos			
¿Las instalaciones de procesamiento de información y de redes están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas?		X	
¿Se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo?		X	
¿Se hace seguimiento de las condiciones ambientales tales como			

temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información y de redes?	X		
Subdominio A11.2.3 Seguridad del Cableado			
Las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información, ¿son subterráneas o cuentan con otra protección alternativa?		X	
¿Los cables de energía eléctrica se encuentran separados de los cables de telecomunicaciones para evitar interferencia?	X		
¿Existen controles para inspecciones físicas al cableado?	X		

Anexo E – A11. Seguridad Física y del Entorno: CuestionarioControlA11

PANAVIAS	AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-CC-003 Versión 1.0

Elaborado por	Ing. Jesús G. Cortés	Fecha	25	oct.	2016.
Respondido por	Ing. Holmes Zuñiga.				

Cuestionario de Control	
Dominio	A11. SEGURIDAD FISICA Y DEL ENTORNO
Proceso	A11.2.1 Ubicación y Protección de los Equipos A11.2.3 Seguridad del Cableado
Objetivo del control	Verificar los controles A11.2.1 de "Ubicación y Protección de los Equipos" y A11.2.3 de "Seguridad del Cableado", según la norma NTC/ISO/IEC 27002:2013.

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Pregunta	Si	No	N/A	Observaciones
¿Las instalaciones de procesamiento de información y de redes están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas?		5		Los equipos de red no estan ubicados en el area de red, como el servidor.
¿Se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo?		4		Existen cámaras de vigilancia y alarmas contra incendio pero estas no abarcan todas las oficinas de la empresa. Cable UTP de cobre, vulnerable a interferencias.
¿Se hace seguimiento de las condiciones ambientales tales como temperatura y humedad, para				El seguimiento lo realiza la empresa Proseguridad, pero

determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información y de redes?	4			este no se realiza periodicamente. Dos veces al año como máximo.
Las líneas de energía eléctrica y de telecomunicaciones que entran a las instalaciones de procesamiento de información, ¿son subterráneas o cuentan con otra protección alternativa?		5		El cableado UTP de cobre no cuenta con protección de blindaje.
¿Los cables de energía eléctrica se encuentran separados de los cables de telecomunicaciones para evitar interferencia?	3			El cableado si se encuentra separado pero hay interferencias implementar fibra optica.
¿Existen controles para inspecciones físicas al cableado?	4			Este señalado tambien lo hace la empresa proveedora
TOTALES	11	14		
PUNTAJE TOTAL	25			

Anexo F – A13. Seguridad en las Telecomunicaciones: Formato_ListadeChequeoA13

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	**Fecha**			

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio A13.1.1 Controles de Redes
Subdominio A13.1.2 Seguridad de los Servicios de Red
Subdominio A13.1.3 Separación en las Redes

Objetivo:

Verificar los controles A13.1.1 de “Control de Redes”, A13.1.2 de “Seguridad de los Servicios de Red”, y A13.1.3 de “Separación en las Redes” según la norma NTC/ISO/IEC 27002:2013.

Control:

13.1.1. “Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.”

13.1.2. “Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.”

13.1.3. “Los grupos de servicios de la información, usuarios y sistemas de información se deberían separar en las redes”

Las políticas de seguridad acerca de “Controles de Redes”, “Seguridad de los Servicios de Red” y “Separación en las Redes” según la normatividad, tiene las siguientes especificaciones:

Ítem	**Si**	**No**	**N/A**
A13.1.1 Controles de Redes			

¿Se establecen responsabilidades y procedimientos para la gestión de equipos de redes?			
¿Se separa la responsabilidad operacional por las redes, de las operaciones de cómputo?			
¿Existen controles para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?			
¿Existen controles para proteger los sistemas y aplicaciones conectados?			
¿Se cuenta con controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados?			
¿Se cuenta con un registro (Logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?			
¿Se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?			
Los sistemas en la red, ¿se autentican?			
¿Se restringe la conexión a dispositivos no autorizados a los sistemas a la red?			
A13.1.2 Seguridad de los Servicios de Red			
¿Existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red?			
¿Existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red?			
¿Existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red?			
A13.1.3 Separación en las Redes			
¿La red se encuentra dividida en dominios de red separados?			
¿Se permite el acceso entre dominios de redes controlando el acceso utilizando firewalls o enrutado de filtrado?			
¿Las redes inalámbricas (redes externas) se encuentran separadas a las redes internas?			
¿Se emplean mecanismos de autenticación, criptografía y			

tecnologías de control de accesos de redes entre las redes?			

Anexo F – A13. Seguridad en las Telecomunicaciones: ListadeChequeoA13

PANAVIAS	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0.

Responsable	Ing. Jesús G. Cortés	Fecha	25	OCT.	2016.

LISTA DE CHEQUEO – NTC/ISO/IEC 27002:2013
Dominio A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio A13.1.1 Controles de Redes
Subdominio A13.1.2 Seguridad de los Servicios de Red
Subdominio A13.1.3 Separación en las Redes

Objetivo:

Verificar los controles A13.1.1 de "Control de Redes", A13.1.2 de "Seguridad de los Servicios de Red", y A13.1.3 de "Separación en las Redes" según la norma NTC/ISO/IEC 27002:2013.

Control:

13.1.1. "Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones."

13.1.2. "Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente."

13.1.3. "Los grupos de servicios de la información, usuarios y sistemas de información se deberían separar en las redes"

Las políticas de seguridad acerca de "Controles de Redes", "Seguridad de los Servicios de Red" y "Separación en las Redes" según la normatividad, tiene las siguientes especificaciones:

Ítem	Si	No	N/A
A13.1.1 Controles de Redes			
¿Se establecen responsabilidades y procedimientos para la gestión de equipos de redes?		X	
¿Se separa la responsabilidad operacional por las redes, de las			

operaciones de cómputo?		X	
¿Existen controles para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?		X	
¿Existen controles para proteger los sistemas y aplicaciones conectados?		X	
¿Se cuenta con controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados?		X	
¿Se cuenta con un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?		X	
¿Se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?		X	
Los sistemas en la red, ¿se autentican?	X		
¿Se restringe la conexión a dispositivos no autorizados a los sistemas a la red?		X	
A13.1.2 Seguridad de los Servicios de Red			
¿Existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red?		X	
¿Existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red?		X	
¿Existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red?		X	
A13.1.3 Separación en las Redes			
¿La red se encuentra dividida en dominios de red separados?		X	
¿Se permite el acceso entre dominios de redes controlando el acceso utilizando firewalls o enrutado de filtrado?			X
¿Las redes inalámbricas (redes externas) se encuentran separadas a las redes internas?			X
¿Se emplean mecanismos de autenticación, criptografía y tecnologías de control de accesos de redes entre las redes?			X

Anexo F – A13. Seguridad en las Telecomunicaciones: CuetionarioControlA13

PANAVIAS INGENIERÍA Y CONSTRUCCIONES NIT 830.130.560-4	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Ref. AP-CC-002 Versión 1.0

Elaborado por	Ing. Jesús G. Cortés	**Fecha**	25	Oct.	2016.
Respondido por	Ing. Holmes Zuñiga.				

Cuestionario de Control	
Dominio	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Proceso	A13.1.1 Controles de Redes A13.1.2 Seguridad de los Servicios de Red A13.1.3 Separación en las Redes
Objetivo del control	Verificar los controles A13.1.1 de "Control de Redes", A13.1.2 de "Seguridad de los Servicios de Red", y A13.1.3 de "Separación en las Redes" según la norma NTC/ISO/IEC 27002:2013.

La política de seguridad acerca del uso de redes y de servicios tiene los siguientes especificaciones:

Pregunta	Si	No	N/A	Observaciones
¿Se establecen responsabilidades y procedimientos para la gestión de equipos de redes?		3		Se establecen responsabilidades, pero no procedimientos.
¿Se separa la responsabilidad operacional por las redes, de las operaciones de cómputo?		4		No se incluye el desarrollo de los procedimientos apropiados para la red.
¿Existen controles para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre las redes inalámbricas?		5		No existen controles para salvaguardar los servicios de S.I. en la red.
¿Existen controles para proteger los sistemas y aplicaciones conectados?		4		No existen controles
¿Se cuenta con controles especiales para mantener la disponibilidad de los servicios de red y computadores		4		No existen controles

conectados?				
¿Se cuenta con un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información?		5		No existe este tipo de control ya que no se monitorean los Servicios de red.
¿Se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información?		5		No se coordinan este tipo de actividades por parte de la gerencia de la empresa.
Los sistemas en la red, ¿se autentican?	2			
¿Se restringe la conexión a dispositivos no autorizados a los sistemas a la red?		3		No hay administración de los dispositivos conectados a la red.
¿Existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red?		3		No existe este tipo de tecnología para cifrar datos sensibles.
¿Existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red?		4		No existen controles para asegurar la conexión segura a la red.
¿Existen procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red?		3		No existen estos procedimientos.
¿La red se encuentra dividida en dominios de red separados?		5		La red no se encuentra dividida.
¿Se permite el acceso entre dominios de redes controlando el acceso utilizando firewalls o enrutado de filtrado?				No aplican, porque la red no esta segmentada.
¿Las redes inalámbricas (redes externas) se encuentran separadas a las redes internas?				No aplican, porque la red no esta segmentada.
¿Se emplean mecanismos de autenticación, criptografía y tecnologías				

de control de accesos de redes entre las redes?				No aplica porque la red no está segmentada.
TOTALES	2	48		
PUNTAJE TOTAL	50			

Anexo G – Pruebas de Penetración: Nmap_equiposSubred

186.116.250.1	186.116.250.65	186.116.250.133	186.116.250.203
186.116.250.2	186.116.250.66	186.116.250.134	186.116.250.206
186.116.250.4	186.116.250.67	186.116.250.136	186.116.250.207
186.116.250.5	186.116.250.68	186.116.250.138	186.116.250.208
186.116.250.6	186.116.250.69	186.116.250.139	186.116.250.209
186.116.250.7	186.116.250.70	186.116.250.140	186.116.250.211
186.116.250.9	186.116.250.72	186.116.250.141	186.116.250.213
186.116.250.10	186.116.250.73	186.116.250.142	186.116.250.214
186.116.250.11	186.116.250.74	186.116.250.143	186.116.250.216
186.116.250.12	186.116.250.75	186.116.250.145	186.116.250.217
186.116.250.13	186.116.250.76	186.116.250.147	186.116.250.218
186.116.250.14	186.116.250.77	186.116.250.149	186.116.250.219
186.116.250.15	186.116.250.79	186.116.250.150	186.116.250.221
186.116.250.16	186.116.250.82	186.116.250.151	186.116.250.222
186.116.250.17	186.116.250.83	186.116.250.152	186.116.250.224
186.116.250.18	186.116.250.85	186.116.250.154	186.116.250.225
186.116.250.19	186.116.250.88	186.116.250.155	186.116.250.226
186.116.250.20	186.116.250.89	186.116.250.157	186.116.250.228
186.116.250.21	186.116.250.90	186.116.250.160	186.116.250.230
186.116.250.22	186.116.250.91	186.116.250.161	186.116.250.232
186.116.250.23	186.116.250.92	186.116.250.162	186.116.250.233
186.116.250.24	186.116.250.93	186.116.250.163	186.116.250.234
186.116.250.25	186.116.250.95	186.116.250.165	186.116.250.235
186.116.250.26	186.116.250.99	186.116.250.167	186.116.250.236
186.116.250.27	186.116.250.100	186.116.250.168	186.116.250.237
186.116.250.28	186.116.250.101	186.116.250.169	186.116.250.238
186.116.250.29	186.116.250.103	186.116.250.170	186.116.250.240
186.116.250.30	186.116.250.104	186.116.250.171	186.116.250.242
186.116.250.31	186.116.250.105	186.116.250.172	186.116.250.243
186.116.250.32	186.116.250.107	186.116.250.173	186.116.250.244
186.116.250.33	186.116.250.108	186.116.250.174	186.116.250.245
186.116.250.35	186.116.250.109	186.116.250.175	186.116.250.246
186.116.250.36	186.116.250.110	186.116.250.177	186.116.250.247
186.116.250.38	186.116.250.111	186.116.250.178	186.116.250.248
186.116.250.39	186.116.250.112	186.116.250.180	186.116.250.249
186.116.250.41	186.116.250.113	186.116.250.181	186.116.250.250
186.116.250.42	186.116.250.114	186.116.250.182	186.116.250.251
186.116.250.43	186.116.250.115	186.116.250.183	186.116.250.252
186.116.250.45	186.116.250.116	186.116.250.185	186.116.250.254
186.116.250.50	186.116.250.117	186.116.250.186	
186.116.250.51	186.116.250.118	186.116.250.187	

186.116.250.52	186.116.250.119	186.116.250.188	
186.116.250.53	186.116.250.120	186.116.250.189	
186.116.250.54	186.116.250.122	186.116.250.190	
186.116.250.55	186.116.250.123	186.116.250.191	
186.116.250.56	186.116.250.125	186.116.250.196	
186.116.250.58	186.116.250.127	186.116.250.197	
186.116.250.59	186.116.250.128	186.116.250.198	
186.116.250.61	186.116.250.129	186.116.250.199	
186.116.250.62	186.116.250.130	186.116.250.200	
186.116.250.63	186.116.250.131	186.116.250.201	
186.116.250.64	186.116.250.132	186.116.250.202	

Anexo H – Guías de Hallazgos: AP-GH-001

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-001

Guía de Hallazgos	
Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Riesgo	R001 - No existen procedimientos de autorización para determinar a quién se permiten acceder a las redes y servicios de red.

Descripción del Hallazgo
No se han establecido controles para establecer la autorización del ingreso al área de red, donde se encuentra el equipo de red distribuido, con lo cual, cualquier funcionario de la empresa Panavias S.A. tiene acceso a esta. El área de sistemas está encargada por un solo funcionario, este tiene acceso a los servicios de red los cuales previamente se encuentran configurados.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 6 **(Riesgo Medio)** Causas: La gerencia no ha establecido controles de acceso al área de red donde únicamente pueda acceder el usuario encargado o usuarios autorizados. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización [E.25] Pérdida de equipos [E.28] Indisponibilidad del personal **[A] Ataques deliberados** [A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.25] Robo de equipos
[A.28] Indisponibilidad del personal
[A.30] Ingeniería social

Recomendaciones – Acciones Correctivas

En el manual de políticas de seguridad de la información, en donde se definen las políticas de seguridad de la información en el recurso humano y responsabilidades, se debe definir quién o quiénes son los funcionarios autorizados para el ingreso al área de red, como la administración de los servicios mismos. Además, también se debe definir en la política de control de acceso, un control que mencione los niveles de acceso a los sistemas y servicio de red que deberían tener los usuarios en la empresa Panavias S.A.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-002

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-002

Guía de Hallazgos	
Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Riesgo	R002 - No existen controles y procedimientos de gestión para proteger el acceso a red y a los servicios de red.

Descripción del Hallazgo
No se han establecido controles para para proteger el ingreso al área de red, en su parte física donde se encuentra el equipo de red distribuido, como también en su parte lógica, ya que en esta última, mucho de los servicios de red no se encuentran protegidos, como por ejemplo los servicios de red en el host (puertos abiertos y servicios vulnerables), como en la red local de la empresa con el software Helysa GW.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 6 **(Riesgo Medio)** Causas: el encargado del área de la red de datos no ha establecido procedimientos para proteger el acceso a la red y los servicios de red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso

[A.11] Acceso no autorizado
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.28] Indisponibilidad del personal

Recomendaciones – Acciones Correctivas

Se recomienda utilizar tanto controles de acceso físico a la oficina asesora de comunicaciones y sistemas, como controles de acceso lógico a la red de la empresa Panavias S.A.

1. Controles de acceso físico: controles para restringir el acceso físico a los equipos, servidores, rack de comunicaciones, etc, entre los cuales se puede encontrar:

- Aseguramiento del edificio: asegurar las puertas de acceso al área de red con llave o tarjeta.
- Cámaras de seguridad: monitoreo del área de red a través de cámaras de seguridad.
- Candados de computadoras: utilizar medios especiales para asegurar el equipo de cómputo y de red como lo son candados con llave MicroSaver y candados de combinación portátiles MicroSaver.

2. Controles de acceso lógico: controles para restringir el acceso lógico a los servicios de red. Se podría considerar las siguientes herramientas:

- OpenNAC: permite gestionar el control de acceso de red a entornos LAN/WAN corporativas. Permite la autenticación, autorización y auditoria basadas en las políticas de acceso a red.
- Otras herramientas para administrar la gestión del control de acceso a la red son IpVoid, SPICEWORKS, zANTI, Fing.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad lógica de la red de datos
- Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.
- Pruebas de penetración a la red con nmap

- Pruebas de penetración a la red para identificar vulnerabilidades con Nessus y UpGuard.

Anexo H – Guías de Hallazgos: AP-GH-003

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-003

Guía de Hallazgos	
Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Riesgo	R003 - No existen medios usados para acceder a las redes y servicios de red como el uso de VPN.

Descripción del Hallazgo
No se han implementado medios para acceder a la red y a los servicios de red como lo son el uso de redes virtuales privadas (VPN) el cual ofrece un acceso seguro de los dispositivos de cómputo y de red.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 9 **(Riesgo Alto)** Causas: el encargado del área de la red de datos no ha establecido procedimientos para establecer accesos seguros a la red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia

[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio

Recomendaciones – Acciones Correctivas

Se recomienda utilizar medios de seguridad perimetral como es el uso de redes virtuales privadas (VPN). Esto podría presentar una ventaja para la organización ya que permite crear una capa extra de seguridad dentro de la red local para proteger los activos de información, como lo es el uso del software Helysa GW, donde se almacena la gran mayoría de los activos de información de la empresa. Además, que la red VPN se basa en el “”protocolo túnel”, el cual cifra los datos que se transmiten dentro de la red privada.

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red de datos
- Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-004

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-004

Guía de Hallazgos	
Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.1.2. Control de Acceso a las Redes y Servicios Asociados
Riesgo	R004 - No existe monitoreo del uso de los servicios de red.

Descripción del Hallazgo
No existe un monitoreo acerca del uso de los servicios de red, el cual permita establecer un seguimiento de la actividad de la red de la empresa. No existen herramientas que permitan el mapeo de redes, revisar el tráfico de red y también el uso de herramientas aplicadas a los servicios de red como el uso activo de protocolos criptográficos para el cifrado de la información.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: No se han establecido controles para realizar el registro de la actividad de la red en la empresa. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.7] Deficiencias en la organización [E.24] Caída del sistema por agotamiento de recursos **[A] Ataques deliberados** [A.8] Difusión de software dañino

[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio

Recomendaciones – Acciones Correctivas

El administrador de red es el encargado de gestionar y controlar los servicios de red que permitan el correcto funcionamiento de la infraestructura telemática. Además, está a cargo de implementar medidas de protección adecuadas, supervisar los registros y actividades que permitan salvaguardar la red tanto en su parte física, como lógica. También implementar herramientas que permitan gestionar y controlar todos los procesos de los servicios de red, como lo son:

4. Herramientas para el mapeo de redes: permiten identificar y gestionar los procesos y servicios de la red y subredes. La herramienta más utilizada para escaneo de redes es Nmap.

5. Herramientas para el escaneo de vulnerabilidades en la red: permiten identificar y explotar vulnerabilidades presentes en la red, esto después de un proceso de pentesting o Auditoria de Seguridad Informática a la red. Existen muchas herramientas, entre las más conocidas se encuentran OWASP-ZAP, Nessus, UpGuard, OpenVAS, Maltego, etc.

6. Herramientas para administrar el tráfico de la red: permiten administrar los paquetes de red y observar (sniffing) lo que está circulando por ella. La herramienta más conocida para tráfico de red es Wireshark.

7. Herramientas para monitorización de la red: permiten una gestión total de los procesos y servicios de red; para llevar registro y prevenir fallas en esta.

Entre las herramientas más conocidas se encuentran Solarwinds, Pandora FMS, Zenoss, Microsoft Network Monitor, etc
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red de datos - Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013. - Pruebas de penetración con UpGuard y Nessus donde se identifican que los protocolos para cifrado de la información están inactivos.

Anexo H – Guías de Hallazgos: AP-GH-005

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-005

Guía de Hallazgos	
Dominio/Proceso	A9. CONTROL DE ACCESO
Subdominio	A9.4.1. Restricción de Acceso a la Información
Riesgo	R005 - No existen controles de acceso físico o lógico para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes.

Descripción del Hallazgo
No existen controles para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación y redes. No se han establecido controles para asegurar los servicios de seguridad informática en los sistemas de información y redes.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles de acceso físico o lógico para asegurar los servicios de seguridad informática dentro de la empresa. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.7] Deficiencias en la organización [E.14] Fugas de información [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información

[E.18] Destrucción de la información
[E.19] Divulgación de información

[A] Ataques deliberados
[A.4] Manipulación de la configuración
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información

Recomendaciones – Acciones Correctivas

En el manual de políticas de seguridad de la información, en donde se definen las políticas de control de acceso, se debe definir un control de claves y nombres de usuario, donde se debe declarar el uso de contraseñas seguras y el cambio periódica de estas, tanto para el acceso de los servicios de red, entre ellos el software Helysa GW, en el cual se almacenan la mayoría delos activos de información de la empresa como también para el ingreso de los equipos de cómputo, con el objetivo de fortalecer la integridad de la información de la empresa.

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red de datos
- Lista de chequeo para verificar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A9. Control de Accesos según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-006

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-006

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R006 - No se establecen procedimientos para la gestión de equipos de redes. No existe inventario de los equipos de red.

Descripción del Hallazgo
No existen procedimientos para gestionar adecuadamente el equipo de red en la empresa Panavias S.A. La utilización de los equipos de red no es idónea, ya que se encuentra mal distribuido, por ejemplo el rack donde los switches no poseen un orden y el cableado no se encuentra etiquetado como también el servidor no se encuentra en el área de red. Además, de no existir un inventario sobre los dispositivos de red. El mantenimiento del equipo de la red no se realiza periódicamente y no se hace dentro de la empresa, lo hace el proveedor.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles para la utilización y gestión de los equipos de red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[I] De origen industrial** [I.8] Fallo de servicios de comunicaciones [I.10] Degradación de los soportes de almacenamiento de la información **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios

[E.2] Errores del administrador
[E.7] Deficiencias en la organización

Recomendaciones – Acciones Correctivas

Implementar controles en cuanto a la gestión de los equipos de redes, como lo son:

- Ordenar el equipo de red, como lo son servidores, switches, routers, cableado, en un armario metálico o rack de comunicaciones.
- El servidor principal se debe encontrar ya sea dentro del rack de comunicaciones o en la oficina de comunicaciones y sistemas de la empresa.
- El cableado debe estar debidamente etiquetado.
- Elaborar un inventario con los activos informáticos de red, tanto en su parte física, como lógica.
- Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-007

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-007

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R007 - No se incluye el desarrollo de los procedimientos de operación apropiados para la red.

Descripción del Hallazgo
No se establece el desarrollo de procedimientos de operación apropiados para la red como lo son el establecimiento de manuales de instrucciones apropiadas de operación y procedimientos de respuesta ante fallas de la infraestructura de red y la implementación de manuales de políticas de seguridad de la información en la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles en cuanto a la creación de de manuales de procedimientos y de políticas de seguridad para la red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.24] Caída del sistema por agotamiento de recursos [E.28] Indisponibilidad del personal

Recomendaciones – Acciones Correctivas

3. Elaborar e implementar un manual de políticas de seguridad de la información para el área de sistemas y comunicaciones de la empresa Panavias S.A. que contenga:
 	
- Políticas de seguridad de la información.
  - Objetivos de la organización.
  - Alcance.
  - Definiciones.
- Políticas de seguridad de la información en el recurso humano y responsabilidades
- Políticas de control de accesos.
  - Categorías y niveles de acceso
  - Control de claves y nombres de usuario
- Políticas de seguridad para la administración de sistemas y comunicaciones
  - Políticas de uso de programas dentro de la empresa.
  - Políticas de uso de los dispositivos dentro de la empresa.
  - Políticas de uso de los puntos de red de datos.
  - Políticas de seguridad para el centro de datos y del centro del cableado.
  - Políticas sobre copias de seguridad.
- Políticas de seguridad física y del entorno.
  - Políticas de seguridad de los equipos.
 	
4. Elaborar e implementar un manual de procedimientos y operaciones para la red de datos de la empresa, que contenga:
 	
- Objetivos de la empresa
- Alcance
- Responsabilidades y funciones
- Inventario y valoración de los elementos de red (físico y lógico)
- Controles de acceso de usuarios
- Herramientas de gestión de la red (herramientas para mapeo de redes, control de tráfico y monitorización de la red)
- Plan de respaldo en caso de incidentes

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A. donde se identificó que no se ha establecido o implementado un manual de procedimientos para la red ante posibles incidentes.
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-008

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-008

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R008 - No existen controles para salvaguardar los servicios de seguridad informática en la red.

Descripción del Hallazgo
No se han implementado controles de seguridad informática para salvaguardar la confidencialidad, la disponibilidad y la integridad de los activos de información e informáticos en la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles para salvaguardar los servicios de seguridad informática en la red de datos de la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.7] Deficiencias en la organización [E.14] Fugas de información [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información [E.18] Destrucción de la información [E.19] Divulgación de información

[A] Ataques deliberados

[A.4] Manipulación de la configuración
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información

Recomendaciones – Acciones Correctivas

Establecer controles para salvaguardar los servicios de seguridad informática en la red, como lo son:

1. Controles de disponibilidad:
- Monitorización de la red.
- Mantenimiento físico y lógico de los elementos y servicios de la red.
- Utilizar un sistema de alimentación ininterrumpida en caso de un fallo eléctrico que afecte la disponibilidad de los servicios de red.
- Hardening (Aseguramiento) de telecomunicaciones y de los equipos de computo

2. Controles de confidencialidad
- Controles de acceso a los servicios de red
- Encriptación
- Uso de cortafuegos o firewalls corporativos
- IDS- sistemas detectores de intrusos e IPS
- Sistemas PROXY y controles de ancho de banda

3. Controles de integridad
- Realización de copias de seguridad o de respaldo
- Uso de firmas electrónicas o certificado digital
- Sistemas antimalware (antivirus y/o antispam)

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red de datos
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-009

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-009

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R009 - No existen controles para proteger los sistemas y aplicaciones conectados.

Descripción del Hallazgo
No se han implementado controles de seguridad informática para proteger los sistemas de red, como la red local y el host; y aplicaciones de la empresa, como lo es el software Helysa GW, ante un incidente o ataque informático, ya sea interno o externo.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles para proteger los sistemas de red y aplicaciones en la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización **[A] Ataques deliberados** [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación de información [A.16] Introducción de falsa información

[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.26] Ataque destructivo
[A.30] Ingeniería social

Recomendaciones – Acciones Correctivas

Se recomienda hacer uso de Sistemas de Seguridad Perimetrales para proteger los sistemas de red y aplicaciones en la empresa como son los siguientes:

- Uso de cortafuegos o firewalls corporativos.
- IDS- Sistemas detectores de intrusos e IPS.
- Controles de contenidos (Listas negras y blancas).
- Sistemas PROXY y controles de ancho de banda.
- Implementación de infraestructuras PKI.
- Criptografía, Esteganografía y Certificados Digitales.
- Implementación de redes VPN cliente-servidor y sitio a sitio.
- Sistemas STORAGE-NAS, para almacenamiento masivo de datos
- Sistemas HONEYPOT (Sistemas trampa para intrusos informáticos)
- Sistemas Antimalware (Antivirus / Anti-SPAM)
- Hardening (Aseguramiento) de telecomunicaciones de micro y macro cómputo.

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red de datos
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Pruebas de penetración con nmap para identificar vulnerabilidades en la red y los servicios de red.

Anexo H – Guías de Hallazgos: AP-GH-010

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-010

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R010 - No existen controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.

Descripción del Hallazgo
No se han implementado controles para mantener la disponibilidad de los servicios de red, aplicaciones y computadoras conectadas a la red ante una falla eléctrica o de algún otro tipo que puede atentar con el correcto funcionamiento de la infraestructura de la red en la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: La gerencia no ha establecido controles especiales para mantener la disponibilidad de los servicios de red, aplicaciones y computadoras conectadas a la red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[I] De origen industrial** [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización [E.24] Caída del sistema por agotamiento de recursos

Recomendaciones – Acciones Correctivas
Se recomienda el uso de un Sistema de Alimentación Ininterrumpida (UPS) en caso de un apagón eléctrico, el cual puede proporcionar energía para que la infraestructura de red y de cómputo pueda seguir funcionando y así no afectar su disponibilidad. Otra ventaja de estos sistemas es filtra las subidas y bajadas de tensión que llega a la carga eléctrica, evitando así un cortos en el flujo eléctrico en la empresa.
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad física de la red de datos - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-011

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-011

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R011 - No existe un registro (logging) y seguimiento adecuados para posibilitar el registro y detección de las acciones que pueden afectar, o son pertinentes a la seguridad la información en la red.

Descripción del Hallazgo
No existe un registro de todos los accesos a la red para realizar un seguimiento que permitan detectar acciones que pueden atentar con los servicios de seguridad informática en la red de datos de la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: No se han establecido procedimientos para realizar seguimientos de todos los accesos a la red de la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.3] Errores de monitorización (log) [E.4] Errores de configuración **[A] Ataques deliberados** [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado

Recomendaciones – Acciones Correctivas
- Realizar un registro de todos los accesos (logged) para producir un rastro de referencia (Reference trail). Esto con el objetivo de realizar un seguimiento de los registros de todos los accesos tanto internos o externos relacionados con la red y los servicios de red, como por ejemplo el software Helysa GW, en la empresa. - Implementar IDS, sistemas detectores de intruso, para detectar acciones que puedan afectar la red y los servicios de red en la empresa.
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red de datos - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-012

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-012

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R012 - No se coordinan actividades de gestión para optimizar el servicio de la organización, como asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información.

Descripción del Hallazgo
No se coordinan actividades para asegurar los servicios de seguridad informática de la red ya que la gerencia no ha establecido estos procedimientos. No se han establecido estos controles ya que documentación referente a manual de procedimiento para la red y los sistemas informáticos ante incidentes y políticas de seguridad de la información, no se ha implementado.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: No se han establecido actividades de gestión ya que no se ha implementado procedimientos y políticas de seguridad informática en la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios [E.2] Errores del administrador [E.7] Deficiencias en la organización

Recomendaciones – Acciones Correctivas
En primer lugar se debe implementar la documentación correspondiente a manual de políticas y manual de procedimientos, con el objetivo de realizar un seguimiento periódico al cumplimiento de estos controles. Las revisiones de estos controles, debe realizarse a manera de auditorías internas en la empresa, con el objetivo de verificar que estos procedimientos se cumplan y se puedan medir. Las políticas y controles ayudaran a la empresa a planificar, desarrollar e implementar soluciones respecto a su infraestructura tecnológica, como también garantizar los servicios de seguridad informática de los activos informáticos y de información.
Evidencias del Hallazgo
- Visitas técnicas a la empresa Panavias S.A. donde se solicitó información referente a manuales y políticas de seguridad de la red y se identificó que esta documentación no existía. - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-013

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-013

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.1. Controles de Redes
Riesgo	R013 - No se restringe la conexión a dispositivos no autorizados a los sistemas a la red.

Descripción del Hallazgo
No existen controles para administrar los dispositivos permitidos conectados a la red de la empresa como lo son registros de los dispositivos permitidos conectados, registro de dispositivos invitados, alarmas contra intrusos que intenten ingresar a la red y bloqueo de estos.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 9 **(Riesgo Alto)** Causas: No se han establecido procedimientos para restringir la conexión a dispositivos no autorizados a la red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.14] Fugas de información [E.15] Alteración de la información **[A] Ataques deliberados** [A.4] Manipulación de la configuración [E.8] Difusión de software dañino [A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.30] Ingeniería social

Recomendaciones – Acciones Correctivas

Se debe crear un registro de todos los equipos y dispositivos que son permitidos, conectados a la red de datos de la empresa Panavias S.A. Este registro debe estar debe contener los siguientes parámetros:

- Nombre del dispositivo (hostname)
- Área de la empresa que pertenece
- Tipo de dispositivo
- Dirección IP
- Dirección MAC
- Características del equipo conectado (marca, sistema operativo, disco duro, etc)

Herramientas que se pueden utilizar para la gestión de dispositivos conectados a una red son IpVoid, PAGLO, SPICEWORKS, BGP Monitor, NTA, zANTI, Fing. Entre los servicios que disponen estar herramientas es la de escanear puertos y servicios, trazar la topología de enrutamiento de los equipos, periodo de actividad de los dispositivos en la red, bloquear los dispositivos no autorizados, etc.

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red.
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Prueba a redes inalámbricas con JumpStart donde se logró ingresar a la red local de la empresa.

Anexo H – Guías de Hallazgos: AP-GH-014

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-014

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.2. Seguridad de los Servicios de Red
Riesgo	R014 - No existe tecnología aplicada a la seguridad de servicios de red, tales como autenticación, criptografía y/o controles de conexión de red.

Descripción del Hallazgo
Los controles de autenticación a la red son limitados y no existen controles para la conexión segura a la red. Los protocolos criptográficos, los cuales existen en el host de la empresa, se encuentran inactivos y no se han implementado técnicas de cifrado para la gestión de los activos de información del software Helysa GW.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 6 **(Riesgo Medio)** Causas: la tecnología aplicada en cuanto a autenticación, conexión segura a la red y criptografía es limitada en la empresa. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.4] Errores de configuración **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.14] Interceptación de información

[A.15] Modificación de información [A.16] Introducción de falsa información [A.19] Divulgación de información
Recomendaciones – Acciones Correctivas
Se recomienda activar los protocolos criptográficos en el host, en caso de que se realicen transacciones o intercambio de información sensible online por medio de su servicio web como lo son por ejemplo, transacciones de pagos, autenticación de usuarios en la página, manejo de cuentas y facturas, intercambio de información con organizaciones externas. En el caso de la red local, donde se opera con el software Helysa GW, que es el cual contiene la mayoría de los activos de información de la empresa, es preciso cambiar de proveedor que ofrezca un protocolo criptográfico más seguro, ya que el actual usa Telnet, y este servicio no se recomienda para los sistemas modernos desde su punto de vista de seguridad por ser muy vulnerable.
Evidencias del Hallazgo
- Entrevista para evaluar la seguridad lógica de la red. - Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013. - Pruebas de penetración con UpGuard y Nessus donde se identifican que los protocolos para cifrado de la información están inactivos.

Anexo H – Guías de Hallazgos: AP-GH-015

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-015

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.2. Seguridad de los Servicios de Red
Riesgo	R015 - No existen controles para asegurar la conexión segura a la red.

Descripción del Hallazgo
No existen parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad en la red de datos de la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 9 **(Riesgo Alto)** Causas: no se ha implementado controles que permitan asegurar la conexión segura a la red de datos de la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.4] Errores de configuración **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.12] Análisis de tráfico [A.13] Repudio [A.11] Acceso no autorizado

[A.14] Interceptación de información
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.19] Divulgación de información
[A.30] Ingeniería social

Recomendaciones – Acciones Correctivas

Se recomienda implementar controles que permitan asegurar la conexión segura a la red de datos de la empresa, como lo son:

- Usar métodos de seguridad de red inalámbrica, como por ejemplo WPA2 y no utilizar la opción WPS.
- Cambiar las contraseñas de red periódicamente.
- Cambiar el identificador de red (SSID) periódicamente.
- Utilización de redes VPN.
- Utilización de cortafuegos o firewalls corporativos.
- Utilización de sistemas PROXY.
- Configuración de Autenticación por niveles de red.

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red.
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Prueba a redes inalámbricas con JumpStart donde se logró ingresar a la red local de la empresa.

Anexo H – Guías de Hallazgos: AP-GH-016

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-016

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.2. Seguridad de los Servicios de Red
Riesgo	R016 - No existen procedimientos del uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red.

Descripción del Hallazgo
No existen procedimientos para el acceso a los servicios de red, como lo son los servicios del host y la red local de la empresa, como de las aplicaciones de administración de información usadas, en este caso, el software Helysa GW, son mínimos.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 9 **(Riesgo Alto)** Causas: no se han establecido procedimientos seguros para restringir el acceso a los servicios o aplicaciones de red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.2] Errores del administrador [E.4] Errores de configuración [E.7] Deficiencias en la organización **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado

[A.14] Interceptación de información
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.19] Divulgación de información

Recomendaciones – Acciones Correctivas

En el manual de políticas de seguridad de la información, en donde se definen las políticas de control de acceso, se debe definir un control de claves y nombres de usuario, donde se debe declarar que el acceso a la información de la red y los servicios de red de la empresa, debe estar controlado. Corresponde a la oficina asesora de Comunicaciones y Sistemas, elaborar, mantener y publicar los documentos de servicios de red y procedimientos de administración de cuentas de usuario para el uso de servicios de red que ofrece la empresa Panavias S.A

Evidencias del Hallazgo

- Entrevista para evaluar la seguridad lógica de la red.
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Prueba de penetración con nmap donde se identifican los servicios de red activos.
- Prueba de penetración con OWASP-ZAP donde se identifican el acceso a algunos servicios de red.

Anexo H – Guías de Hallazgos: AP-GH-017

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-017

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	A13.1.3. Separación en las Redes
Riesgo	R017 - La red se no se encuentra dividida en dominios de red separados o segmentada.

Descripción del Hallazgo
La red de la empresa Panavias S.A. no se encuentra dividida en nodos separados o segmentada, lo cual permita aumentar el número de equipos conectados a ella y la mejora en la disponibilidad y rendimiento de la misma.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: no se ha dividido o segmentado la red de la empresa Panavias S.A. en nodos separados. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de información

Recomendaciones – Acciones Correctivas

Se recomienda segmentar la red la empresa, con el objetivo de que al dividir la red en segmentos, aumenta su rendimiento y disponibilidad, esto para el caso de la red de la empresa que contiene muchos equipos y dispositivos conectados. Se podría segmentar la red en tres dominios o subredes distribuidos de la siguiente manera:

1. Red de tres Dominio/Subredes:

- Dominio/Subred 1: Gerencia (oficina de gerencia, sala de conferencias, oficina de comunicaciones y sistemas)
- Dominio/Subred 2: Administración 1 (oficinas de control interno, jurídica, planeación y contabilidad)
- Dominio/Subred 3: Administración 2 (oficina administrativa, despacho)

La segmentación de redes se realiza cuando se sobrepasa el número de equipos y/o dispositivos registrados que una topología permite y para mejorar el tráfico de la red. Para la segmentación de red se pueden utilizar hubs, repetidores, bridges, routers, gateways.

Evidencias del Hallazgo

- Visitas técnicas a la red donde se realiza una entrevista previa con el encargado para conocer las características de la red de la empresa.
- Entrevista para evaluar la seguridad física de la red.
- Lista de chequeo para verificar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A13. Seguridad en las Telecomunicaciones según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-018

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-018

Guía de Hallazgos	
Dominio/Proceso	A13. SEGURIDAD EN LAS TELECOMUNICACIONES
Subdominio	
Riesgo	R018 - Vulnerabilidad por puertos sensibles abiertos y expuestos.

Descripción del Hallazgo
Tras el escaneo de red para identificar vulnerabilidades en la red local y el host de la empresa Panavias S.A., se muestra múltiples puertos sensibles expuestos que corren riesgo de ser explotados. También de información expuesta en algunos de ellos, como en el caso del host, donde se encontró datos encriptados que pueden corresponder a usuarios o contraseñas.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 16 **(Riesgo Alto)** Causas: no se ha establecido controles para la seguridad de los servicios de red como es el caso de vulnerabilidad por puertos abiertos con riesgo a ser explotados. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[E] Errores y fallos no intencionados** [E.4] Errores de configuración [E.14] Fugas de información [E.20] Vulnerabilidades de los programas (software) **[A] Ataques deliberados** [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso
[A.15] Modificación de información
[A.17] Corrupción de la información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.30] Ingeniería social

Recomendaciones – Acciones Correctivas

Durante la ejecución de pruebas de penetración, se encontró puertos con información sensible que pueden ser explotados, tanto en la dirección del host como de la red local. En el host, se muestran puertos abiertos de riesgo como lo son:

- Puerto 21, servicio FTP
- Puerto 26, servicio SMTP
- Puerto 110, servicio POP3
- Puerto 143, servicio IMAP
- Puerto 443, servicio ssl/http
- Puerto 587, servicio smtp
- Puerto 993, servicio ssl/imap
- Puerto 3306, servicio mysql

Se recomienda cerrar los puertos a aquellos servicios de red que no se estén utilizando, además de la configuración de un firewall para los servicios del host.

En el caso de la red local, se muestran puertos que se encuentran filtrados, con presencia de firewall configurado por defecto, pero este no resulta muy eficaz. Se recomienda configurar un firewall corporativo para gestionar los servicios de la red local de la empresa como lo es el software Helysa GW.

Evidencias del Hallazgo

- Prueba de penetración con nmap para identificar vulnerabilidades en la red y realizar acciones de escaneo de servicios, subred y fingerprinting.
- Prueba de penetración con zenmap para recolectar información en el enrutamiento y la ejecución de scripts de nmap para recolocar información sensible en los puertos abiertos.
- Pruebas de penetración con UpGuard y Nessus para identificar y analizar vulnerabilidades en la red.

Anexo H – Guías de Hallazgos: AP-GH-019

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-019

Guía de Hallazgos	
Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.1. Ubicación y Protección de los Equipos
Riesgo	R019 - Las instalaciones de procesamiento de información y de redes no están ubicadas cuidadosamente para reducir el riesgo de que las personas no autorizadas puedan acceder a ellas

Descripción del Hallazgo
El área de red está encargada por un solo funcionario, pero no existen controles de acceso físico o lógico y cualquier funcionario de la empresa puede ingresar. La ubicación del equipo de red no es idónea, ya que se encuentra mal distribuido, por ejemplo el rack donde los switches no poseen un orden y el cableado no se encuentra etiquetado como también el servidor no se encuentra en el área de red, este se encuentra en la oficina financiera.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: No se han establecido procedimientos para la ubicación de los equipos de red en la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[I] De origen industrial** [I.8] Fallo de servicios de comunicaciones [I.10] Degradación de los soportes de almacenamiento de la información **[E] Errores y fallos no intencionados** [E.1] Errores de los usuarios

[E.2] Errores del administrador
[E.7] Deficiencias en la organización
[E] Errores y fallos no intencionados
[E.25] Pérdida de equipos

[A] Ataques deliberados
[A.25] Robo de equipos

Recomendaciones – Acciones Correctivas

Se recomienda establecer los siguientes controles:

- Establecer responsabilidades sobre quien tiene acceso al área de red y los equipos de red.
- Ordenar en el equipo de red en el área que corresponde. Se debe ordenar en un armario metálico o rack de comunicaciones con cada uno de sus elementos registrados en un inventario y su cableado debidamente etiquetado.
- Implementar controles en cuanto a la gestión de red que permita monitorizar, controlar, planificar y coordinar los equipos y servicios de red dentro de la empresa Panavias S.A.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-020

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-020

Guía de Hallazgos	
Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.1. Ubicación y Protección de los Equipos
Riesgo	R020 - No se han adoptado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales como robo, incendio, explosivos, humo, agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo

Descripción del Hallazgo
No se han implementado controles para minimizar el riesgo de amenazas físicas y ambientales potenciales. Existen cámaras de vigilancia y alarmas contra incendio, pero estas no abarcan toda la empresa, por lo que son vulnerables. No se han realizado actividades para mitigar riesgos de origen natural o industrial.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 8 **(Riesgo Alto)** Causas: No se han establecido controles para minimizar riesgos de amenazas físicas, ambientales y de origen industrial. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[N] Desastres naturales** [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales **[I] De origen industrial**

[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información

[A] Ataques deliberados
[A.25] Robo de equipos

Recomendaciones – Acciones Correctivas

Se recomienda utilizar cámaras de vigilancia para cada una de las áreas de la empresa para prevenir el posible robo de equipos. También, implementar las alarmas contra incendio en cada área de la empresa para prevenir posibles incendios o expansión de humo de este en caso de una eventualidad.

Realizar revisiones periódicas, evaluar y controlar permanentemente la seguridad física para minimizar riesgos de amenazas físicas, ambientales y de origen industrial que se puedan presentar dentro de la empresa.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.
- Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-021

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-021

Guía de Hallazgos	
Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.1. Ubicación y Protección de los Equipos
Riesgo	R021 - El seguimiento y mantenimiento de las de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información e instalación de redes no lo realiza el personal encargado de la misma empresa.

Descripción del Hallazgo
El seguimiento lo hace la empresa proveedora, pero no lo realiza periódicamente. Se realiza en un plazo de máximo entre una o dos veces al año. Es preciso que esto se gestione con el personal de la misma empresa, estableciendo responsabilidades al encargado del área de la oficina de comunicaciones y sistemas de la empresa Panavias S.A. para el mantenimiento y seguimiento de las condiciones ambientales que puedan afectar las operaciones o las instalaciones de cómputo y de red.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 8 **(Riesgo Alto)** Causas: No se han establecido controles para el mantenimiento y seguimiento de las condiciones ambientales que puedan afectar las operaciones o las instalaciones de cómputo y de red. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[N] Desastres naturales**

[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

[I] De origen industrial
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información

[E] Errores y fallos no intencionados
[E.7] Deficiencias en la organización

Recomendaciones – Acciones Correctivas

En el manual de políticas de seguridad de la información, en donde se definen las políticas de seguridad de la información en el recurso humano y responsabilidades, se debe definir, como parte de las obligaciones del encargado de la oficina asesora de comunicaciones y sistemas de la empresa, funciones que tienen que ver con el mantenimiento y seguimiento de las condiciones ambientales que puedan afectar las operaciones o las instalaciones de cómputo y de red. Estas deben ser revisadas periódicamente para prevenir cualquier eventualidad que puedan afectar la infraestructura de la empresa.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.
  Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Anexo H – Guías de Hallazgos: AP-GH-022

PANAVIAS INGENIERIA & CONSTRUCCIONES NIT. 891.201.840 - 6	**AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIAS S.A.**	UNAD Universidad Nacional Abierta y a Distancia Versión 1.0. Ref. AP-GH-022

Guía de Hallazgos	
Dominio/Proceso	A11. SEGURIDAD FISICA Y DEL ENTORNO
Subdominio	A11.2.3. Seguridad del Cableado
Riesgo	R022 - Las líneas de telecomunicaciones que entran a las instalaciones de procesamiento de información no cuentan con protección alternativa.

Descripción del Hallazgo
El cableado UTP de cobre no cuenta con protección de blindaje y es vulnerable a interferencias. El cableado no posee ordenamiento ni etiquetado. No existen procedimientos contra interceptación daños al cableado de telecomunicaciones que transporta los datos o brinda soporte a los servicios de información de la empresa Panavias S.A.
Riesgo – Nivel de Riesgo (Causas / Efectos)
Evaluación del riesgo = 12 **(Riesgo Alto)** Causas: No se han establecido controles para la seguridad del cableado de telecomunicaciones de la empresa Panavias S.A. Efectos: De acuerdo a Magerit V3, se podrían presentar las siguientes posibles amenazas: **[I] De origen industrial** [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios o suministros esenciales **[E] Errores y fallos no intencionados** [E.7] Deficiencias en la organización
Recomendaciones – Acciones Correctivas

Se recomienda realizar las siguientes acciones para la seguridad del cableado UTP:

4. En primer lugar, cambiar de empresa proveedora, ya que la actual utiliza cableado de cobre (UTP categoría 3), es preciso cambiar a cable de patch cord de fibra óptica para obtener mejoras en el rendimiento y disponibilidad de la red.

5. Si se mantiene con cableado de cobre, debe cumplir con especificaciones como:

- Cableado UTP blindado de categoría 6.
- Conductores de cobre solido de calibre entre 22 y 26 AWG.
- Utilizar forro PVC.
- El etiquetado del cableado debe contener: nombre del fabricante, tipo de cable, numero de pares, tipo y número de listado.

6. Si se cambia a cable patch cord de fibra óptica, se recomienda que este deba tener las siguientes especificaciones:

- Deben ser probados para soportar velocidades hasta de 10 GB.
- Debe ser compatible con todos los sistemas de cómputo y de red.
- Debe ser cableado certificado para generar un desempeño óptimo de su función.
- El cableado debe tener retardante de fuego y recubrimiento tipo Tight Buffer.

Evidencias del Hallazgo

- Visitas técnicas al área de red de la empresa Panavias S.A.
- Entrevista para evaluar la seguridad física de la red de datos
- Lista de chequeo para verificar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.
  Cuestionario de control para evaluar los controles dominio A11. Seguridad Física y del Entorno según la normatividad ISO/IEC 27002:2013.

Resumen Analítico Educativo (RAE)

Título de Documento.	Auditoría a la Seguridad de la Red de Datos de la empresa Panavias S.A.
Autor	Cortes Camacho, Jesus Germán
Palabras Claves	Auditoría, Información, Pruebas de penetración, Seguridad informática, Control, Riesgo, Amenaza, Vulnerabilidad

Descripción

El presente proyecto aplicado, tiene como finalidad realizar una auditoría de seguridad a la red de datos de la empresa Panavias S.A. en la ciudad de San Juan de Pasto el cual tiene por objetivo formular controles y procedimientos con el fin de establecer un sistema de gestión adecuado, identificando vulnerabilidades y amenazas por medio de pruebas de penetración y los procesos de auditoria de sistemas.

Fuentes Bibliográficas	CÓDIGO PENAL. Ley 1273 de 2009 De la Protección de la Información y de los Datos. Colombia, 2009. Ministerio de la Información y las Comunicaciones de Colombia. MAGERIT Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II Catálogo de Elementos. Ministerio de Hacienda y Administraciones Públicas. España, 2012. NTC-ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. NTC-ISO-IEC 27002:2013. Tecnología de la Información. Técnicas de Seguridad. Código de Practica para Controles de Seguridad de la Información. SOLARTE, Nicolás Javier. GUSTIN LOPEZ, Enith. HERNANDEZ, Ricardo Javier. Manual de Procedimientos para llevar a la Práctica la Auditoria Informática. San Juan de Pasto, Colombia. 2012.

	TAPIADOR, Ángeles Sanz. Controles y Auditoria en Redes de Datos. Guía Práctica. Escuela Politécnica Superior. Facultad de Ingeniería Técnica en Informática de Gestión. Madrid, España. 2010. VARGAS AVILES, Julio Rito. Conceptos sobre Auditoria Informática. Colombia, 2009. Universidad Nacional de ingeniería. Facultad de Ingeniería de Sistemas. Departamento de Ingeniería. NORMA ISO/IEC 27000. Portal ISO 27000 en Español [en línea]. [Consultado el 26 de Agosto de 2016]. Disponible en: <http://www.iso27000.es/>

Contenido:

Planteamiento del Problema

El problema general que se presenta en la empresa PANAVIAS S.A. es que no existe una adecuada segmentación de la red lo que está generando problemas de confidencialidad de la información que se maneja en las diferentes dependencias ya que todos los usuarios están en una sola red, lo que permite el acceso a los servicios y datos privados de la organización.

Otro de los problemas en la empresa PANAVIAS S.A. es que no cuenta con el personal para la administración de la red de datos, existe personal de sistemas pero no un administrador de red que opere los servicios que están configurados en ella.

En la actualidad, la empresa Panavias S.A. posee desconocimiento del estado de seguridad de la red de datos ya que a lo largo de su historia nunca se han realizado auditorias de seguridad informática.

Tampoco existen políticas y procedimientos de seguridad o sistemas de control informático que ayuden a mitigar las vulnerabilidades y amenazas que se podrían presentar.

Objetivo General

Desarrollar una auditoría a la seguridad de la red de datos que permita diseñar un sistema de gestión de seguridad informático que contenga los controles y procedimientos para la red en la empresa Panavias S.A.

Objetivos Específicos

- Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la empresa Panavias S.A. para verificar la existencia de las vulnerabilidades y amenazas existentes en los activos informáticos y de información.

- Seleccionar la norma que se va a aplicar, dominios, diseñar los instrumentos de recolección de información y pruebas aplicables a la red de datos de la empresa Panavias S.A.

- Aplicar los instrumentos diseñados y ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a seguridad de la red de datos de la empresa Panavias S.A.

- Elaborar un informe de los resultados obtenidos en la auditoria que contenga los hallazgos y recomendaciones para el diseño del SGSI que contenga los controles que permitan mitigarlos.

Metodología

La metodología se realizara de acuerdo a las fases de la auditoria de sistemas que son en relación a los cuatro objetivos específicos del proyecto.

- Etapa 1: Fase de Reconocimiento.
- Etapa 2: Fase de Planeación
- Etapa 3: Fase de Ejecución
- Etapa 4: Fase de Resultados

Conclusiones

La auditoría a la seguridad de la red de datos en la empresa Panavias S.A.,

finalizo cumpliendo cada una de las fases propuestas.

Se ejecutaron los instrumentos necesarios para identificar las vulnerabilidades existentes en la red de datos de la empresa Panavias S.A.

Determinar los riesgos informáticos a los cuales está expuesto la red de la empresa Panavias S.A., permitió establecer los procedimientos necesarios para garantizar los niveles de confidencialidad, integridad y disponibilidad de la información.

Las recomendaciones de seguridad formuladas para la red de la empresa Panavias S.A., permitirán implantar nuevos controles para proteger y mantener la seguridad de la información que actualmente se maneja en el área de sistemas.

Recomendaciones.

Se recomienda hacer uso e implementar los controles propuestos en las guías de hallazgos como también en la declaración de aplicabilidad.

Se debería elaborar e implementar un manual de políticas de seguridad de la información en la empresa Panavias S.A. que contenga la gestión de los activos de información, los activos informáticos, respecto al equipo e cómputo y de red en la empresa y la delegación de responsabilidades para dichos activos y acciones.

Una vez implementada la documentación respectiva a las políticas de seguridad y el manual de procedimientos de la red de datos de la empresa Panavias S.A., se deben coordinar actividades de gestión, con el apoyo y aprobación de la gerencia de la empresa, para optimizar el servicio de red en la organización y que los controles se apliquen en forma coherente

El desarrollo de la presente auditoria, ayudara a la empresa Panavias S.A. a establecer un sistema de gestión de seguridad informático adecuado que le permita mitigar vulnerabilidades y amenazas presentes en su red de datos.