ANALISIS DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED EN COMPAÑIA MULTINACIONAL DEL SECTOR INDUSTRIAL

PRESENTADO POR:
JULIAN DAVID GUEVARA RIVERA
HASVERTH STIVEN TELLEZ CASTILLO

ASESOR TÉCNICO DE PROYECTO:
INGENIERO JOHN FREDY CHACON SANCHEZ

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
Julio 7 de 2020

RESUMEN

El objetivo principal de este trabajo es realizar un análisis de seguridad a los dispositivos de infraestructura de red principales y a un grupo de servidores que son de alto impacto en la Compañía Multinacional del Sector Industrial, la metodología propuesta consiste en realizar un levantamiento de información donde se determinara cuáles son los dispositivos de infraestructura tecnológica de mayor importancia con esta información se generó un análisis de vulnerabilidades, puertos y servicios versiones de firmware y sistemas operativos con la finalidad de encontrar brechas de seguridad. Con este levantamiento de información se generaron informes con los hallazgos y se entregaron una serie de recomendaciones y buenas prácticas para generar los controles y remediaciones necesarios para mejorar los estándares de seguridad de la compañía en busca de mejorar la confidencial, integridad y disponibilidad de la información.

PALABRAS CLAVE

Vulnerabilidad, seguridad, infraestructura, análisis, sistemas, servicios, información, evaluación, cumplimiento políticas.

ABSTRACT

The main objective of this work is to perform a security analysis to infrastructure devices of the principal network and a group of servers that represent a high impact in a multinational company of the industrial sector, the proposed methodology consists of carrying out an information survey where is determined the most important technological infrastructure devices. so with this information, a vulnerability analysis was made highlighting ports, services and firmware versions and operating systems in order to identify security breaches.

With this information gathering, reports were generated with the findings and a series of recommendations and good practices were delivered to generate the necessary controls and remediations to improve the company's security standards searching for the improvement of Information confidentiality, integrity and availability.

KEYWORDS

Vulnerability, security, infrastructure, analysis, systems, services, information, evaluation, policy compliance.

Tabla de contenido

Índice de Graficas

Índice de Diagramas

Índice de Tablas

1. Título

ANALISIS DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED EN COMPAÑIA MULTINACIONAL DEL SECTOR INDUSTRIAL

2. Introducción

El crecimiento tecnológico durante los últimos años ha evolucionado de manera significativa obligando a las empresas a estar a la vanguardia de los últimos avances en todos los campos de infraestructura tecnológica, es de vital importancia que el impulso tecnológico sea cultura en las diferentes áreas de las organizaciones y de esta forma apalancar los nuevos desarrollos e innovaciones en el mundo digital.

Apoyándose en las nuevas tendencias de seguridad y herramientas tecnológicas las empresas estarán en una constante evolución en sus estrategias de mercado siendo más flexible a los cambios y mejorando el desempeño tanto de su plataforma tecnológica como la productividad de su capital humano fortaleciendo todos los campos de acción de la organización.

Los nuevos enfoques en inteligencia de negocios y la analítica de datos generan un alto volumen de información que obliga a las organizaciones a implementar buenas prácticas y procedimientos que generen una cultura que priorice la protección de los datos.

La multinacional del sector industrial trata de mantenerse en constante evolución e innovación en el mercado digital, la empresa se apoya en sus diferentes áreas con el fin de impulsar su fuerza de ventas y su interacción digital por lo cual es de vital importancia la disponibilidad de sus sistemas de información, aplicaciones y en general su plataforma tecnológica.

El replanteamiento de las metodologías utilizadas se enfatiza en desaprender y aprender nuevas formas de abordar el uso de los sistemas proporcionados por la empresa maximizando sus prestaciones en pro de la compañía.

Las medidas de seguridad que posee actualmente no permiten garantizar una eficiencia del uso de los servicios prestados, en la actualidad se hace necesario el proteger y garantizar el flujo de información en la empresa adoptando normativas internacionales que permitan generar buenas prácticas a nivel de seguridad informática apoyando que la seguridad sea un pilar dentro

de la organización que necesita ser revisado y evaluado constantemente.

3. Descripción general del proyecto

El fin de este proyecto es generar a la compañía industrial textil un estudio de vulnerabilidades en seguridad de redes informáticas aplicando las mejores prácticas y algunas herramientas del mercado, que permitan obtener unos resultados que puedan generar una guía a sus políticas y normativas aplicables al desempeño óptimo de la red inalámbrica y cableada de la organización así como a la seguridad perimetral bajo los estándares de la seguridad informática en algunos controles que tiene la norma ISO 27001 v2013.

En primera instancia se plantea realizar un levantamiento de información que permita identificar el estado actual de la compañía y su funcionamiento en términos de seguridad informática, este será insumo para detectar las falencias que se tienen y sus efectos, de esta manera proponer una serie de recomendaciones y un plan de trabajo que pueda ayudar a la organización a mejorar su esquema actual de seguridad en redes telemáticas.

3.1 Definición del problema

La empresa de procedencia manufactura y textil de origen colombiano con más de 20 años de trayectoria en la industria textil en Latinoamérica está enfocada en crear artículos de calidad.

La operación se centra en el uso constante de su aplicación ERP, herramientas colaborativas las cuales demandan una alta disponibilidad y uso en la red del 99.99%; dentro de los dispositivos utilizados se cuentan con equipos de escritorio, equipos portátiles, equipos móviles, terminales inalámbricos, impresoras, plotters y otros dispositivos.

La empresa se encuentra en constante proyección y expansión debido a las exigencias de la industria orientada a la confección, alistamiento, ventas y distribución de artículos de forma presencial y a través de su portal Web. Viendo la necesidad de que se garantice la prestación de sus sistemas y canales de comunicación y la prestación de servicios para sus más de 1000 empleados distribuidos a nivel nacional y sus clientes; la compañía ve de vital importancia un análisis detallado de la seguridad de su infraestructura de red y telecomunicaciones con el fin de asegurar su desempeño y mejora continua.

La compañía ha implementado controles básicos de seguridad en redes; sin embargo, presenta la necesidad de identificar las brechas de seguridad de la información existentes y aplicar los controles necesarios que permitan entregar sus servicios con los mínimos estándares de calidad a sus clientes, esto debido también, a su constante proyección y expansión con la intención de mejorar su rendimiento y detener las interrupciones de servicio.

Debido a su constante crecimiento y expansión su fuerte se encuentra en sus puntos de ventas físicos y virtuales y los envíos de diferentes artículos de manufactura textil a nivel nacional. Cuenta con una planta de personal de aproximadamente 3000 empleados con 5 sedes administrativas y más de 100 puntos de venta a nivel nacional. La empresa exporta artículos finales e importa suministros y realiza comercio electrónico.

Dado el alto volumen de información que se maneja y la alta transaccionalidad de solicitudes, requieren una infraestructura tecnológica consolidada, la organización tiene diferentes áreas administrativas, técnicas y/o operativas de producción y desarrollo las cuales se encuentran en funcionamiento 7x24x365.

La dirección de tecnología cuenta con 6 ingenieros, quienes son responsables de realizar la administración de los servidores, bases de datos y sistemas de redes de comunicación además se cuenta con un grupo de desarrollo de aplicaciones de 5 personas y una mesa de ayuda de 20 personas las cuales son lideradas con un jefe de área y un gerente de tecnología.

A nivel de documentación, la dirección de tecnología, cuenta con información básica de la configuración de los equipos y los diagramas de la topología de red implementada en la organización.

Para la empresa es de vital importancia el resguardo de su información, abarcando los diseños de sus artículos, su estado financiero quienes, y como acceden a los mismos, y la alta disponibilidad de sus plataformas en la actualidad la compañía cuenta con una política estándar de roles y usuarios y algunos procesos del aseguramiento de la infraestructura de red de comunicaciones.

De esta manera, la norma ISO 27000 es el referente para garantizar la mejora, en términos de seguridad de la información, los aspectos débiles de la empresa puesto que establece los requisitos mínimos y los objetivos de control necesarios para la implementación de un Sistema de Gestión de Seguridad de la Información. El proyecto no está enfocado en la implementación del Sistema; sin embargo, se aplicarán distintos controles de seguridad atribuible a los procesos y sistemas de la organización.

La seguridad en las redes es de gran importancia en las organizaciones y se debe asumir de primera mano, en la actualidad en la compañía se han presentado evidencias de la falencia que se tienen en seguridad de su infraestructura de TI:

- Los usuarios pueden acceder desde los servidores de producción a otros servidores de pruebas y desarrollo.
- Se han presentado ataques de phishing.
- Encripción de discos duros.
- Al conectar un cable de red en cualquier punto de la red de la compañía se tiene acceso a internet y las redes corporativas de la empresa.
- Las personas traen sus equipos personales y se conectan a la red para usar los recursos de la empresa.
- Los usuarios que tienen asignadas VPN tienen acceso a todos los segmentos de la red corporativa.
- La administración de los equipos se encuentra descentralizada.
- Durante algunas horas del día se presenta lentitud en la red.
- Se ha detectado que varios usuarios utilizan el mismo usuario o clave de ingreso en los equipos

Conforme con la problemática asociada, se ha detectado una serie de causas que no han permitido mejorar la seguridad de la información, como:

- La conexión en los puntos físicos de la red no es controlada.
- Las políticas de seguridad definidas para dispositivos externos no son claras.
- El firewall cuenta con algunas reglas no agrupadas
- Algunos equipos se encuentran con sistemas operativos desactualizados
- Se evidencian conexiones de Hub que extendían la red
- Todas las Vlan se pueden ver y acceder entre ellas
- Existe gran variedad de equipos multimarca.
- Los usuarios pueden acceder a las redes inalámbricas con claves genéricas.

La compañía se encuentra expuesta a ataques cibernéticos bloqueos a nivel de internet y aplicaciones, accesos indebidos y fuga de información.

Lo anterior podría llegar a generar un bloqueo en el área de despacho de productos si se detiene el sistema y no se puede entregar a tiempo, esto ocasionaría gastos considerables acompañado de las multas que la empresa tendría que asumir por el incumplimiento de la entrega de productos, la detención de la banda de distribución puede generar tiempos de improductividad de 10 personas, adicional el gasto operativo que incurriría en tener una o varias personas sin realizar sus tareas diarias, en el caso de que se genere daño de los equipos de la infraestructura tecnológica se puede presentar fallas en el acceso a la información y perdida de la misma, también se está expuesto a la indisponibilidad de la plataforma web lo cual impactaría directamente las ventas.

3.2 Aspectos a solucionar

- La conexión en los puntos físicos de la red no es controlada
- Las políticas de seguridad definidas para dispositivos externos no son claras.
- Se tiene versiones de firmware y sistemas operativos desactualizados
- Se evidencian conexiones de Hub que extendían la red
- Existe gran variedad de equipos multimarca.
- Los usuarios pueden acceder a las diferentes redes inalámbricas con claves genéricas

3.3 Solución propuesta

Con el fin de mejorar y robustecer la seguridad de la infraestructura de red y telecomunicaciones de la compañía se propone realizar un levantamiento de información de dispositivos críticos de la infraestructura de red y servidores generando un análisis de estado de la seguridad utilizando herramientas de escaneo de puertos, servicios y vulnerabilidades obteniendo un insumo que nos permita entregar una serie de recomendaciones y buenas prácticas.

Se sugiere una estandarización de marca de dispositivos entendiendo que no puede ser inmediata que es un proceso a largo plazo ya que la inversión monetaria es alta esto permitirá un mejor control y administración de la infraestructura (este primer punto aplica de acuerdo a la Norma ISO 27000 al objetivo de control A.8.2.3 - Manejo de activos), es importante generar políticas de acceso a la red WLAN y LAN (de acuerdo al objetivo de control A.9.1.2 Accesos a Redes y a Servicios en Red de la ISO 27000) que ayuden con la seguridad de los accesos a la red, a sus vez la definición de roles permitirá la segmentación de permisos de usuarios de acuerdo a sus responsabilidades (de acuerdo a los objetivos de control A.9.2.1 y A.9.2.2 referente al control de acceso a usuarios) adicionalmente diseñar una propuesta de sistema de monitoreo de los dispositivos de red adecuado para la empresa que permita un control y visibilidad del estado de los servicios de red verificando el nivel de disponibilidad y respuesta de estos servicios.

4. Estado del arte

4.1 Marco de referencia teórico

Diferentes artículos y estudios previos sobre redes telemáticas, comunicaciones, seguridad y sistemas de información; Jesús Salinas en su escrito "Telemática y educación: expectativas y desafíos" ha descrito la importancia de la tecnología y su correcta aplicabilidad, reflejando que la tecnología apalanca y apoya el alto nivel de productividad en las diferentes áreas de la empresa, McKinsey & Company en su artículo "La ventaja de mover primero en la industria: Valor empresarial con fábricas digitales" afirma que los productores líderes en aplicar tecnologías digitales sacan provecho de su ventaja inicial generando aún más valor a nivel de toda la empresa.

Anteriormente se pensaba que la seguridad de nuestros equipos tecnológicos se basaba solo en contraseñas y protección de desastres naturales como fuego o inundaciones, pero a medida que evolucionaban las empresas confiaban su seguridad al sentido común de los usuarios para garantizar la seguridad de la organización. Durante la evolución de las tecnologías y su deseo por mejorar obligo a que las empresas se mantuvieran a la vanguardia, un factor determinante y motivante para generar tendencia hacia la ciberseguridad fue la necesidad de mitigar las amenazas hacia la información.

El desconocimiento de la importancia de la seguridad en los dispositivos o aplicaciones tecnológicas que utilizamos en nuestras empresas ocasionan vulnerabilidades evidentes para los atacantes, originando que se creen estándares a nivel mundial en temas de seguridad como la norma IEEE 802.x la cual se define como:

"IEEE 802 es un proyecto del Institute of Electrical and Electronics Engineers (más conocido por sus siglas, IEEE). Se identifica también con las siglas LMSC (LAN/MAN Standards Committee). Su misión se centra en desarrollar estándares de redes de área local (LAN) y redes de área metropolitana (MAN), principalmente en las dos capas inferiores del modelo OSI.1".

(wikipedia, s.f.)

Estos estándares y metodologías internacionales en seguridad nos proporcionan un marco de referencia basado en las mejores prácticas que se adaptan y complementan a cada organización dentro de las que podemos destacar:

- Instalar una solución de seguridad en los diferentes dispositivos como son pc, equipos de comunicaciones, servidores y dispositivos móviles.
- Actualizar los equipos de la infraestructura tecnológica con los últimos parches de seguridad de sistema operativo y aplicaciones.
- Borrado de cuentas de usuario innecesarias.
- Alto nivel de seguridad de las contraseñas.

- La realización de copias de seguridad periódicas de todos los dispositivos y sistemas de información.
- El control de las aplicaciones de los dispositivos móviles las cuales deben provenir de fuentes seguras.

De estos conceptos, metodologías y mejores prácticas nace el término de Ciberseguridad el cual se define como la Seguridad de la Información, la protección, confidencialidad, integridad y la disponibilidad de la información. Siendo esto el conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, acciones, formación y prácticas idóneas a nivel tecnológico que pueden utilizarse para proteger la información y los diferentes medios por donde se transmite.

Ventajas

- Aseguramiento de la integridad y privacidad de la información de un sistema informático y sus usuarios.
- Medidas de seguridad para evitar daños y problemas que pueden ocasionar los intrusos.
- Barreras de seguridad para que nuestras aplicaciones y dispositivos como: cortafuegos, antivirus, anti espías, encriptación de la información y uso de contraseñas, protejan la información y los equipos de los usuarios.
- Capacitar a los usuarios sobre las nuevas tecnologías y las amenazas que pueden traer el mal uso de los recursos de la compañía.
- Protección para sus equipos, teléfonos móviles y todo tipo de dispositivos tecnológicos.
- Sistema de Gestión de riesgo, que permite proteger nuestros equipos y organizaciones.

Desventajas

- La obsolescencia de los elementos tecnológicos que son perjudiciales para el medio ambiente.
- La seguridad absoluta no es posible.

- Los equipos desactualizados al instalar un antivirus realmente efectivo pueden ser muy pesado esto puede hacerlos más lento y ocupar mucho espacio en memoria.
- La creación de contraseñas es cada vez más compleja y el cambio de contraseñas con frecuencia se ha vuelto obligatorio.
- El costo elevado de los servicios de ciberseguridad hace que las empresas no inviertan en este campo.

Según la norma ISO 27002 la seguridad de la información es la protección de la información contra todo tipo de amenazas y poder asegurar la continuidad del negocio. Aunque la seguridad no es absoluta se necesita abarcar la seguridad en todos sus niveles (seguridad física y de entorno, seguridad lógica y seguridad de control)

Seguridad física comprende todo el entorno donde se encuentran alojados los equipos y software tecnológico, salas de cómputos, centros de cableado condiciones ambientales etc.

Seguridad lógica que comprende todo el aseguramiento y control del software y aplicaciones, el transporte de los datos a través de la red y todos los métodos de autenticación y autorización como contraseñas, biométricos, etc.

Seguridad de control la cual comprende mantener una capacitación del recurso humano, supervisar continuamente los controles de la seguridad física y lógica y corregir cualquier tipo de inconveniente referente a la seguridad informática y de la información en las organizaciones.

Estos niveles de seguridad nos permiten combatir todo tipo de ataque, amenazas, vulnerabilidades y riesgos los cuales se pueden dividir de la siguiente manera:

Una **VULNERABILIDAD** es una falla o debilidad en el sistema que pone en riesgo la seguridad de la información permitiendo ser atacada y comprometiendo su integridad,

confidencialidad o disponibilidad estas fallas suelen ser errores de configuración, diseño o implementación.

Una **AMENAZA** son las acciones que se aprovechan de las vulnerabilidades para atentar contra la seguridad de los sistemas de información teniendo un impacto negativo sobre nuestros sistemas un ejemplo de estas amenazas son ataques dirigidos, robos de información, virus, desastres naturales o mal manejo de las herramientas proporcionadas por la empresa a sus usuarios.

Un **RIESGO** es toda la probabilidad de que se produzca un incidente de seguridad que ocasione que una amenaza se materialice.

Las amenazas más comunes que pueden comprometer la seguridad en una empresa son:

- Factores humanos: errores de usuario accidental o dirigido.
- Falla en sistemas de información: errores de instalación, desarrollo o configuración.
- Desastres naturales: incendio, inundaciones o fallas en la infraestructura física.
- Malware, Virus informáticos o código malicioso que permiten a atacante ejecutar acciones sobre los equipos por ejemplo (botnets, spyware, malware, virus, troyanos, phishing, trashing).

- Uso no autorizado de Sistemas Informáticos.
- Robo de Información.
- Fraudes basados en el uso de computadores.
- Suplantación de identidad como lo es suplantar la dirección IP, el ARP o el DNS, páginas web o correo electrónico.
- Denegación de Servicios (DoS) el cual causa que el sistema o servicio no esté disponible.
- Ataques de Fuerza Bruta.
- Alteración de la Información.
- Divulgación de Información.
- Sabotaje, Vandalismo y Espionaje.
- Ingeniería social utilizada la persuasión y buena voluntad de los usuarios.
- APT o amenazas persistentes avanzadas las cuales son ataques dirigidos.
- Errores de programación o mal desarrollo de una aplicación.
- Uso no controlado de redes sociales que pueden poner en riesgo la reputación de la empresa.
- Accesos no autorizados a instalaciones.
- Incumplimiento de normas y políticas de seguridad.
- Fallas de comunicaciones, hardware o software.

La seguridad informática se va convirtiendo en algo necesario de implementar y no solo como un apoyo del área de TI sino una unidad de apoyo transversal en las organizaciones.

Guía de buenas Prácticas Recomendadas por Cisco nos permitirá identificar según el fabricante que recomendaciones debemos tener implementadas en nuestros dispositivos, en las opciones que nos ofrece estaría:

Operaciones de Seguridad. Guías de configuraciones y buenas prácticas para evitar la revelación involuntaria de información, mejorar el rendimiento de las redes, entender la seguridad operacional, lograr una configuración segura de direcciones IP o evaluar la seguridad de

proveedores de aplicaciones de servicio para las empresas.

Seguridad en Redes. Guías de configuración y buenas prácticas centradas en mejorar la seguridad de productos concretos de Cisco Systems, así como para hacerlos más resistentes a ataques, aplicar un descarte selectivo de paquetes o la creación de listas de control de acceso para la protección de infraestructuras.

Seguridad del Host. Técnicas de identificación de ataques y su mitigación para mejorar la seguridad de los hosts. Observación de actividad login en un Honeypot (técnica en la que se utiliza un ordenador o servidor como cebo para atraer a gestores de botnets que lo conviertan en zombie y posteriormente analizar y seguir la pista de su actividad), guía para diferenciar las modalidades de amenazas existentes (virus, gusanos, troyanos, bots, etc.) y cómo protegerse de forma efectiva frente a ellas.

Seguridad en Aplicaciones. Guías en seguridad, la telefonía por Internet y la encriptación de bases de datos para el desarrollo de aplicaciones. identificación y técnicas de mitigación de ataques, destacan la identificación y correlación de indicadores de ataque, buenas prácticas DNS, protección de redes e identificación de ataques a las mismas. entender la inyección SQL y los vectores de amenaza en el Cross-Site Scripting (XSS).

La aplicación de la norma ISO 27001 es un documento base para el desarrollo del proyecto el cual nos permitirá tener un horizonte de en el desarrollo del análisis e identificar que controles de seguridad debemos revisar esta norma nos permitirá

Utilizar métodos más ágiles: el compromiso con la certificación bajo la norma ISO 27001 dependiendo en gran medida del nivel de recursos y la gestión de un tiempo necesario. Simplificando y agilizando los procedimientos que usa un software sobre la gestión de la norma ISO 27001 para reducir la utilización de recursos innecesariamente, no sólo en la ejecución, sino también en marcha, gestión y presentación de informes.

Evitar utilizar plantillas de políticas de seguridad: cada empresa tiene su propio

perfil único y condiciones de seguridad individuales.

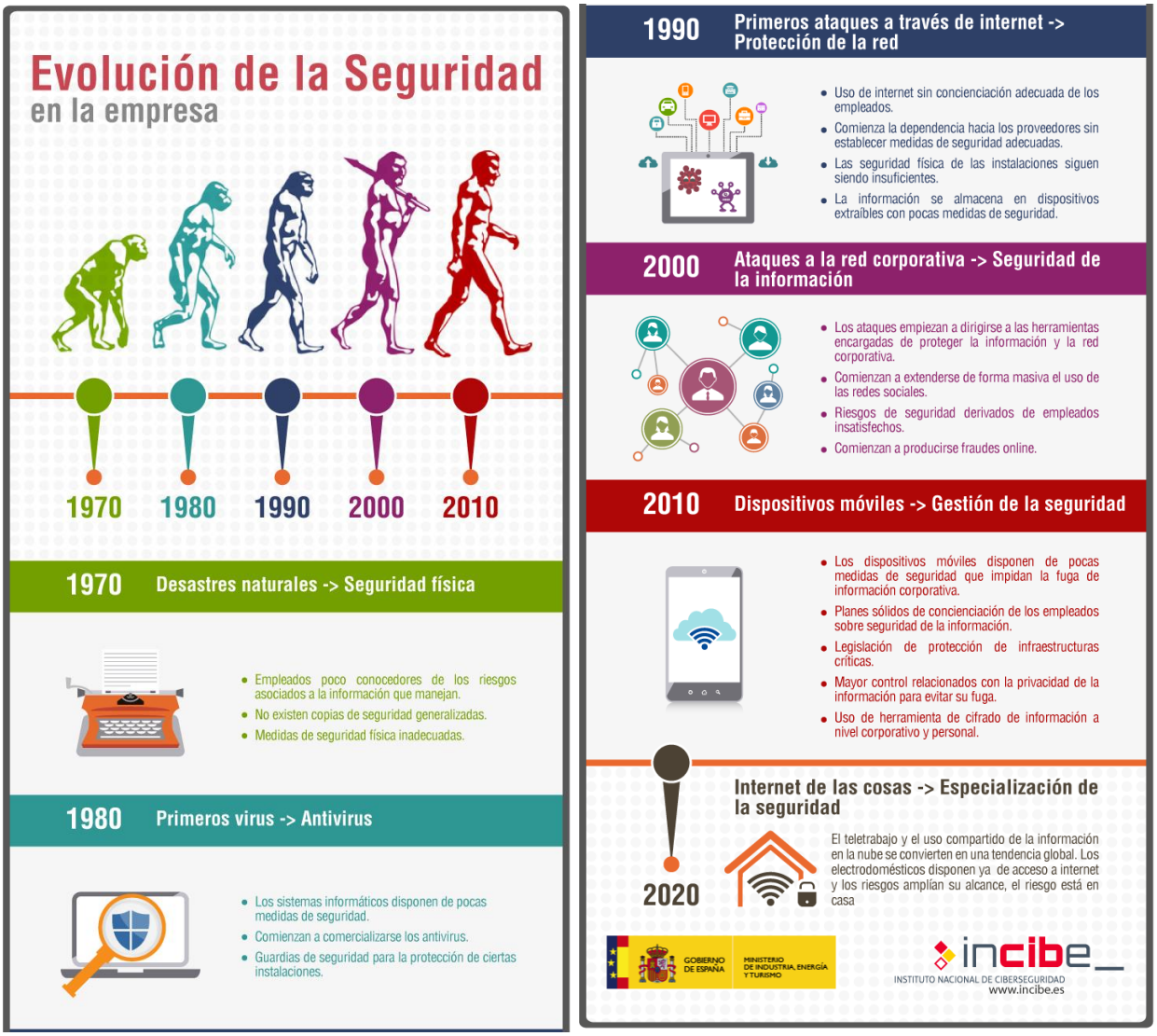
Saber utilizar el software para evaluar los riesgos: las plantillas de las políticas, existe un peligro en la utilización de la evaluación de otra persona de riesgo. El software es para simplificar y mejorar el proceso, lo que facilita la aplicación de un conjunto de criterios con los que asegurar todos los activos de información.

El Sistema de Gestión de Seguridad de la Información: la aplicación de la norma ISO 27001 adaptarse al panorama digital en constante cambio. con el conjunto correcto de herramientas que llega a su propio conjunto de políticas y procedimientos de gestión del riesgo asegurará que su Sistema de Gestión de Seguridad de la Información se convierte en una parte integrada e integral de sus procesos de la compañía.

Garantizar una comprensión de la seguridad de la información en toda la empresa: un Sistema de Gestión de Seguridad de la Información se basa en el conocimiento y aceptación de todos los partidos dentro de la empresa. Comunicar las políticas y controles que pueden ser fácilmente mantenidos y comunicados de forma pertinente, se asigna para el cumplimiento y la formación que puede ser evidenciado.

Crear una cultura de mejora continua: la norma ISO 27001 2013 es un estándar que incorpora el concepto de mejora continua, en la que se involucra todo el personal en el proceso para mejorar la seguridad de la información promoviendo el compromiso.

A continuación, se muestra una imagen de la evolución de la seguridad



Fuente www.Incibe.es

El monitoreo de los diferentes dispositivos de red es de gran importancia en las organizaciones el uso de una herramienta adecuada que nos permita tener una mayor visibilidad de la disponibilidad de la infraestructura y obtener un mayor control de los dispositivos es algo a lo cual se le debe apuntar, esto posibilita tener históricos y estadísticas que permitan generar

un seguimiento al comportamiento de los dispositivos.

Las herramientas de monitoreo se pueden obtener en el mercado teniendo en cuenta tres modelos de distribución: **software como servicio** (SaaS), **software de código** abierto y soluciones de código cerrado o soluciones **en propiedad** algunas de estas son:

SaaS

- Acronis Monitoring Service
- New Relic
- LogicMonitor

Código abierto

- Sensu
- Icinga
- Zabbix
- Nagios

En propiedad

- Paessler
- SolarWinds

4.2 Marco de referencia tecnológico

Herramientas de monitorización SaaS (software como servicio)

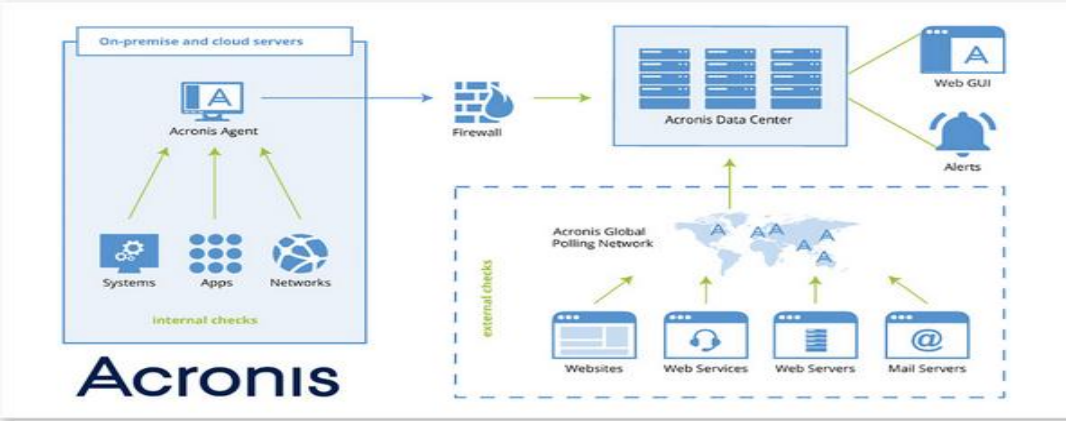
En este modelo de distribución, el cliente tiene acceso vía Internet al software de monitoreo, el cual está alojado en servidores de terceros (nube), mediante el pago de una suscripción al servicio. El modelo SaaS tiene muchos beneficios, tales como el ahorro, la escalabilidad, la accesibilidad, la productividad y rentabilidad. Con ello, las empresas dejan de invertir grandes cantidades de capital para instalar, mantener y actualizar infraestructura tecnológica y se puede llegar a pagar cantidades razonables para operaciones mediante suscripciones. De acuerdo al crecimiento de la empresa, se puede cambiar a la suscripción SaaS que más sea conveniente, esto permite añadir más capacidades y no tendrá que invertir en más

servidores o en mayores anchos de banda de red.

Su escalabilidad genera que sea factible para proveedores de servicios porque las suscripciones se pueden mejorar de acuerdo con el número de usuarios o sitios web, sin que por ello haya que adquirir más hardware u otros costosos recursos.

Un gran número de compañías están optando por herramientas de monitoreo basadas en SaaS combinándolas con otras herramientas complementarias de código abierto como Zabbix.

Acronis Monitoring Service

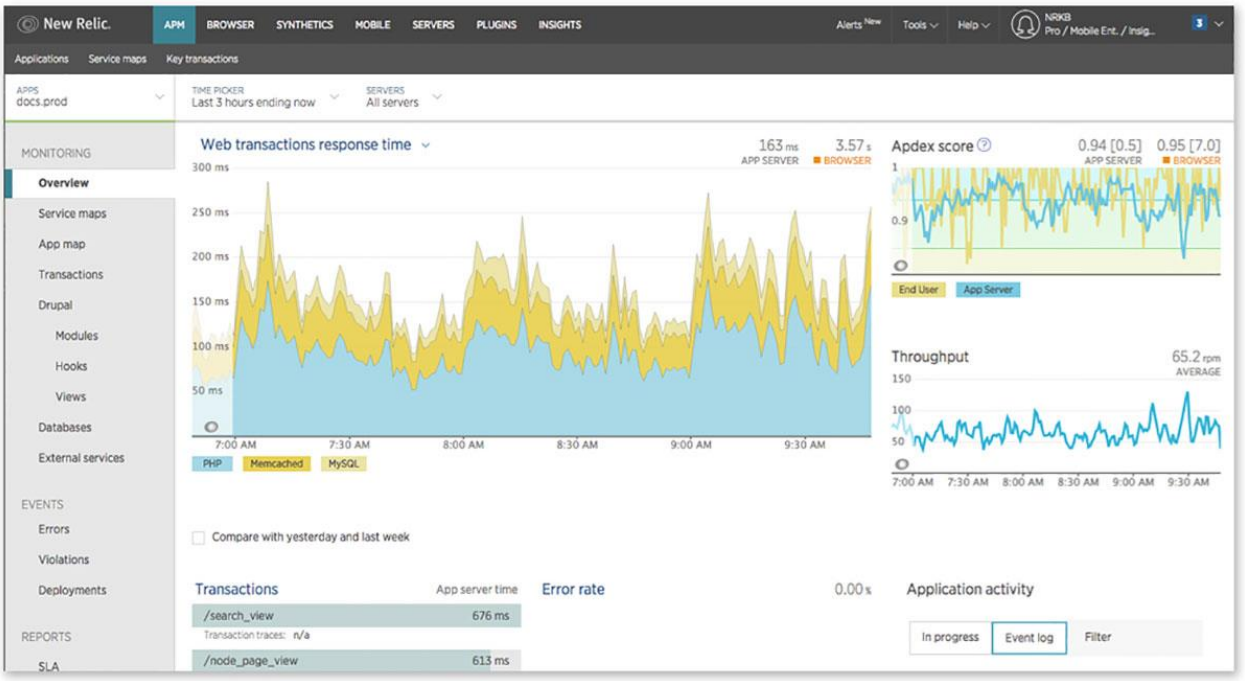


Precio: desde 200 usd al año

Es una solución que fácilmente puede ser implementada una herramienta de monitoreo de servidores on-premises y sistemas basados en IaaS.

Acronis Monitor Service es una aplicación con agentes a prueba de contratiempos, configuraciones basadas en GUI y una solución administrada para el uso inmediato y la disponibilidad para entornos pequeños y medianos brinda soporte para infraestructuras múltiples, vista única de panel de todos los activos digitales que permite asignación de responsabilidades. La herramienta tiene capacidad para monitorizar todos los elementos: redes, rendimiento de los servidores, sistemas operativos, aplicaciones, servicios y comprobaciones web sintéticas.

New Relic



Precio: Desde 80 usd mensuales.

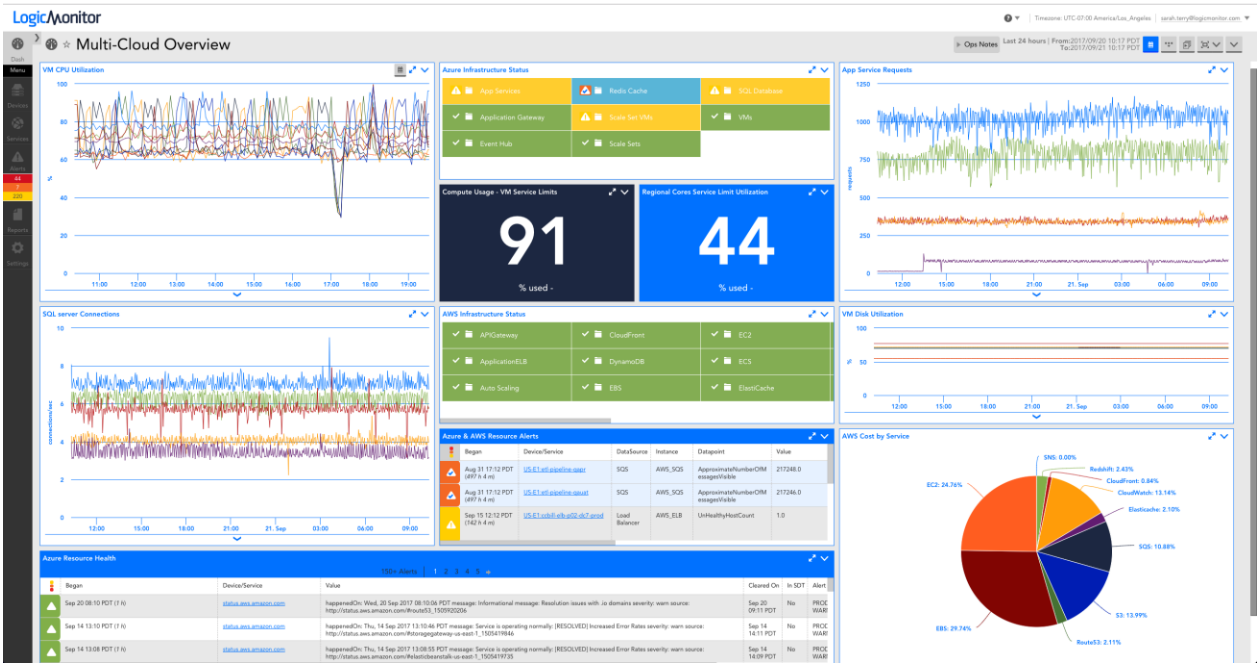
Es una solución de monitoreo exhaustivo de rendimiento, basada en SaaS, de aplicaciones para entornos en la nube e on-premises.

New Relic es una herramienta integral completa para la monitorización del rendimiento de las aplicaciones. Brinda una plataforma de análisis de software para pruebas sintéticas, monitoreo de usuarios reales y administración del rendimiento de las aplicaciones, para aplicaciones implementadas en centros de datos on premises y entornos de nube. Genera el monitoreo de una gran cantidad de parámetros, entre los que se incluyen servidor, aplicaciones, experiencia de usuario final al igual que el análisis de los datos monitoreados.

La herramienta APM posibilita la obtención parámetros detallados de rendimiento en tiempo real y dispone de la capacidad de detectar códigos lentos, errores y los sitios en los que

los usuarios están teniendo problemas. El agente de java de New Relic se puede utilizar para hacer recopilar y hacer seguimiento de los datos de rendimiento tales como problemas de rendimiento u otros errores dentro del código. El agente es compatible con tecnologías como Python, Java, .Net, Node.js y PHP.

LogicMonitor



Precio: desde 5000 usd anuales.

Es una solución de monitoreo basada en SaaS para infraestructuras de tamaños medio y grande. LogicMonitor recurre a un conjunto de recolectores basados en Java, o agentes de software, para monitorear una gran variedad de hardware de red y recursos de software. Es compatible con una gran cantidad de tecnologías que comúnmente se instalan en la red del cliente y así descubren los dispositivos de la red para luego reenviar los datos a la plataforma de procesamiento en la nube de LogicMonitor.

Esta herramienta maneja un potente portal que monitorea las capacidades, predicciones e informes que permite que los ingenieros de redes puedan hacer un seguimiento de la capacidad, actividad, disponibilidad, tráfico de la red, datos y transacciones de los usuarios y a su vez permitiendo crear informes personalizados.

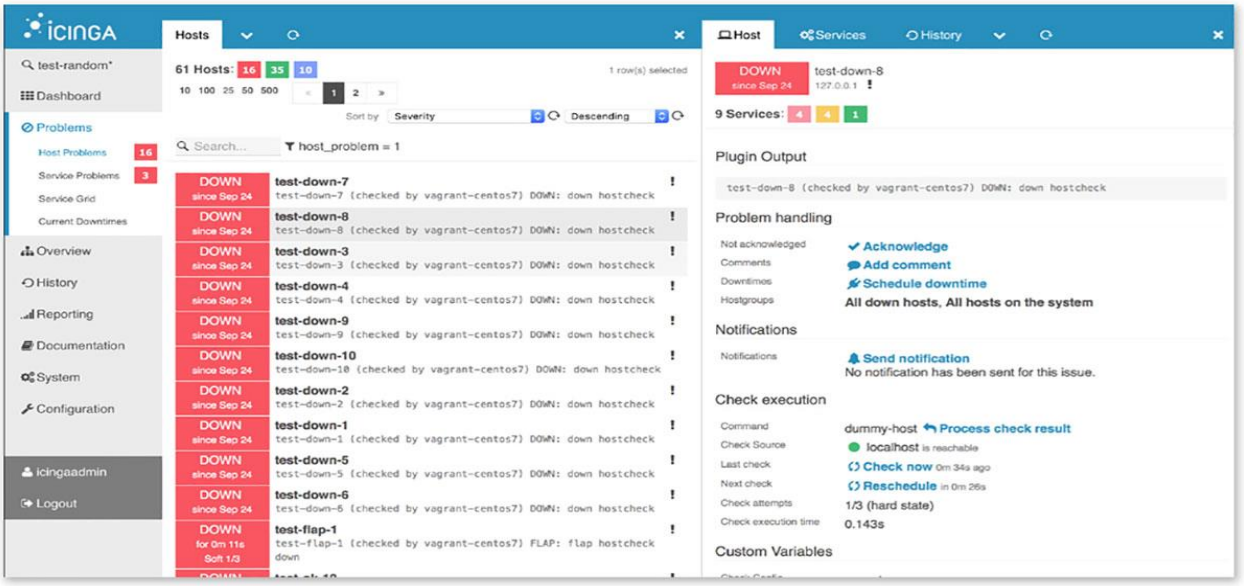
Herramientas de Monitoreo de Código Abierto

Las soluciones de monitoreo de código abierto no tienen costo y vienen con grandes opciones de personalización con lo que podemos adaptarlas a cualquier tipo de monitoreo. Sin embargo, algunas carecen de servicio técnico profesional y aquellas empresas que implementen estas soluciones deberán estar preparadas para capacitar a sus propios colaboradores o incurrir en costos con otros proveedores para los servicios de soporte.

En algunas ocasiones, la seguridad sigue siendo el punto débil, lo que lleva a algunos administradores de TIC a evitar este tipo de soluciones. Aun así, aquellas empresas le apuntan a la investigación y el autoaprendizaje pueden inclinarse por el código abierto.

Nagios y Zabbix son las herramientas de monitoreo de código abierto más utilizadas, con mayor recorrido y grado de madurez. Aunque también hay otras herramientas alternativas en crecimiento, como Sensu e Icinga.

Icinga

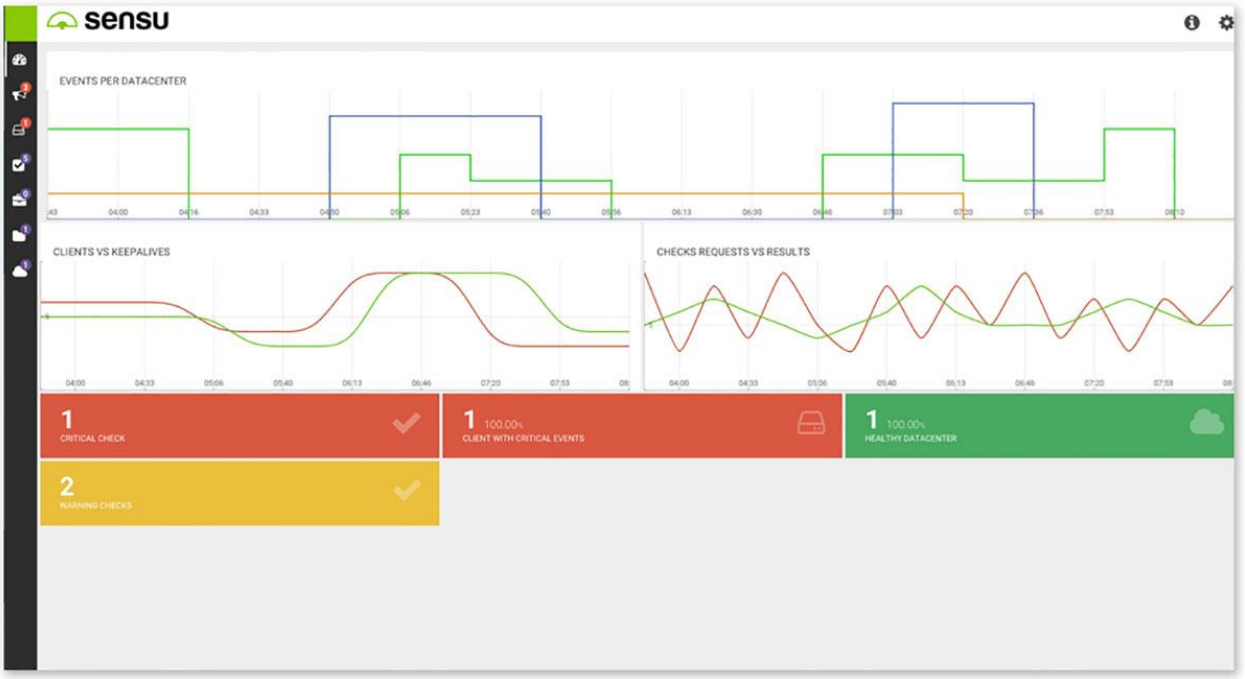


Precio: Gratis, versión paga desde 1995 USD

Icinga es una solución de código abierto escalable, que comprueba la disponibilidad de los servicios y recursos de red, genera datos de rendimiento e informa a los responsables acerca de interrupciones u otras incidencias. Esta herramienta que funciona en una amplia variedad de entornos, que van desde infraestructuras TIC medianas o pequeñas hasta otras muy complejas, tiene la capacidad de comprobar las redes, los componentes o los recursos en diferentes ubicaciones.

Icinga tiene una interfaz de usuario amigable, plantillas de configuración intuitivas, controladas por reglas de fácil aplicación, y en cuestión de minutos se instala y se puede comenzar a monitorear. Dispone de una gran cantidad de funciones y una interfaz de monitorización rápida y moderna.

Sensu

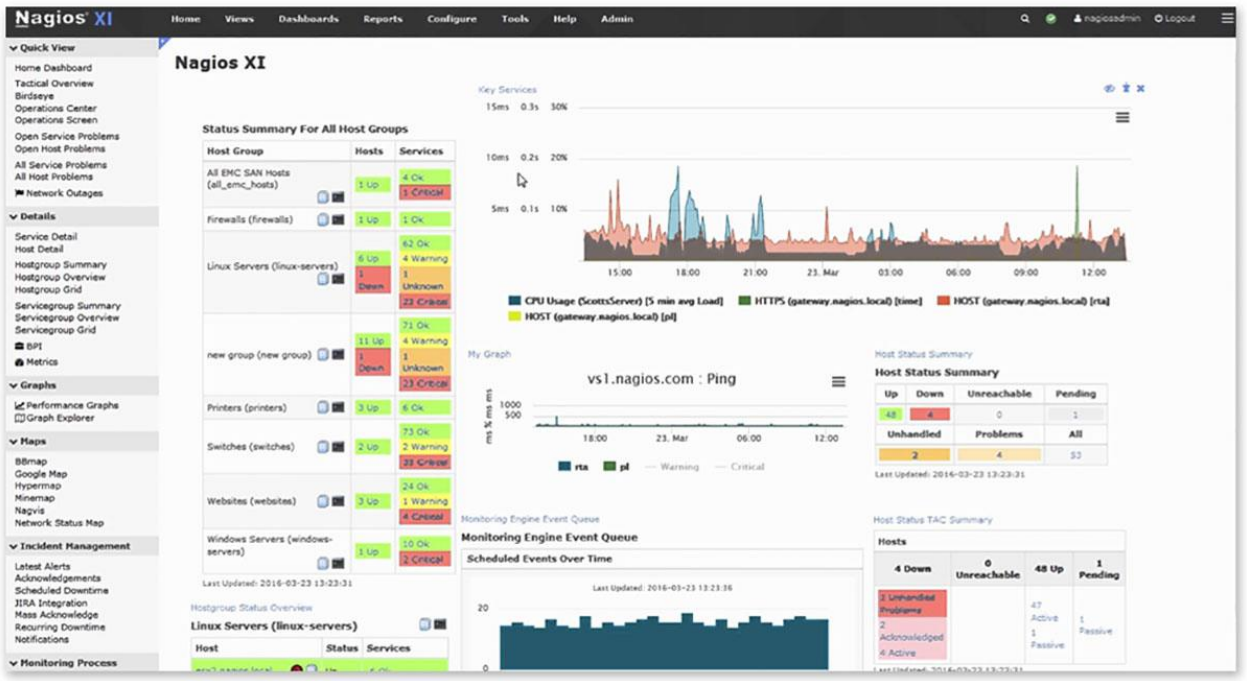


Precio: Gratis (Sensu Core), desde 60 dólares al mes (Sensu Enterprise)

Es una plataforma de monitoreo que puede utilizarse para monitorear servidores completos, virtuales y basados en nube, aplicaciones web, recursos de terceros y dispositivos de red como routers y switches.

La arquitectura de Sensu contiene un agente de monitoreo, procesador de eventos, almacenamiento de datos, transporte seguro y un programador de realización de comprobaciones, permite realizar comprobaciones de servicio, eventos de procesamiento y recopilar datos de parámetros a escala. El cliente cuenta con un conector TCP y UDP susceptible de recibir datos externos JSON, que permiten a las aplicaciones utilizar la interfaz para enviar datos de parámetros específicos de la aplicación o informar sobre errores a Sensu.

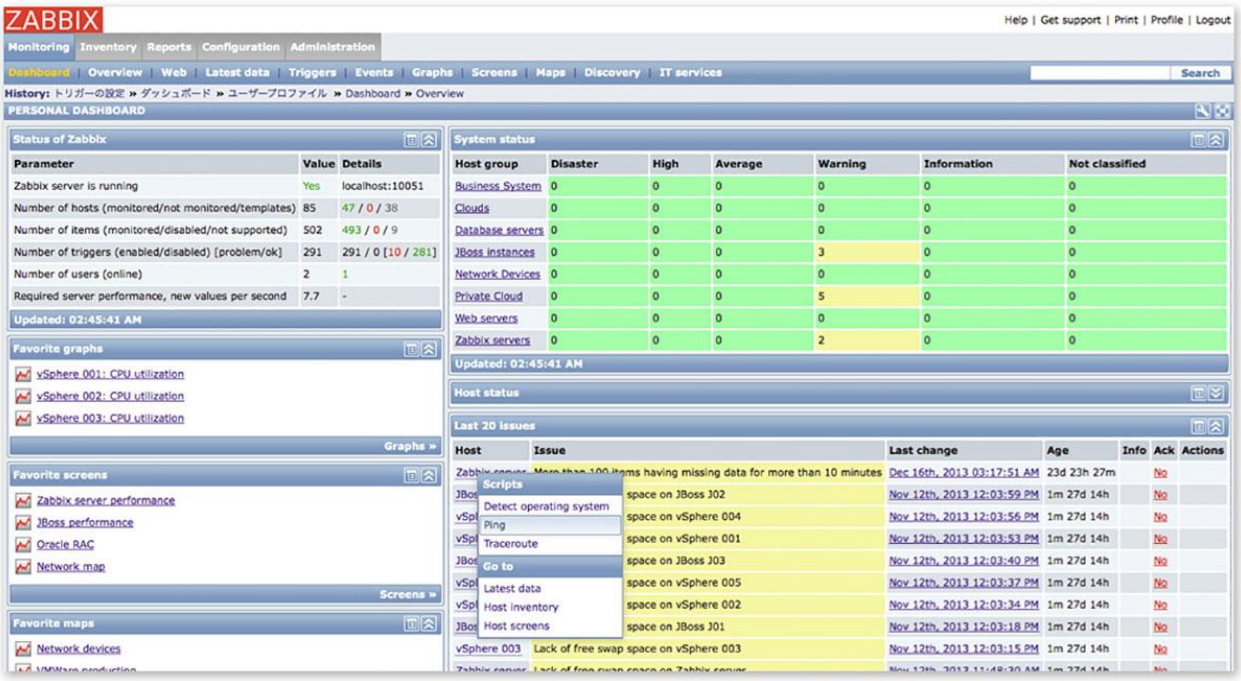
Nagios



Precio: gratis (Nagios Core), desde 2000 Usd (NagiosXL).

Nagios es un sistema de monitorización de redes altamente utilizado, de código abierto, potente, flexible y escalable que permite que los equipos de TIC detecten problemas en las infraestructuras con bastante antelación, evitando así que afecten los procesos de las empresas. Es un software que brinda una gran versatilidad permite monitorear una gran variedad de parámetros y enviar alertas mediante informes específicos, secuencias de comandos personalizados, correos electrónicos o SMS.

Zabbix



Precio: Gratis

Zabbix es un sistema de monitorización de redes que dispone de una interfaz web de fácil uso con autenticación de usuario segura, cuenta con varias opciones de visualización entre las que se encuentran informaciones generales, gráficos, mapas, pantallas, y dispone de varios métodos flexibles para el análisis de datos al igual que para crear alertas.

Zabbix es compatible con sondeo y captura, monitorización sin agentes al igual que agentes de rendimiento nativos para recopilar datos de los sistemas operativos más comunes.

El software se entrega gratuitamente, aunque Zabbix ofrece servicio técnico por el pago de una suscripción, con el cual asegura implementaciones a prueba de imprevistos.

Zabbix como herramienta de monitoreo con código de acceso libre permite a los usuarios utilizar, redistribuir y cambiar el software adecuándolo al propósito y funcionalidad que se necesite esto genera un gran atractivo para las empresas el poder personalizar de la mejor forma la herramienta a sus necesidades y con la gran ventaja de no incurrir en costos de licenciamiento.

No debemos confundir software libre con Open Source que es lo que aplicable para Zabbix La FSF (Free Software Foundation) establece cuatro libertades esenciales de los usuarios y bajo las mismas poder crear un software a partir de otro:

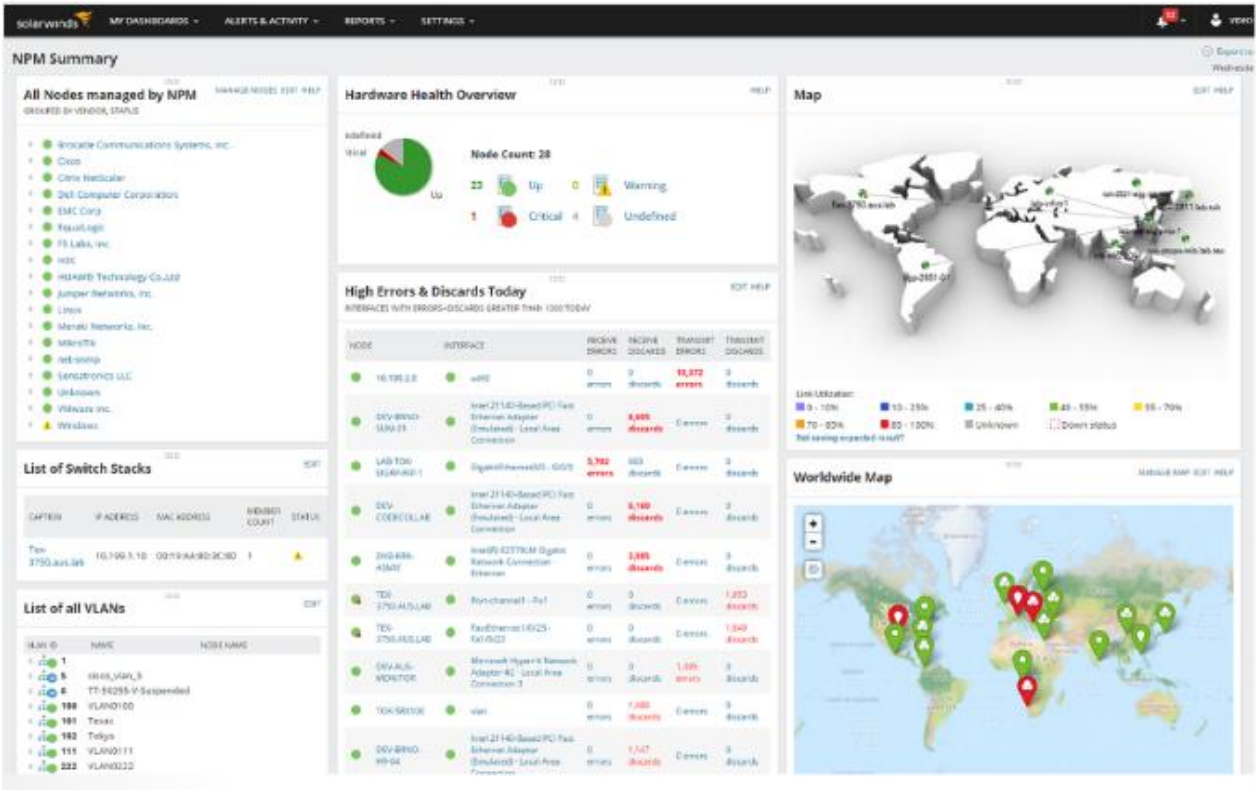
- Libertad para ejecutar el software como se desee y con cualquier propósito.
- Libertad para estudiar el funcionamiento del software y poder cambiarlo para lo que se desee. por el acceso al código fuente que se tiene.
- Libertad para distribuir copias.
- Libertad para distribuir copias de versiones modificadas a terceros.

En el cuadrante mágico de Gartner Zabbix se ubica como uno de los grandes competidores presentando ya una etapa adulta siendo utilizada para evaluar cualquier infraestructura de TI aplicaciones y recursos, es una herramienta extremadamente escalable que ofrece la oportunidad de monitoreo en tiempo real desde decenas a miles de servidores, máquinas virtuales o dispositivos de red que en la actualidad se descarga más de 4.000.000 de veces al año. Como producto Zabbix logra que las empresas alrededor del mundo tengan la certeza del monitoreo de su infraestructura TI ofreciendo si se desea a su vez una amplia gama de servicios profesionales que fueron diseñados para adaptarse a los requerimientos, complejidades y necesidades de los clientes.

Herramientas de monitorización en propiedad

En comparación con las herramientas de monitoreo open source el software en propiedad cuenta con asistencia posventa y es más asequible a la formación acreditada. El precio de adquisición es normalmente más elevado, ya que incluye todos los derechos del producto adquirido y soporte posventa para errores, actualizaciones y documentación revisada en cuanto liberen nuevas versiones.

SolarWinds



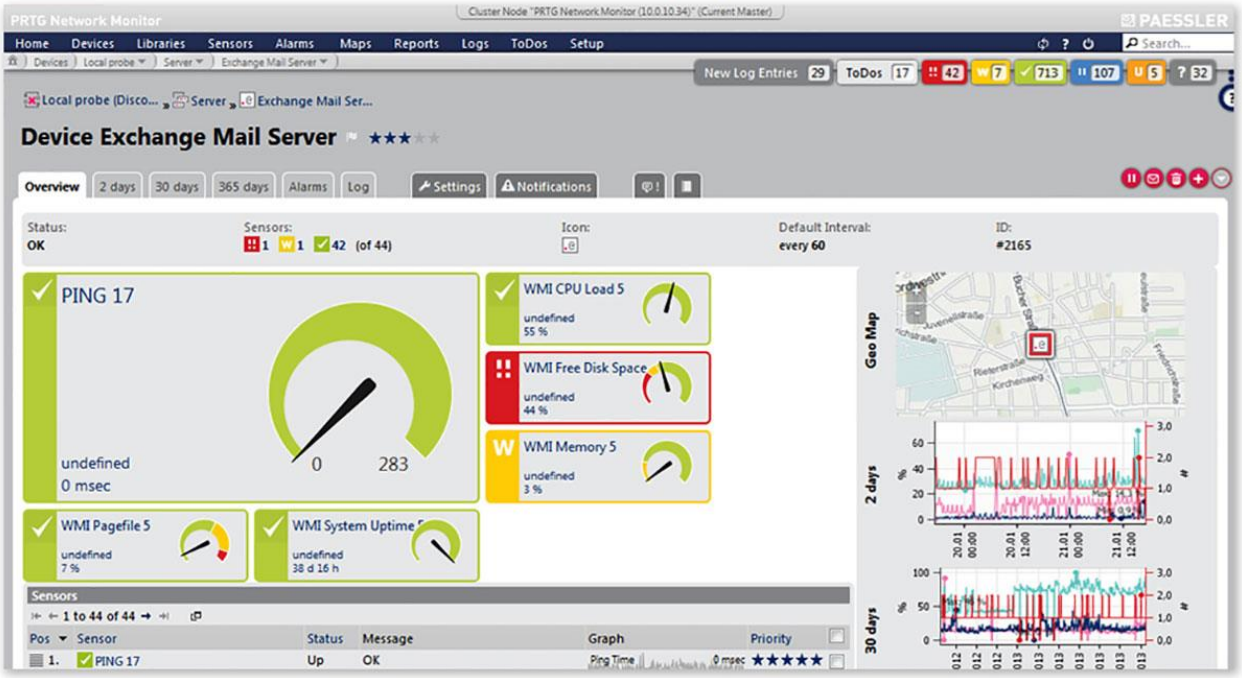
Precio: desde 3000 USD

SolarWinds es una plataforma de monitoreo que proporciona vistas integrales de aplicaciones comerciales y personalizadas que se ejecuta en entornos privados, públicos y híbridos. Algunas de sus características son la gestión del rendimiento y errores al igual que herramientas de conformidad, configuración. Se puede implementar en entornos físicos o virtuales para proporcionar parámetros detallados sobre la disponibilidad, el estado y el rendimiento de sus aplicaciones.

El software cuenta con monitoreo sin agentes, para los sistemas on premises, como con tecnología con agentes para servicios radicados en la nube. Tiene opción automática de descubrimiento y dependencia de aplicaciones que le permite fácilmente descargar, instalar y

encontrar los componentes e iniciar su monitoreo. Se puede personalizar la monitorización creando o cambiando las plantillas incorporadas o importando los archivos de comando que le permitirán monitorear aplicaciones de la empresa al igual que aplicaciones personalizadas o internas.

Paessler



Precio: en la versión de pago desde 2000 usd.

Paessler es un software de monitoreo de redes flexible que abarca una gran cantidad de componentes. Este software de monitoreo que cuenta con 200 tipos de sensores que son capaces de monitorizar la mayoría de los componentes en una infraestructura TIC, entre los que se están los dispositivos de red, servidores, entornos virtuales, aplicaciones, sistemas remotos, ancho de banda, Internet de las cosas VPN, etc. Esta poderosa herramienta cuenta con una interfaz web y una rápida función de alerta incorporada.

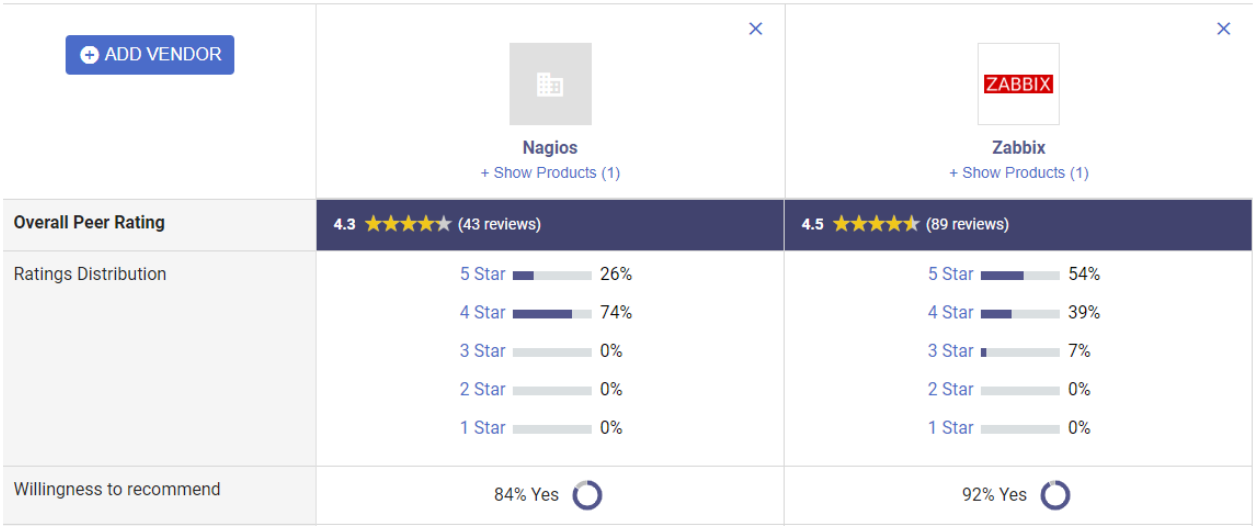
Llega a descubrir y trazar automáticamente un mapa de sus dispositivos en red, cableados o no, permitiendo monitorear los parámetros de rendimiento en clientes inalámbricos. Este

software es capaz de detectar y agregar automáticamente servidores virtuales al esquema de monitoreo.

Selección de herramienta de monitoreo

Se realizo una preselección de dos herramientas Zabbix y Nagios las cuales fueron evaluadas desde todas las aristas analizando principalmente su funcionabilidad y aplicabilidad para la compañía algunas de estas características nombradas anteriormente, una vez generada este análisis y evaluación la herramienta seleccionada para el despliegue fue Zabbix ya que cumple con las cualidades requeridas para el monitoreo de los dispositivos es una plataforma de fácil administración su interface es amigable, no generaba costo por temas de licenciamiento incluso la empresa tenía conocimiento previo del funcionamiento de la herramienta lo cual genero confianza para autorizar el prototipo, Zabbix dispone de varias características que eran de nuestro interés y el de la compañía permitió incluir al monitoreo por medio de Snmp y agentes los dispositivos que se consideraron críticos para la compañía de una manera ágil el poder generar dashboard personalizadas, reportes y alertas decidiendo por esta solución.

Según Gartner una de las herramientas más recomendadas de software libre para el monitoreo es Zabbix.



HERRAMIENTAS PARA REALIZAR SCANEO DE VULNERABILIDADES

OpenVas

Es una aplicación de software libre con excelentes características para generar búsqueda de vulnerabilidades en aplicaciones y equipos, en esta herramienta podemos seleccionar la dirección IP y apuntarle al análisis de dicho dispositivo recogiendo información de los puertos abiertos, fallos de configuración, servicios en funcionamiento y posibles vulnerabilidades conocidas referentes al software del dispositivo o servidor sus funciones incluyen pruebas autenticadas y no autenticadas.

Algunas de sus características principales son:

- Puede ser utilizada de forma individual o integral (OSSIM(Open Source Security Information Management).
- Se encuentra Kali Linux como herramienta predefinida.
- Se puede ejecutar escaneos de forma automática.
- Escáner de vulnerabilidades de código abierto.
- Detecta los errores de seguridad en sistemas y aplicaciones remotas.
- Soporta HTTP y HTTPS.
- Genera reportes claros y completos.
- Se puede reiniciar o detener las tareas de escaneo cuando se requiera.
- Genera informes en diferentes XML, HTML.
- Cuenta con OpenVAS Transfer Protocol (OTP)

Nessus

Es una herramienta de escaneo de vulnerabilidades utiliza un demonio que genera el escaneo al sistema objetivo y Nessus el cliente que va mostrando el avance de los diferentes análisis, desde la consola Nessus se pueden realizar escaneos programados fáciles de usar, su

analizador de seguridad de redes es potente con una amplia cantidad de plugins que son actualizados a diario es un programa de escaneo que opera en diversos sistemas operativos.

Los resultados de los escaneos pueden se guardados en una base de conocimiento. La herramienta permite escaneos de forma remota en una red o de forma local en un equipo específico. La interfaz muestra los resultados del análisis en tiempo real. Nessus está respaldado por un equipo de expertos de investigación de vulnerabilidades y una de las bases de datos más grandes del mundo. La escalabilidad de Nessus se ajusta para servir desde pequeñas empresas hasta las organizaciones más grandes y brinda una gran facilidad para su implementación.

¿Cómo funciona?

Desde consola Nessus puede ser programado para hacer escaneos programados con cron:

- Escanea el servidor, dispositivo o aplicación con la dirección IP o Url.
- Se escoge el nombre del análisis, de acuerdo a su gran cantidad de módulos y se relaciona el dispositivo objetivo.
- Cuando se complete el análisis clic en resultados.
- En la opción HOSTS muestra las vulnerabilidades en porcentajes clasificadas en 5: Críticas, Altas, Medias, Bajas y de información.
- Se puede ingresar a cada vulnerabilidad para una descripción más detallada.

Beneficios

Nessus es una herramienta de seguridad web de fácil uso con una comunidad muy amplia a nivel mundial, algunos de sus beneficios son:

- Cuenta con una gran base instalada y la mejor experiencia en la industria, Nessus ofrece a los clientes la capacidad de identificar sus mayores amenazas y responder rápidamente.

- Detecta amenazas como virus, malware, puertas traseras y servidores que se comunican con sistemas infectados con botnets.

- Informa y comunica problemas de seguridad en toda la organización mediante informes de solución.

- Es Detallado: Paneles de mando detallados para ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas

- Es Rentable: Nessus reduce el tiempo y costo de seguridad en el escaneo y asegura los términos de cumplimientos de seguridad.

Nmap

Es un escáner para auditorias de seguridad en red que permite escanear servicios UDP, TCP, ICMP, RPC, de la misma forma como el sistema operativo. Nmap utiliza paquetes IP sin procesar de formas novedosas para determinar que equipos están disponibles en la red que servicios están entregando esos equipos que sistemas operativos y versión de sistemas operativos están ejecutando, el tipo de paquetes de filtrado que firewalls están en uso. Nmap Fue diseñado para escanear de manera rápida grandes redes, pero funciona bien con equipos en específico además del clásico ejecutable Nmap de línea de comandos la suite de Nmap incluye una GUI avanzada y un visor de resultados (Zenmap) una herramienta flexible de transferencia de datos, redirección y depuración (Ncat), una utilidad para comparar resultados de escaneo (Ndiff) y una herramienta de generación de paquetes y análisis de respuesta (Nping).

Algunas de sus principales características son:

- Flexible: Permite docenas de técnicas avanzadas para mapear redes llenas de filtros IP, firewalls, enrutadores y otros obstáculos. Esto incluye muchos mecanismos de

escaneo de puertos (TCP y UDP), detección de sistema operativo, detección de versión, barridos de ping y más.

- Potente: Nmap se ha utilizado para escanear grandes redes de cientos de miles de máquinas.
- Portátil: Es compatible con la mayoría de sistemas operativos Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS.

Acunetix

Acunetix Vulnerability es un escáner utiliza un rastreador rápido y multiproceso en una herramienta totalmente automatizada que combina tecnologías de escaneo dinámico y estático para detectar vulnerabilidades que de otro modo se perderían mientras se mantienen los falsos positivos al mínimo. Utiliza un agente de supervisión dedicado y proporciona un paquete completo de gestión de vulnerabilidades.

Acunetix no es solo un escáner de vulnerabilidades web, es una solución completa para pruebas de seguridad de aplicaciones web que se puede usar tanto de forma independiente como parte de entornos complejos. Ofrece evaluación de vulnerabilidad y gestión de vulnerabilidad incorporadas, así como muchas opciones para la integración con herramientas de desarrollo de software líderes en el mercado. Al hacer que Acunetix sea una de sus medidas de seguridad, puede aumentar significativamente su postura de seguridad cibernética y eliminar muchos riesgos de seguridad a un bajo costo de recursos.

Detecta más de 4.500 vulnerabilidades de aplicaciones web, escanea aplicaciones de código abierto y personalizadas con 100% de precisión en la detección de vulnerabilidades críticas, inyección SQL avanzada y pruebas de secuencias de comandos entre sitios (XSS) además puede rastrear aplicaciones de una sola página del lado del cliente (SPA).

Nikto

Es un escáner de servidores web de código abierto basado en lenguaje Perl que evalúa posibles vulnerabilidades de seguridad. No es una herramienta invisible, Nikto prueba abiertamente un servidor web dentro de un período de tiempo mínimo y es visible para archivos de registro o sistemas de detección, prevención de intrusiones (IDS / IPS). De hecho, Nikto puede ser una herramienta útil para probar un IDs IPS desplegados, Nikto descubre automáticamente servidores y software web instalados, comprueba más de 6.700 archivos y programas peligrosos, versiones desactualizadas para más de 1.250 servidores y problemas específicos de la versión para más de 270 servidores. Analiza vulnerabilidades de configuración del servidor, como múltiples archivos de índice, scripts olvidados, opciones HTTP, etc.

5. Glosario de términos

Access Point: Dispositivo de interconexión de equipos en una red inalámbrica

Administración centralizada: Define la administración de todos los dispositivos desde un punto o equipo central

Amenaza: Todo elemento o acción que atenta contra la seguridad de la información, las amenazas surgen a partir de la existencia de vulnerabilidades.

Análisis de vulnerabilidades: Proceso de identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas

Ataque cibernético: Es el intento de obtener el control de un sistema informático u equipo con fines de robar, exponer, modificar o dañar la información o el mismo sistema.

Controladora Wi-Fi: Es un equipo físico o software que administra de manera centralizada los diferentes puntos de acceso de una red inalámbrica que se conectan a la red.

Clave: Conjunto de atributos en informática que permiten el acceso a un sistema

Convergencia: Término que se utiliza en telecomunicaciones para designar aquellas redes, sistemas y servicios, que se construyen a partir de otras redes, sistemas o servicios

Firewall: Parte de un sistema informático (hardware y/o software) que está diseñado para bloquear el acceso no autorizado

Firmware: El firmware o soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Hardening: Es el proceso de asegurar un sistema para reducir sus vulnerabilidades en búsqueda de generar la reducción de las formas de ataque disponibles generalmente incluye el cambio de contraseñas predeterminadas, la eliminación de software innecesario nombres de usuario o inicios de sesión innecesarios, y la desactivación o eliminación de servicios innecesarios combinado con la actualización de los sistemas.

Información: Es el activo más importante de una compañía.

Infraestructura de Red: Son todos los elementos básicos y necesarios para que los servicios de telecomunicaciones sean funcionales**.**

ITIL v4: Son las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías

Listas de acceso: Concepto de seguridad informática que de determinar los permisos de acceso a un objeto o medio.

Monitoreo: Es el uso de un sistema constante que monitoriza la infraestructura red y sistemas en busca de fallas o lentitud para informar por medio de reportes y alertas.

Norma ISO 27001: Norma que determina los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Norma ISO 9001: Norma que determina los requisitos para un Sistema de Gestión de la Calidad.

Protocolo de seguridad: Reglas definidas con la finalidad de unificar criterios en tareas de seguridad informática.

Política de seguridad: Son reglas que todo personal de una compañía debe cumplir con el fin de asegurar la integridad, disponibilidad y privacidad de una infraestructura informática.

Prototipo: Define como cualquier tipo de maquina o sistema diseñado para realizar modelos de pruebas o demostraciones de funcionalidad.

Puerto: Es una interfaz de tipo físico o virtual a través de la cual se pueden enviar y recibir los diferentes tipos de datos.

Protocolo de Comunicaciones: Es un sistema de reglas que permiten que dos o mas sistemas de comunicaciones se comuniquen entre ellas para transmitir información a través de diversos medios físicos.

Redes LAN: Define la red de computadores locales en un edifico o casa

Redes WAN: Define una red de computadoras que enlaza diferentes redes locales LAN

Redes WLAN: Define el sistema de comunicación inalámbrico en una red local

Riesgo informático: Problema que potencialmente puede ocurrir que afecte la continuidad del sistema informático.

Switch: Dispositivo de interconexión de equipos en una red local.

Servidor: Es una máquina física o virtual integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software y provee datos a otras máquinas.

Sistema operativo: Es el software principal o un conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.

Seguridad perimetral: Seguridad perimetral informática se refiere a la seguridad que afecta a la frontera de la red de nuestra empresa también llamada perímetro. Esta frontera o perímetro, está formada por el conjunto de máquinas y dispositivos que interactúan con el exterior, con otras redes.

Telnet: Nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente

Vulnerabilidad: Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

6. Justificación

Con el análisis de vulnerabilidades se busca que la empresa comprenda la necesidad de una correcta implementación de políticas y estándares de seguridad a través de metodologías y buenas prácticas de uso en los dispositivos que intervienen en la red, que pueda afectar a la organización y como asegurar la información vital de la compañía que es el activo más importante.

Las herramientas escogidas para realizar este análisis evaluando su capacidad, accesibilidad, licenciamiento y costo son: NMAP herramienta Gratuita para realizar escaneo de puertos y NESSUS versión comunidad de uso estudiantil la cual permite el análisis de 16 dispositivos debido a que es una herramienta de licenciada.

7. Objetivos

7.1. General.

Diseñar un Análisis a nivel de seguridad perimetral e infraestructura de la red local, que permita generar unas recomendaciones para lograr el desempeño óptimo de los recursos de red, siguiendo las recomendaciones de la norma ISO 27001 v2013 del uso los estándares de seguridad internacionales, donde aplique.

7.2. Específicos

- Generar un levantamiento de información de los equipos de la infraestructura de red local y la seguridad perimetral.
- Análisis de resultados la información recopilada
- Realizar un análisis de vulnerabilidades a nivel general de la infraestructura de red de los elementos críticos identificados en la organización.
- Proponer una serie de recomendaciones que puedan entregar un apoyo en la definición de medidas y modelos de seguridad para los dispositivos de red
- Diseñar una propuesta de un sistema de monitoreo para la infraestructura de red como plan de mejora de la seguridad y disponibilidad de los dispositivos críticos en las redes telemáticas de la organización.

8. Requerimientos

8.1 Requerimientos funcionales

- Las políticas de fortalecimiento contraseñas de dispositivos de red
- Las políticas de acceso y restricción entre VLANS
- Definición de tipo de seguridad y numero de SID propagados en la red Wi-Fi
- Políticas de conectividad a la red Wi-Fi
- Tener un monitoreo de los dispositivos de red.

8.2 Requerimientos no funcionales

- Plan de distribución y asignación de VLANS
- Descripción del plan de direccionamiento y permisos ente los mismos
- Plan de segmentación de SID en red Wireless
- Levantamiento de información del estado de la infraestructura actual
- Informe de análisis de Seguridad básico del estado actual de la configuración de los dispositivos de red y puertos en algunos servidores de producción y pruebas delegados por la empresa
- Informe de recomendaciones y buenas prácticas en seguridad

9. Metodología

En el desarrollo de la metodología para la Seguridad en Redes de la Empresa se realizó previamente un análisis de cómo se encuentra en la actualidad a nivel de seguridad, identificando sus posibles amenazas y debilidades a nivel de red, analizando cómo estas afectan los medios de comunicación y el correcto desarrollo tecnológico de las diferentes áreas de la empresa, permitiendo realizar un diagnóstico de estas fallas de seguridad informática y de esta forma plantar una serie de recomendaciones, planes, procedimientos, políticas y buenas prácticas para mejorar e incrementar estos niveles de seguridad.

Niveles de desarrollo de la metodología

1. Planteamiento e identificación de la problemática asociada.
   Identificar los alcances y que se quiere lograr al realizar un análisis de la infraestructura de red de la empresa.
2. Identificación de la problemática asociada.
3. Realizar un levantamiento de información de todos los activos de red críticos de la empresa.
4. Identificar niveles y tipos de seguridad que se quieren evaluar.
5. Realización de un análisis de vulnerabilidades a la empresa en búsqueda de falencias de seguridad física y lógica, utilizando las herramientas definidas para el desarrollo de la actividad.
6. Análisis de la información de las debilidades de seguridad identificadas.
7. Análisis de evidencias encontradas con el diagnostico.
8. Diseño de planes de mejoramiento de la seguridad.
9. Generación de una serie de informes entregables para la compañía.
10. Entrega de informe de seguridad, recomendaciones y buenas prácticas.
11. Entrega a la compañía del análisis de vulnerabilidades realizado, evidencias y propuestas de la solución.

10. Capítulos de desarrollo

Durante el desarrollo de la metodología se muestra la información de los diferentes tipos de equipos permitidos por la organización para realizar una evaluación más precisa del estado actual de al red en la Empresa para proceder con el análisis de vulnerabilidades realizando un escaneo de puertos con la herramienta NMAP y un posterior análisis con la Herramienta NESSUS para identificar las vulnerabilidades más importantes que requieren atención.

10.1 Levantamiento de Información

TOPOLOGIA DE RED	ARBOL
USUARIOS	650
CANALES DE INTERNET	3
CANALES DE MPLS	2
SSID PUBLICADOS WLAN	6
AUTENTICACION WLAN	WEP Y WPA

EQUIPOS DE NETWORKING					
TIPO	**MARCA**	**MODELO**	**THROGHPUT**	**PUERTOS**	**CANTIDAD**
CORE	DELL	N4032	640 Gbps	48	2
CORE	DELL	N4064	640 Gbps	24	2
ACCESO	DELL	N1524	128 Gbps	24	8
ACCESO	DELL	N1548	176 Gbps	48	16
ACCESO	HP	5130	128 Gbps	24	22
ACCESO	HP	5130	176 Gbps	48	10
FIREWALL	SONICWALL	6600	12 Gbps	20	2
CONTROLADORA WI-FI	CISCO	5508	8 Gbps	8	1
ACCESPOINT	CISCO	1852	2 Gbps	1	28
ACCESPOINT	CISCO	2702	5 Gbps	1	50
ACCESPOINT	RUCKUS	R310	1,1 Gbps	1	1

Tabla 1: Información de Infraestructura de Red

SERVIDORES Y EQUIPOS						
DESCRIPCION	**TIPO**	**MARCA**	**SISTEMA OPERATIVO**	**CPU**	**RAM**	**DISCO**
SERVIDOR DE ARCHIVOS 6	Servidor	HP	Windows Server 2008 Estándar 32 Bits	4 Core	16 GB	20000 GB
SERVIDOR FTP	Servidor	HP	Windows Server 2012 R2 Estándar	4 Core	12 GB	400 GB
SERVIDOR DE ARCHIVOS 5	Servidor	HP	Windows Server 2012 R2 Estándar	12 Core	32 GB	1500 GB
SERVIDOR APLICACIONES 4	Servidor	HP	Windows Server 2003 R2 Estándar	2 Core	2 GB	500 GB
SERVIDOR DIRECTORIO ACTIVO 5	Servidor	HP	Windows Server 2012 R2 Estándar	8 Core	8 GB	200 GB
SERVIDOR DIRECTORIO ACTIVO 3	Servidor	HP	Windows Server 2012 R2 Estándar	4 Core	14 GB	400 GB

SERVIDOR BASE DE DATOS 7	Servidor	HP	Windows Server 2008 R2 Enterprise	16 Core	64 GB	2300 GB
SERVIDOR DE BASE DE DATOS 0	Servidor	HP	Windows Server 2016 Estándar	32 Core	196 GB	4000 GB
SERVIDOR DE APLICACIONES 3	Servidor	HP	Windows Server 2012 R2 Estándar	2 Core	8 GB	200 GB
EQUIPO WINDOWS 7	Equipo cliente	HP	Windows 7 Profesional	4 Core	4 GB	500 GB
EQUIPO WINDOWS 10	Equipo cliente	HP	Windows 10 Profesional	4 Core	4 GB	500 GB

Tabla 2: Información de Servidores y Equipos

10.2 Diagramas

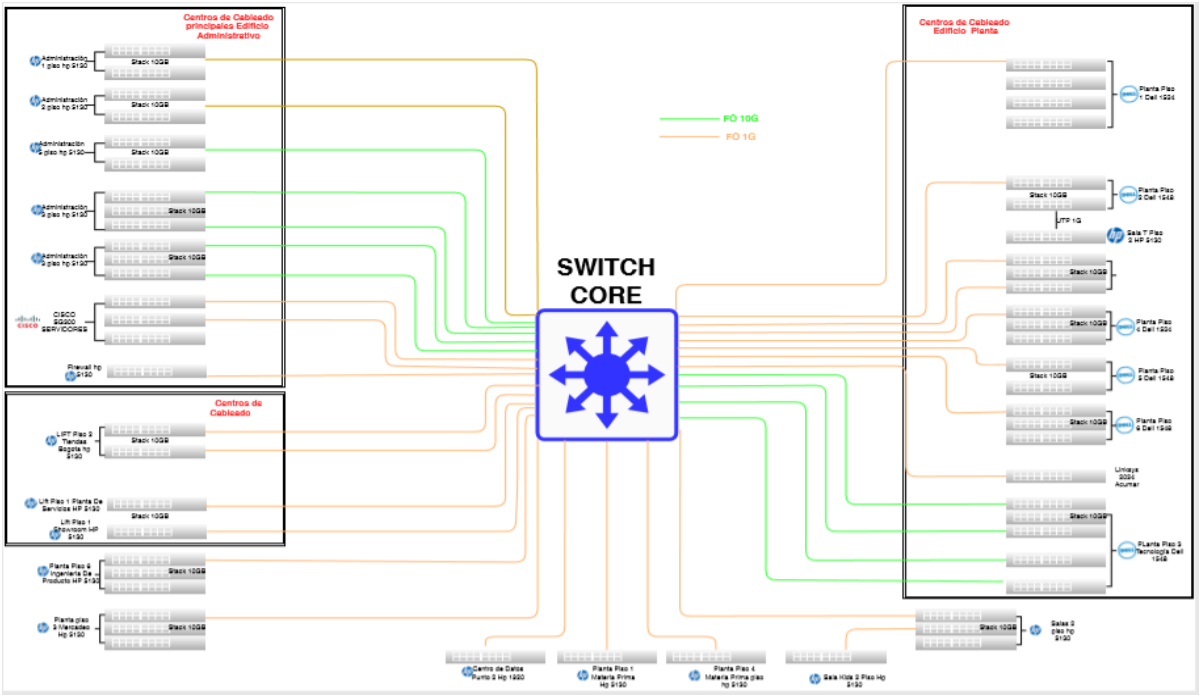


Diagrama 1: Topología de Red

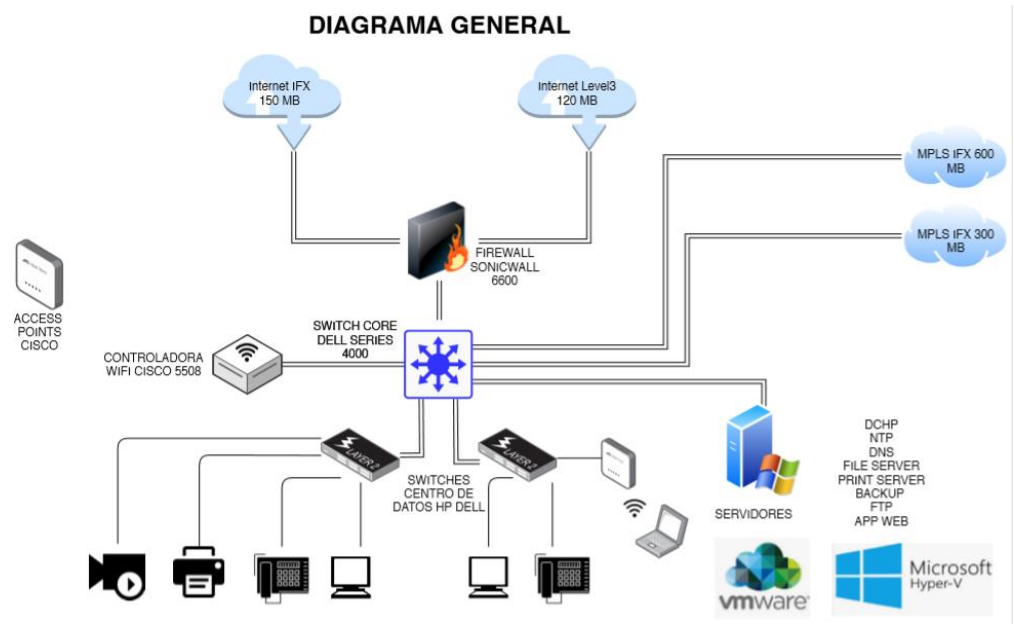


Diagrama 2: Diagrama General de Conectividad

10.3 Escaneo de Vulnerabilidades

Por medio de la herramienta NMAP se procede a escanear los puertos que se encuentren abiertos, de la misma forma se utiliza la herramienta NESSUS en busca de las vulnerabilidades de los diferentes tipos de dispositivos de red, equipos de usuarios y servidores seleccionados.

- CONTROLADORA WI-FI
- SWITCH CORE
- SWITCH HP
- SWITCH DELL
- FIREWALL
- EQUIPO WINDOWS 7
- EQUIPO WINDOWS 10
- SERVIDOR DE ARCHIVOS 5
- SERVIDOR DE ARCHIVOS 6
- SERVIDOR FTP
- SERVIDOR DE APLICACIONES 4
- SERVIDOR DE DIRECTORIO ACTIVO 5
- SERVIDOR DE APLICACIONES 93
- SERVIDOR DE DIRECTORIO ACTIVO 83
- SERVIDOR DE BASE DE DATOS 7
- SERVIDOR DE BASES DE DATOS 0

EVIDENCIAS DE LOS PROCEDIMIENTOS RELACIONADOS

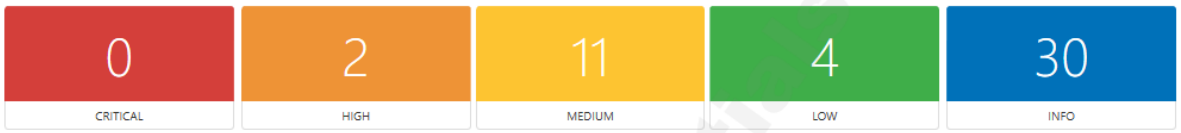
Herramientas utilizadas:
Escaneo de puertos – NMAP Versión 7.08
Escaneo de vulnerabilidades - NESSUS Versión 8.9

CONTROLADORA WI-FI

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [3] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	Cisco WLC sshd		
443	tcp	open	https	syn-ack			
444	tcp	open	snpp	syn-ack			
16113	tcp	open	unknown	syn-ack			

RESULTADOS DE ESCANEO DE VULNERABILIDADES NESSUS



Severity	CVSS	Plugin	Name
HIGH	7.8	130208	Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	7.8	118461	Cisco Wireless LAN Controller Multiple Vulnerabilities
MEDIUM	6.8	124334	Cisco Wireless LAN Controller Locally Significant Certificate Denial of Service Vulnerability
MEDIUM	6.8	124331	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	124332	Cisco Wireless LAN Controller Software IAPP Message Handling Denial of Service Vulnerabilities
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	76474	SNMP 'GETBULK' Reflection DDoS
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported

LOW	3.3	124333	Cisco Wireless LAN Controller Secure Shell Unauthorized Access Vulnerability
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SWITCH CORE

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.5	protocol 2.0
23	tcp	open	telnet	syn-ack	Dell OpenManage telnetd		
80	tcp	open	http	syn-ack	Dell N2000-series switch http admin		

Resultados de Escaneo de vulnerabilidades NESSUS

0	0	1	0	16
CRITICAL	HIGH	MEDIUM	LOW	INFO

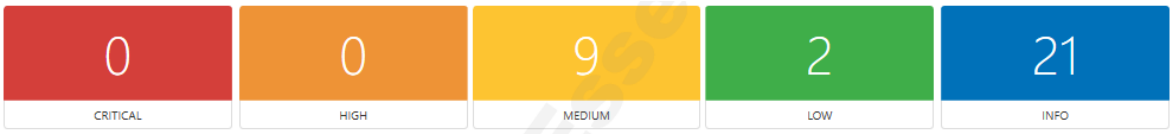
Severity	CVSS	Plugin	Name
MEDIUM	5.8	42263	Unencrypted Telnet Server

SWITCH HP

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	HP Comware switch sshd	7.1.070	protocol 2.0
443	tcp	open	https	syn-ack	HTTPD		

Resultados de Escaneo de vulnerabilidades NESSUS



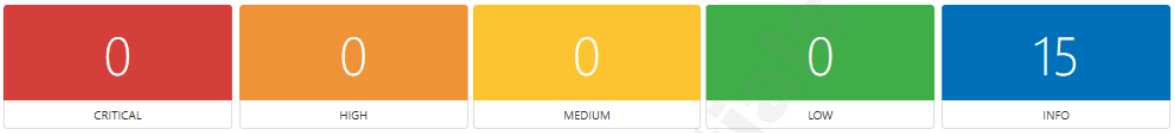
Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

SWITCH DELL

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.5	protocol 2.0
80	tcp	open	http	syn-ack	Web Server		

Resultados de Escaneo de vulnerabilidades NESSUS

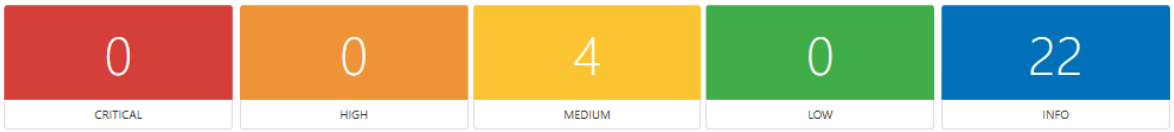


FIREWALL

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.2	protocol 2.0
80	tcp	open	http	syn-ack	SonicWALL firewall http config		
443	tcp	open	http	syn-ack	SonicWALL firewall http config		

Resultados de Escaneo de vulnerabilidades NESSUS



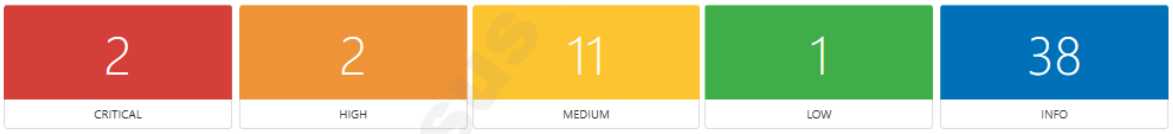
Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

EQUIPO WINDOWS 7

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	GeoVision GeoHttpServer for webcams		
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Windows 7 Professional 7601 Service Pack 1 microsoft-ds		workgroup: CAMARAS
3389	tcp	open	ms-wbt-server	syn-ack			
4550	tcp	open	geovision-control	syn-ack	Geovision webcam control		
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
5550	tcp	open	sdadmind	syn-ack			
8081	tcp	open	blackice-icecap	syn-ack			
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49161	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS



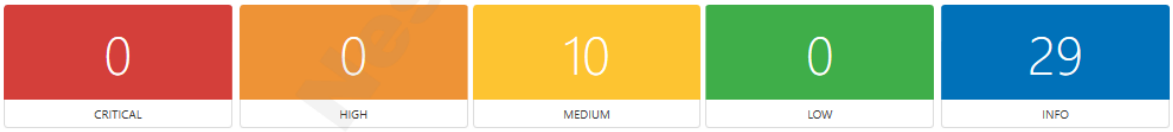
Severity	CVSS	Plugin	Name
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

EQUIPO WINDOWS 10

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	GeoWebServer 5.1.0.0		
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
443	tcp	open	https	syn-ack	GeoWebServer 5.1.0.0		
445	tcp	open	microsoft-ds	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
8081	tcp	open	blackice-icecap	syn-ack			

Resultados de Escaneo de vulnerabilidades NESSUS



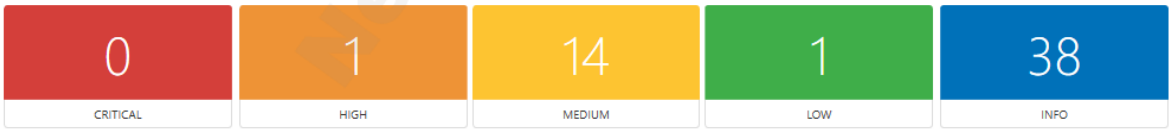
Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported

SERVIDOR DE ARCHIVOS 5

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	Microsoft ftpd		
80	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
443	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds		
2179	tcp	open	vmrdp	syn-ack			
2260	tcp	open	apc-2260	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS



Severity	CVSS	Plugin	Name
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

SERVIDOR DE ARCHIVOS 6

Resultados de Escaneo de puertos – NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Windows Server (R) 2008 Standard 6003 Service Pack 2 microsoft-ds		workgroup: [redacted]
1311	tcp	open	http	syn-ack	Dell PowerEdge OpenManage Server Administrator httpd admin		
3389	tcp	open	ms-wbt-server	syn-ack			
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
5633	tcp	open	giop	syn-ack	omg.org CORBA naming service		
5666	tcp	open	tcpwrapped	syn-ack			
6101	tcp	open	backupexec	syn-ack			
6106	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
8081	tcp	open	blackice-icecap	syn-ack			
10000	tcp	open	ndmp	syn-ack	Symantec/Veritas Backup Exec ndmp		Name: [redacted]1; OS ver: 6.0; OS Build: 6003; OS Service Pack: 2
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49157	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

2	1	15	4	42
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported

MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SERVIDOR FTP

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	FileZilla ftpd		
22	tcp	open	ssh	syn-ack	WeOnlyDo sshd	3.3.0.424	protocol 2.0
80	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2012 R2 Standard 9600 microsoft-ds		
3389	tcp	open	ms-wbt-server	syn-ack			
8081	tcp	open	http	syn-ack	McAfee AntiVirus		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49167	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	2	31

Severity	CVSS	Plugin	Name
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled

SERVIDOR DE APLICACIONES 4

Resultados de Escaneo de puertos – NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	6.0	
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2003 R2 3790 Service Pack 2 microsoft-ds		
1025	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
1029	tcp	open	java-rmi	syn-ack	Java RMI		
1033	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
1433	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2000	8.00.766.00; SP3a	
2522	tcp	open	windb	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Service		
5666	tcp	open	tcpwrapped	syn-ack			
5800	tcp	open	vnc-http	syn-ack	RealVNC	4.0	resolution: 400x250; VNC TCP port: 5900
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.8

Resultados de Escaneo de vulnerabilidades NESSUS

4	2	3	0	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	72091	Adobe ColdFusion Unsupported Version Detection
CRITICAL	10.0	97994	Microsoft IIS 6.0 Unsupported Version Detection
CRITICAL	10.0	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.5	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	48340	Adobe ColdFusion 'locale' Parameter Directory Traversal
MEDIUM	5.0	57608	SMB Signing not required

SERVIDOR DE DIRECTORIO ACTIVO 5

Resultados de Escaneo de puertos – NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack			
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2020-05-14 03:07:15Z
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: Principal-Site
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: Principal-Site
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: Site: Principal-Site
3269	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: Principal-Site
3389	tcp	open	ms-wbt-server	syn-ack			
10000	tcp	open	ndmp	syn-ack	Symantec/Veritas Backup Exec ndmp		Name: ; OS ver: 6.2; OS Build: 9200; OS Service Pack: 0
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49158	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
49159	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49999	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

0	1	8	1	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SERVIDOR DE APLICACIONES 3

Resultados de Escaneo de puertos – NMAP

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
25	tcp	open	smtp	syn-ack	Microsoft ESMTP	8.5.9600.16384	
80	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
113	tcp	closed	ident	reset			
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
443	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
2000	tcp	open	cisco-sccp	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
5060	tcp	open	sip	syn-ack			
8081	tcp	open	blackice-icecap	syn-ack			
8086	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
8087	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
9090	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
9091	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49160	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

0	1	10	2	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

SERVIDOR DE DIRECTORIO ACTIVO 3

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack			
88	tcp	open	kerberos-sec	syn-ack	Microsoft Windows Kerberos		server time: 2020-05-14 03:18:04Z
113	tcp	closed	ident	reset			
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: IFX-Site
445	tcp	open	microsoft-ds	syn-ack			
464	tcp	open	kpasswd5	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: IFX-Site
2000	tcp	open	cisco-sccp	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: IFX-Site
3269	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: , Site: IFX-Site
3389	tcp	open	ms-wbt-server	syn-ack			
5060	tcp	open	sip	syn-ack			
5666	tcp	open	nrpe	syn-ack			
8081	tcp	open	blackice-icecap	syn-ack			
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49158	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
49159	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49160	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

0	1	9	3	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6	31705	SSL Anonymous Cipher Suites Supported
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SERVIDOR DE BASE DE DATOS 7

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	7.5	
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack			
1433	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2008 R2	10.50.2500.00; SP1	
2000	tcp	open	tcpwrapped	syn-ack			
2383	tcp	open	ms-olap4	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
5060	tcp	open	tcpwrapped	syn-ack			
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Resultados de Escaneo de vulnerabilidades NESSUS

2	3	12	3	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	9.3	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

SERVIDOR DE BASES DE DATOS 0

Resultados de Escaneo de puertos - NMAP

Port		State (toggle closed [1] | filtered [0])	Service	Reason	Product	Version	Extra info
113	tcp	closed	ident	reset			
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
445	tcp	open	microsoft-ds	syn-ack			
1433	tcp	open	ms-sql-s	syn-ack	Microsoft SQL Server 2016	13.00.4451.00; SP1+	
2000	tcp	open	cisco-sccp	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
5060	tcp	open	sip	syn-ack			

Resultados de Escaneo de vulnerabilidades NESSUS

0	0	8	0	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

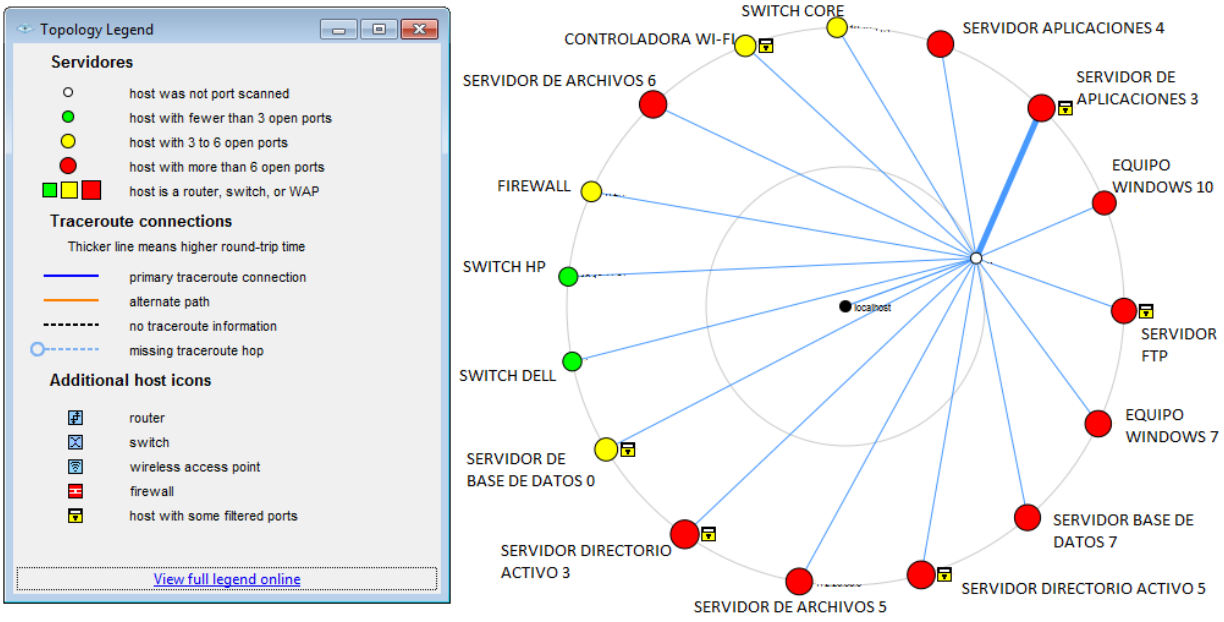
Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	121010	TLS Version 1.1 Protocol Detection
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

11. Resultados

Con los resultados obtenidos se procede a continuación a realizar el análisis de la información obtenida validando el estado actual de la seguridad en la red y el grado de importancia de las vulnerabilidades identificadas con el que deben ser abordados para mitigar los riesgos de seguridad.

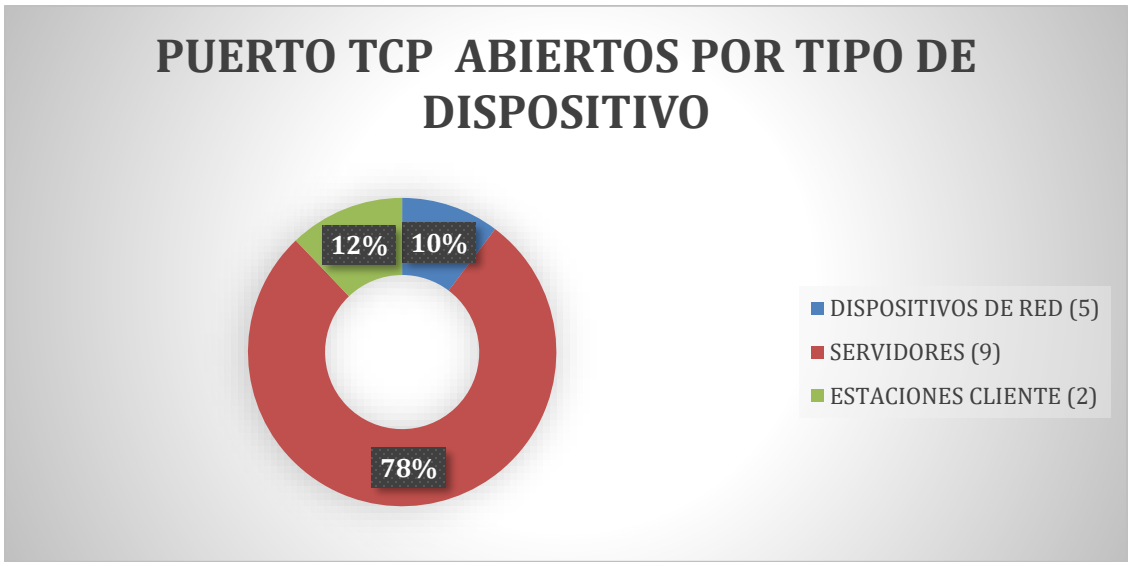
11.1 Análisis de vulnerabilidades

Con el fin de obtener una visibilidad del estado actual de la seguridad con los diferentes equipos que interactúan en la red y el grado de importancia con el que deben ser abordados y evaluados de los cuales NO se tomara para el plan de remediación las vulnerabilidades de clase INFORMATIVA, identificando que en inicialmente no generan impacto sobre la evaluación del riesgo. La información de estos riesgos de bajo nivel se encuentra en el Anexo no. 5 del reporte proporcionado por la herramienta Nessus.



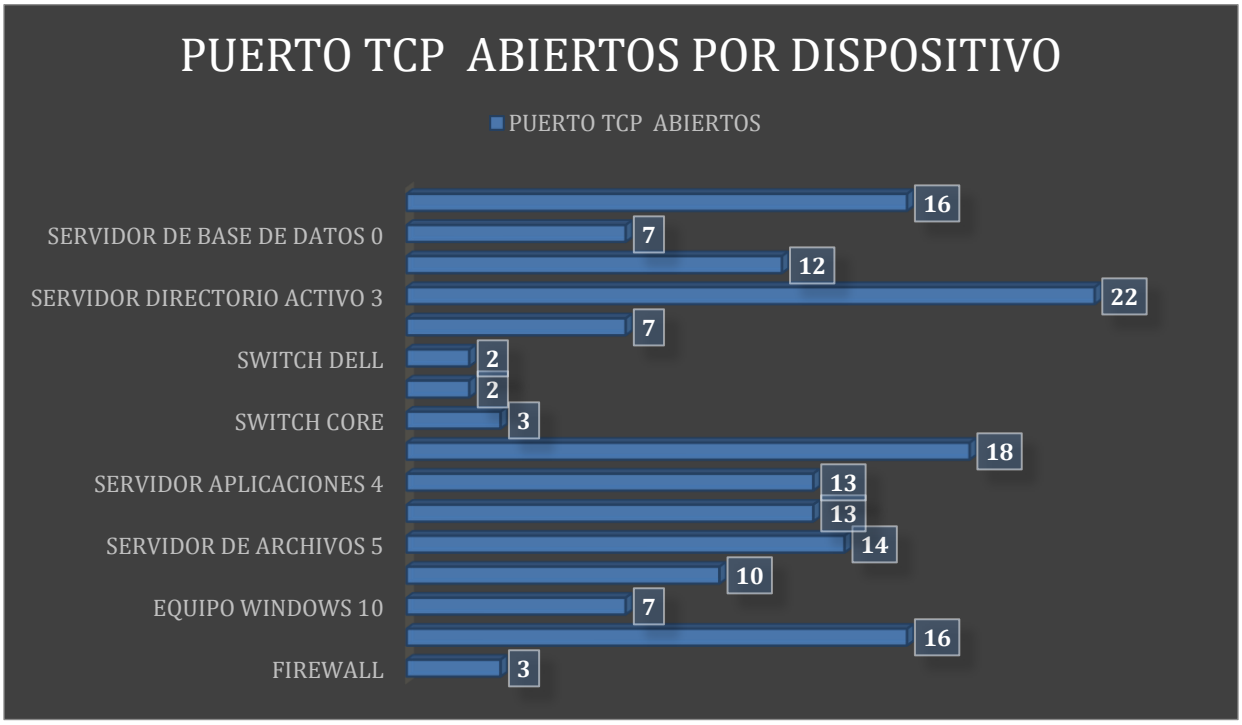
Grafica 1: Estado General de Puertos Abiertos

Los servidores y los equipos cliente Windows son los que más presentan puertos abiertos.
Rojo – con mas de 6 puertos abiertos
Amarillo – de 3 a 6 puertos abiertos
Verde – hasta 3 puertos abiertos



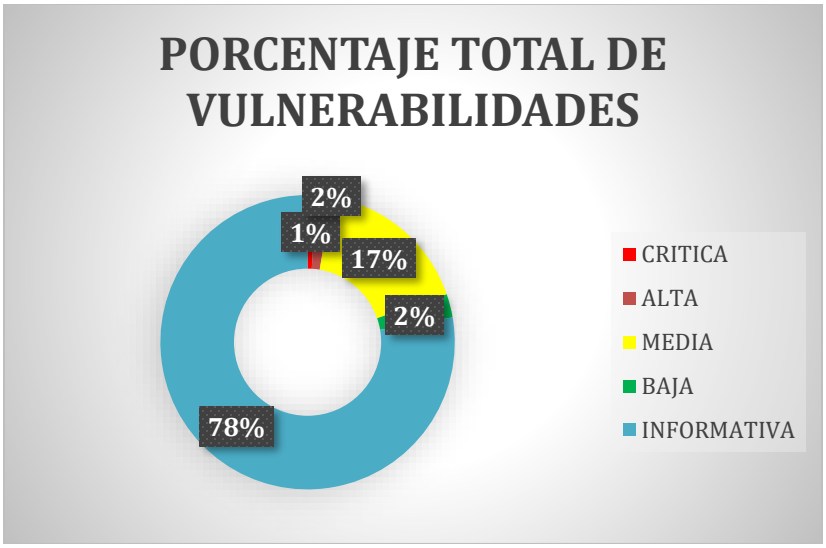
Grafica 2: Puertos TCP Abiertos Por Tipo De Dispositivo

El 78 % de los equipos con más puertos abiertos son los servidores



Grafica 3: Puertos TCP Abiertos Por Dispositivo

Los Servidores de directorio activo son los equipos con más cantidad de puertos abiertos



Grafica 4: Porcentaje Total De Vulnerabilidades

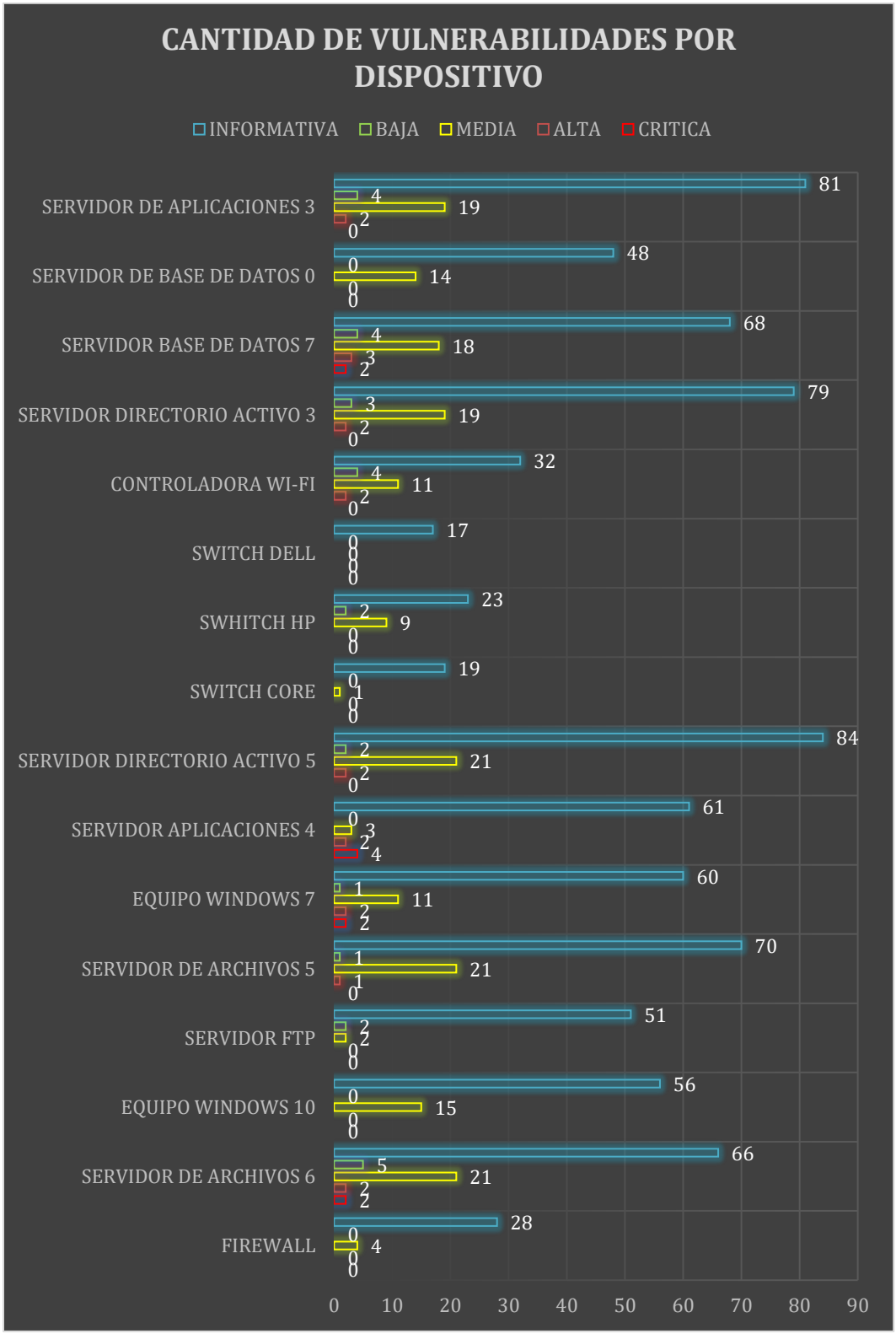
Del total de vulnerabilidades escaneadas el 1% es Critico el 2 % es alto las cuales requiere mayor atención

Grafica 5: Vulnerabilidades Que Requiere Atención

En la evaluación de vulnerabilidades podemos observar que de los 16 dispositivos escaneados tenemos que tenemos una gran cantidad de vulnerabilidades que deben ser mitigadas según el impacto.

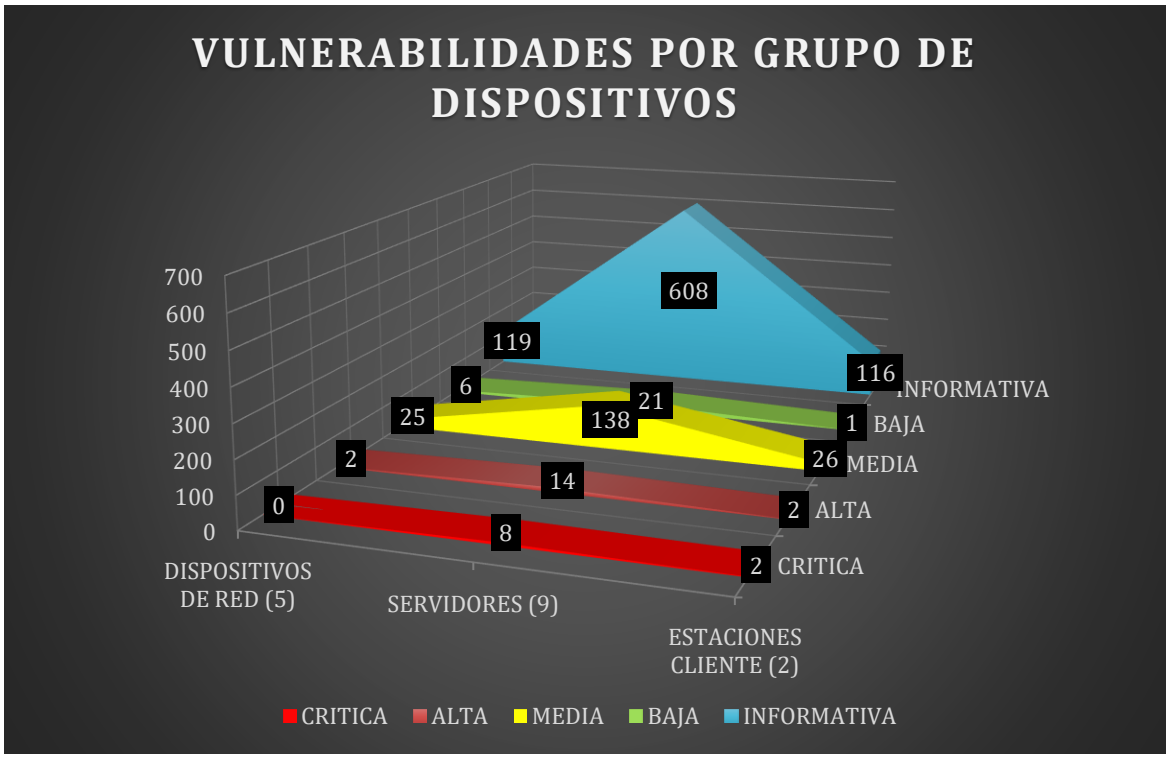
OBJETIVOS	CRITICA	ALTA	MEDIA	BAJA	INFORMATIVA
16	18	34	338	51	1536

Tabla 3: Total De Vulnerabilidades



Grafica 6: Vulnerabilidades Por Dispositivo

El servidor de aplicaciones 4 es el que más vulnerabilidades tiene con 4 vulnerabilidades críticas y 2 vulnerabilidades altas seguido del servidor de base de datos 0 que tiene 2 vulnerabilidades críticas y 3 vulnerabilidades altas, el firewall tiene 4 vulnerabilidades altas



Grafica 7: Vulnerabilidades Por Grupo De Equipos

Los dispositivos de red no cuentan con vulnerabilidades críticas.

11.2 Plan de Mitigación

El Cuadro de mitigación de vulnerabilidades se realiza con el fin de identificar los tres tipos de vulnerabilidades más importantes (vulnerabilidades CRITICAS, vulnerabilidades ALTAS y vulnerabilidades MEDIAS) las cuales deben ser revisadas y tenidas en cuenta por la organización para realizar el correcto aseguramiento de los equipos.

RESULTADOS NESSUS

IMPACTO	PLUGIN	VULNERABILIDAD	DESCRIPCIÓN	REMEDIACIÓN	DISPOSITIVOS AFECTADOS
CRITICO	125313	El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código.	El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el protocolo de escritorio remoto (RDP). Un atacante remoto no autenticado puede explotar esto, a través de una serie de solicitudes especialmente diseñadas, para ejecutar código arbitrario.	Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, 2008, 7 y 2008 R2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 7, SERVIDOR BASE DE DATOS 7
CRITICO	108797	No es soportado el sistema operativo remoto o servicie pack	La versión remota de Microsoft Windows le falta un Service Pack o ya no se admite. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualizar a un Service Pack o sistema operativo compatible	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 7, SERVIDOR DE APLICACIONES 4, SERVIDOR APLICACIONES 4, SERVIDOR BASE DE DATOS 7,

CRITICO	72091	Detección de versiones no compatibles de Adobe ColdFusion	Según su versión, la instalación de Adobe ColdFusion que se ejecuta en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualice a una versión de Adobe ColdFusion que sea compatible actualmente.	SERVIDOR DE APLICACIONES 4
CRITICO	97994	Detección de versiones no compatibles de Microsoft IIS 6.0	Según su número de versión auto informado, ya no se admite la instalación de Microsoft Internet Information Services (IIS) 6.0 en el host remoto. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualice a una versión de Microsoft IIS que sea compatible actualmente.	SERVIDOR APLICACIONES 4,

CRITICO	84729	El sistema operativo remoto ya no es compatible Microsoft Windows Server 2003	El host remoto ejecuta Microsoft Windows Server 2003. El soporte para este sistema operativo por parte de Microsoft finalizó el 14 de julio de 2015. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca los informes de vulnerabilidades.	Actualice a una versión de Windows que sea soportada actualmente.	SERVIDOR DE APLICACIONES 4
ALTO	20007	Detección de protocolos SSL versión 2 y 3	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos, incluyendo: - Un esquema de relleno inseguro con cifrados CBC. - Esquemas de renegociación y reanudación de sesiones inseguras.	Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior en su lugar.	SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVOS 5, SERVIDOR DIRECTORIO ACTIVO 5, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR DE APLICACIONES 3

			Un atacante puede explotar estos defectos para llevar a cabo ataques de tipo "man-in-the-middle" o para descifrar las comunicaciones entre el servicio afectado y los clientes.		

ALTO	97833	MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)	El host remoto de Windows se ve afectado por las siguientes vulnerabilidades: - Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente	Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también lanzó parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8. Para sistemas operativos Windows no compatibles, p. Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente	EQUIPO WINDOWS 7, SERVIDOR BASE DE DATOS 7

			diseñado, para revelar información confidencial. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits del Grupo de ecuaciones reveladas el 14/04/2017 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group.	bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.	

ALTO	100464	Vulnerabilidades múltiples de Microsoft Windows SMBv1	El host remoto de Windows tiene habilitado el Bloque de mensajes de servidor Microsoft 1.0 (SMBv1). Por lo tanto, se ve afectado por múltiples vulnerabilidades: - Existen múltiples vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para revelar información confidencial. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)	Aplique la actualización de seguridad aplicable para su versión de Windows: - Windows Server 2008 : KB4018466 - Windows 7 : KB4019264 - Windows Server 2008 R2 : KB4019264 - Windows Server 2012 : KB4019216 - Windows 8.1 / RT 8.1. : KB4019215 - Windows Server 2012 R2 : KB4019215 - Windows 10 : KB4019474 - Windows 10 Versión 1511 : KB4019473 - Windows 10 Versión 1607 : KB4019472 - Windows 10 Versión 1703 : KB4016871 - Windows Server 2016 : KB4019472	EQUIPO WINDOWS 7, SERVIDOR DE APLICACIONES 4, SERVIDOR BASE DE DATOS 7

ALTO	26920	Autenticación de sesión nula de Microsoft Windows SMB	El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión utilizando una sesión NULL (es decir, sin inicio de sesión o contraseña). Dependiendo de la configuración, puede ser posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.	Aplique los siguientes cambios en el registro según los avisos de TechNet a los que se hace referencia: Conjunto: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1 Reinicie una vez que se completen los cambios en el registro.	SERVIDOR DE APLICACIONES 4
ALTO	130208	Vulnerabilidad de denegación de servicio de Cisco Wireless LAN Controller Secure Shell (SSH) (cisco-sa-20191016-wlc-ssh-dos)	Según su versión auto informada, el controlador de LAN inalámbrica de Cisco (WLC) se ve afectado por una vulnerabilidad de denegación de servicio (DoS) en su componente Secure Shell (SSH) debido a una limpieza de proceso insuficiente. Un atacante remoto autenticado puede explotar este problema, iniciando repetidamente las	Actualice a la versión fija relevante a la que se hace referencia en el Id. De bug Cisco CSCvp34148	CONTROLADORA WI-FI,

			conexiones SSH, para agotar los recursos del sistema y hacer que el sistema deje de responder.		
ALTO	41028	Nombre de comunidad predeterminado del agente SNMP (público)	Es posible obtener el nombre de comunidad predeterminado del servidor SNMP remoto. Un atacante puede usar esta información para obtener más conocimiento sobre el host remoto o para cambiar la configuración del sistema remoto (si la comunidad predeterminada permite tales modificaciones).	Deshabilite el servicio SNMP en el host remoto si no lo usa. Filtre los paquetes UDP entrantes que van a este puerto o cambie la cadena de comunidad predeterminada.	CONTROLADORA WI-FI,
Medio	51192	El certificado SSL no es confiable	Los certificados para este servicio no están firmados por una entidad de certificación reconocida, si el host remoto es un host público en producción esto	Adquirir un certificado SSL adecuado para este servicio	FIREWALL, SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVO 5, EQUIPO WINDOWS 7, SERVIDOR DE DIRECTORIO

			anula el uso SSL ya que cualquiera podría establecer un ataque tipo "man-in-the-middle" contra el host remoto.		ACTIVO 5, SWITCH HP, CONTROLADORA WI-FI, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR DE APLICACIONES 3
Medio	57582	Certificado SSL autoafirmado	Los certificados para este servicio no están firmados por una entidad de certificación reconocida, si el host remoto es un host público en producción esto anula el uso SSL ya que cualquiera podría establecer un ataque tipo "man-in-the-middle" contra el host remoto.	Adquirir un certificado SSL adecuado para este servicio	FIREWALL, SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR DE ARCHIVO 5, EQUIPO WINDOWS 7, SERVIDOR DE DIRECTORIO ACTIVO 5, SWITCH HP, CONTROLADORA WI-FI, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR DE APLICACIONES 3.

Medio	12101 0	Detección de protocolo TLS versión 1.1	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 carece de compatibilidad con los conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticados como GCM no se pueden utilizar con TLS 1.1 A partir del 31 de marzo de 2020, los puntos de conexión que no están habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales exploradores web y los principales proveedores.	Habilitar la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.	FIREWALL, EQUIPO WINDOWS 10, SERVIDOR DE ARCHIVO 5, SERVIDOR DIRECTORIO ACTIVO 5, SWITCH HP, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR DE APLICACIONES 3.
Medio	35291	Certificado SSL firmado mediante algoritmo de hash débil	El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para	Ponerse en contacto con la entidad de certificación para que se vuelva a emitir el certificado SSL.	FIREWALL, SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVO 5, EQUIPO WINDOWS 7, CONTROLADORA WI-FI, SERVIDOR BASE DE DATOS 0

			generar otro certificado con la misma firma digital, lo que permite a un atacante hacerse pasar por el servicio afectado.		
MEDIUM	104743	Detección de protocolo TLS versión 1.0	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más recientes de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben utilizarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos de conexión que no están habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales exploradores web y los principales proveedores.	Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR DE ARCHIVO 5, EQUIPOS WINDOWS 7, SWITCH HP, CONTROLADORA WI-FI, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR DE APLICACIONES 3.

MEDIUM	184 05	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	La versión remota del servidor de protocolo de escritorio remoto (servicio terminal) es vulnerable a un ataque de intermediario (MiTM). El cliente RDP no hace ningún esfuerzo para validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico desde el servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque MiTM de esta naturaleza permitiría al atacante obtener cualquier información confidencial transmitida, incluidas las credenciales de autenticación	Forzar el uso de SSL como capa de transporte para este servicio si se admite, o y-Seleccione la opción 'Permitir conexiones solo desde equipos que ejecutan Escritorio remoto con autenticación a nivel de red' si está disponible.	SERVIDOR DE ARCHIVOS 6, SERVIDOR FTP, SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR BASE DE DATOS 7, SERVIDOR DE APLICACIONES 3.

MEDIUM	57608	No se requiere firma SMB	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para llevar a cabo ataques de tipo "man-in-the-middle" contra el servidor SMB.	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la directiva 'Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se denomina "firma del servidor".	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR FTP, SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR DE APLICACIONES 4, SERVIDOR BASO DE DATOS 7, SERVIDOR BASE DE DATOS O
MEDIUM	15901	Certificado SSL expirado	Este plugin comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha expirado	Comprar o genere un nuevo certificado SSL para reemplazar el existente.	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR BASE DE DATOS 7,

MEDIUM	58453	Servicios de Terminal Server no utiliza autenticación de nivel de red (NLA) solamente	Los servicios de Terminal Server remotos no están configurados para utilizar solamente la autenticación de nivel de red (NLA).NLA utiliza el protocolo Credential Security Support Provider (CredSSP) para realizar una autenticación de servidor segura a través de mecanismos TLS/SSL o Kerberos, que protegen contra ataques de tipo "man-in-the-middle". Además de mejorar la autenticación, NLA también ayuda a proteger el equipo remoto de usuarios y software malintencionados completando la autenticación de usuario antes de establecer una conexión RDP completa..	Habilite la autenticación de nivel de red (NLA) en el servidor RDP remoto. Esto se hace generalmente en la pestaña "Remoto" de la configuración del 'Sistema' en Windows.	SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR BASE DE DATOS 7, SERVIDOR DE APLICACIONES 3.

MEDIUM	57690	El nivel de cifrado de servicios de terminal es medio o bajo	El servicio remoto de Terminal Services no está configurado para usar criptografía sólida. El uso de criptografía débil con este servicio puede permitir que un atacante escuche las comunicaciones con mayor facilidad y obtenga capturas de pantalla y / o pulsaciones de teclas.	Cambie el nivel de cifrado RDP a uno de: 3. alto 4. Cumple con FIPS	SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR BASE DE DATOS 7, SERVIDOR DE APLICACIONES 3.
MEDIUM	104743	Detección de protocolo TLS versión 1.0	El servicio remoto acepta conexiones encriptadas usando TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas contra estos defectos y deben usarse siempre que sea posible. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con	Habilitar TLS 1.1 y 1.2 de TLS como protocolos seguros	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR DE ARCHIVO 5, SERVIDOR DIRECTORIO ACTIVO 5, SWITCH HP,

			los principales navegadores web y los principales proveedores.		
MEDIUM	42873	El servicio remoto admite el uso de cifrados SSL de potencia media	El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa el conjunto de encriptación 3DES. Tenga en cuenta que es considerablemente más fácil eludir el cifrado de fuerza media si el atacante está en la misma red física.	Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.	SERVIDOR DE ARCHIVOS 6, EQUIPO WINDOWS 10, SERVIDOR DE ARCHIVO 5, EQUIPO WINDOWS 7, SERVIDOR DE DIRECTORIO ACTIVO 5, SWITCH HP, CONTROLADORA WI-FI, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR DE APLICACIONES 3.

MEDIUM	65821	El servicio remoto admite el uso del cifrado RC4.	El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado. El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, de modo que se introduce una amplia variedad de pequeños sesgos en la secuencia, disminuyendo su aleatoriedad. Si el texto sin formato se encripta repetidamente (por ejemplo, cookies HTTP), y un atacante puede obtener muchos (por ejemplo, decenas de millones) de textos cifrados, el atacante puede derivar el texto sin formato.	Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.	SERVIDOR DE ARCHIVOS 6, EQUIPO DE WINDOWS 10, SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR DIRECTORIO ACTIVO 5, SWITCH HP, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR BASE DE DATOS 0, SERVIDOR APLICACIONES 3.
MEDIUM	26928	El servicio remoto admite el uso de cifrados SSL débiles.	El host remoto admite el uso de cifrados SSL que ofrecen cifrado débil. Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.	Vuelva a configurar la aplicación afectada, si es posible para evitar el uso de cifrados débiles.	SERVIDOR DE ARCHIVOS 6, EQUIPO DE WINDOWS 10, SWITCH HP, SERVIDOR DIRECTORIO ACTIVO 3,

MEDIUM	90510	MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD (3148527) (Badlock) (verificación sin credencial)	El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM) y de la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación sobre los canales de Llamada a procedimiento remoto (RPC). Un atacante hombre en el medio capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la disminución del nivel de autenticación, permitiendo que el atacante se haga pasar por un usuario autenticado y acceda a la base de datos SAM.	Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.	SERVIDOR DE ARCHIVOS 5, EQUIPO WINDOWS 7, SERVIDOR DE APLICACIONES 4,
MEDIUM	45411	El certificado SSL para este servicio es para un host diferente.	El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.	Compre o genere un certificado SSL adecuado para este servicio.	SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVOS 5, SERVIDOR DIRECTORIO ACTIVO 5, SERVIDOR

					DIRECTORIO ACTIVO 3,
MEDIUM	78479	SSLv3 Padding Oracle en la vulnerabilidad de cifrado heredado degradado (POODLE)	El host remoto se ve afectado por una vulnerabilidad de divulgación de información man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados usando cifrados de bloque en modo de encadenamiento de bloque de cifrado (CBC). Los atacantes MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden forzar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas.	Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que SSLv3 se pueda deshabilitar.	SERVIDOR DE ARCHIVOS 6, SERVIDOR DE ARCHIVOS 5, SERVIDOR DIRECTORIO ACTIVO 5, SERVIDOR DIRECTORIO ACTIVO 3, SERVIDOR BASE DE DATOS 7, SERVIDOR DE APLICACIONES 3.

MEDIUM	48340	Una aplicación que se ejecuta en el servidor web remoto se ve afectada por una vulnerabilidad transversal del directorio.	La versión de Adobe ColdFusion que se ejecuta en el host remoto se ve afectada por una vulnerabilidad transversal del directorio en la interfaz web administrativa. La entrada al parámetro 'locale' de varias páginas no se desinfecta correctamente. Un atacante remoto no autenticado puede explotar esto enviando solicitudes HTTP especialmente diseñadas, lo que le permite descargar archivos arbitrarios del sistema. Un atacante podría usar esto para descargar el archivo de contraseña de ColdFusion (que contiene la contraseña de administrador), obteniendo así acceso a la interfaz web administrativa. El acceso administrativo autenticado puede provocar la ejecución de código arbitrario.	Aplique la revisión a la que se hace referencia en el aviso de Adobe.	SERVIDOR DE APLICACIONES 4

MEDIUM	42263	Servidor telnet sin cifrar	El host remoto ejecuta un servidor Telnet a través de un canal sin cifrar. No se recomienda utilizar Telnet a través de un canal no cifrado, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto sin cifrar. Esto permite que un atacante remoto de intermediario escuche a escondidas una sesión de Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor.	Deshabilite el servicio Telnet y use SSH en su lugar.	SWITCH CORE
MEDIUM	97861	El servidor NTP remoto responde a las consultas del modo 6.	El servidor NTP remoto responde a las consultas del modo 6. Los dispositivos que responden a estas consultas tienen el potencial de ser utilizados en ataques de amplificación NTP. Un atacante remoto no autenticado podría explotar esto, a través de una consulta de modo 6 especialmente diseñada, para causar una condición reflejada	Restrinja las consultas del modo NTP 6.	SWITCH HP,

			de denegación de servicio.		
MEDIUM	81606	El host remoto admite un conjunto de cifrados débiles.	El host remoto admite conjuntos de cifrado EXPORT_RSA con claves menores o iguales a 512 bits. Un atacante puede factorizar un módulo RSA de 512 bits en un corto período de tiempo. Un atacante de intermediario puede degradar la sesión para usar conjuntos de cifrado EXPORT_RSA (por ejemplo, CVE-2015-0204). Por lo tanto, se recomienda eliminar el soporte para conjuntos de cifrado débiles.	Vuelva a configurar el servicio para eliminar la compatibilidad con los conjuntos de cifrado EXPORT_RSA.	SERVIDOR DE ARCHIVOS 6, SWITCH HP

MEDIUM	118461	Vulnerabilidades múltiples del controlador de LAN inalámbrica de Cisco	Según su versión auto informada, el Cisco Wireless LAN Controller (WLC) se ve afectado por las siguientes vulnerabilidades: - Una vulnerabilidad de escalada de privilegios debido al análisis incorrecto de un atributo TACACS específico. Un atacante remoto, autenticándose en TACAC a través de la GUI, podría crear una cuenta local con privilegios administrativos. (CVE-2018-0417) - Una vulnerabilidad de denegación de servicio debido a fallas con mecanismos de temporizador específicos. Un atacante remoto podría hacer que el temporizador se bloquee y provocar una condición DoS. (CVE-2018-0441)	Actualice a la versión fija relevante a la que se hace referencia en los Id. De error de Cisco CSCvf66680, CSCvh65876, CSCve64652 y CSCvf66696.	CONTROLADORA WI-FI,

MEDIUM	1243334	Cisco Wireless LAN Controller Vulnerabilidad de denegación de servicio al dispositivo le hace falta un parche de seguridad.	Cisco Wireless LAN Controller (WLC) se ve afectado por la siguiente vulnerabilidad - Una vulnerabilidad en la administración del certificado localmente significativo (LSC) para el controlador de LAN inalámbrica de Cisco (WLC) podría permitir que un atacante remoto autenticado haga que el dispositivo se reinicie inesperadamente, lo que provoca una condición de denegación de servicio (DoS). El atacante necesitaría tener credenciales de administrador válidas. La vulnerabilidad se debe a una validación de entrada incorrecta de la URL HTTP utilizada para establecer una conexión con la Autoridad de Certificación (CA) de LSC. Un atacante podría aprovechar esta vulnerabilidad autenticándose en el dispositivo objetivo y configurando un certificado LSC. Un	Actualice a la versión a la que se hace referencia en el Id. De bug Cisco CSCvj07995	CONTROLADORA WI-FI,

			exploit podría permitir al atacante causar una condición DoS debido a un reinicio inesperado del dispositivo. (CVE-2019-1830)		
MEDIUM	1 2 4 3 3 1	Cisco Wireless LAN Controller Software GUI Configuration Vulnerabilidades de denegación de servicio	Múltiples vulnerabilidades en la función de configuración administrativa de la GUI del software Cisco Wireless LAN Controller (WLC) podrían permitir que un atacante remoto autenticado haga que el dispositivo se recargue inesperadamente durante la	Actualice a la versión fija relevante a la que se hace referencia en el Id. De bug Cisco CSCvf16322	CONTROLADORA WI-FI,

			configuración del dispositivo cuando el administrador esté usando esta GUI, causando una denegación de servicio (DoS)		
MEDIUM	124332	Software de controlador de LAN inalámbrica de Cisco Vulnerabilidades de denegación de servicio de gestión de mensajes IAPP	Múltiples vulnerabilidades en el manejo de mensajes del Protocolo de punto de acceso intermedio (IAPP) por el software del controlador de LAN inalámbrica de Cisco (WLC) podrían permitir que un atacante adyacente no autenticado cause una condición de denegación de servicio (DoS)	Actualice a la versión fija relevante a la que se hace referencia en los Id. De error de Cisco CSCvh91032, CSCvh96364, CSCvi89027	CONTROLADORA WI-FI,
MEDIUM	76474	El servicio SNMP remoto se ve afectado por una vulnerabilidad que permite un ataque de denegación de servicio distribuido reflejado.	El demonio SNMP remoto responde con una gran cantidad de datos a una solicitud 'GETBULK' con un valor mayor que el normal para 'repeticiones máximas'. Un atacante remoto puede usar este servidor SNMP para realizar un ataque de denegación de	Deshabilite el servicio SNMP en el host remoto si no lo usa. De lo contrario, restrinja y monitoree el acceso a este servicio y considere cambiar la cadena de comunidad 'pública' predeterminada	CONTROLADORA WI-FI,

			servicio distribuido reflejado en un host remoto arbitrario.		
MEDIUM	90317	SSH Algoritmos débiles compatibles	Nessus ha detectado que el servidor SSH remoto está configurado para usar el cifrado de flujo Arcfour o ningún cifrado. RFC 4253 desaconseja el uso de Arcfour debido a un problema con claves débiles.	Póngase en contacto con el proveedor o consulte la documentación del producto para eliminar las cifrados débiles.	CONTROLADORA WI-FI,

12. Discusión

Teniendo en cuenta el levantamiento de información realizado en la empresa del sector industrial y el análisis generado de dicha información acompañado de las herramientas de identificación de vulnerabilidades se generan una serie de recomendaciones y buenas prácticas mencionadas en este documento para mejorar los estándares de seguridad informática en la infraestructura analizada.

Para lograr un buen nivel de aseguramiento en la infraestructura no solo se deben enfocar en los dispositivos, esto debe acompañarse de procesos y procedimientos que apunten a la seguridad de manera integral en la organización.

Es importante que el personal que administra la infraestructura se encuentre capacitado en temas de ciberseguridad y consciente de la responsabilidad del manejo de la información. Encontrarse actualizado en esta temática de seguridad permite establecer tareas que prevengan posibles amenazas minimizando los riesgos asociados y la utilización de los sistemas de forma no autorizada y en general mal intencionada.
La adopción de medidas adecuadas de ciberseguridad ayuda a la organización a cumplir sus objetivos, permite proteger los recursos financieros, sistemas de información, reputación, situación legal, y otros bienes tangibles e intangibles.

12.1 Recomendaciones

Las vulnerabilidades encontradas generan amenazas que pueden ser aprovechadas por actores malintencionados y llegar a terminar materializando riesgos potenciales; de esta forma las recomendaciones que se entregaran a continuación tienen la intención de mitigar las amenazas a las cuales se ve enfrentada la compañía lo cual podría implicar una pérdida o fuga de información, indisponibilidad de servicio parcial o total a nivel de conectividad o de sus plataformas, páginas web y que su planta de producción se vea afectada. Todo esto lleva a perdidas monetarias para la empresa.

- Es recomendable fortalecer el uso de contraseñas utilizando contraseñas no menores a 12 caracteres alfanuméricos y que no tengan relación con datos personales.
- Se encuentran sistemas operativos Windows desactualizados y fuera de soporte no se cuenta con un proceso que controle dichas actualizaciones a continuación las recomendaciones de actualización sobre estos sistemas:

DESCRIPCION	TIPO	SISTEMA OPERATIVO ACTUAL	SISTEMA OPERATIVO RECOMENDADO	SOPORTE ESTANDAR	SOPORTE EXTENDIDO
SERVIDOR DE ARCHIVOS 6	Servidor	Windows Server 2008 Estándar 32 Bits	Windows Server 2016 o 2019	Sin soporte ni actualizaciones Microsoft	Sin soporte ni actualizaciones Microsoft
SERVIDOR FTP	Servidor	Windows Server 2012 R2 Estándar	Windows Server 2016 o 2019	Vencido	Hasta 2023
SERVIDOR DE ARCHIVOS 5	Servidor	Windows Server 2012 R2 Estándar	Windows Server 2016 o 2019	Vencido	Hasta 2023
SERVIDOR APLICACIONES 4	Servidor	Windows Server 2003 R2 Estándar	Windows Server 2016 o 2019	Sin soporte ni actualizaciones Microsoft	Sin soporte ni actualizaciones Microsoft
SERVIDOR DIRECTORIO ACTIVO 5	Servidor	Windows Server 2012 R2 Estándar	Windows Server 2016 o 2019	Vencido	Hasta 2023
SERVIDOR DIRECTORIO ACTIVO 3	Servidor	Windows Server 2012 R2 Estándar	Windows Server 2016 o 2019	Vencido	Hasta 2023
SERVIDOR BASE DE DATOS 7	Servidor	Windows Server 2008 R2 Enterprise	Windows Server 2016 o 2019	Sin soporte ni actualizaciones Microsoft	Sin soporte ni actualizaciones Microsoft
SERVIDOR DE BASE DE DATOS 0	Servidor	Windows Server 2016 Estándar	-	Hasta 2022	Hasta 2027
SERVIDOR DE APLICACIONES 3	Servidor	Windows Server 2012 R2 Estándar	Windows Server 2016 o 2019	Vencido	Hasta 2023
EQUIPO WINDOWS 7	Equipo cliente	Windows 7 Profesional	Windows 10 Profesional	Sin soporte ni actualizaciones Microsoft	Sin soporte ni actualizaciones Microsoft
EQUIPO WINDOWS 10	Equipo cliente	Windows 10 Profesional	-	Hasta 2021	Hasta 2022

Tabla 4: Versiones de Sistemas Operativos

- Generar un procedimiento de actualizaciones de sistemas operativos que realice un control continuo de los últimos parches y sistemas operativos liberados, ya que se identificó vulnerabilidades múltiples en varios dispositivos en Microsoft Service Message Block (Eternal Blue) que permiten que un atacante no identificado pueda explotar estas vulnerabilidades a través de paquetes especialmente diseñados posibilitando la divulgación de información sensible los dispositivos afectados son : **Equipo Windows 7, Servidor de Aplicaciones 4, Servidor de Base de Datos 7.**

- Implementar el despliegue de una herramienta como Wsus que permite administrar los parches liberados y desplegar actualizaciones controladas automáticamente.

- Se encuentran versiones de software no soportados por fabricantes como adobe cold fusión en el **SERVIDOR DE APLICACIONES 4** es necesario actualizar este software a una versión soportada.

- Verificar que todo recurso compartido en red este atado a un medio de autenticación para su acceso utilizando el controlador de dominio ya que se identificó accesos abiertos a los recursos en el **SERVIDOR DE APLICACIONES 4.**

- Se identifican varios equipos con vulnerabilidad de ejecución remota de código en el protocolo de escritorio remoto RDP se recomienda aplicar parches mencionados en el anexo de Vulnerabilidades Nessus los equipos afectados son: **Servidor de Archivos 6, Equipo Windows 7 y Servidor Base de Datos 7.**

- Se encuentra servicio web IIS 6.0 en el **SERVIDOR DE APLICACIONES 4** este producto está fuera de soporte se recomienda actualizar a IIS 10.

- Se identifica que varios de los elementos analizados manejas certificados SSL 2.0 y 3.0 se recomienda que todos estos dispositivos se deshabiliten SSL 2.0 y 3.0 y se habilite certificados TLS 1.2. o TLS 1.3 los cuales manejan protocolos de encripción y cifrado más robustos que aseguran el flujo de información sobre los sitios web validar los equipos identificados con esta vulnerabilidad en Anexo de vulnerabilidades de Nessus.

- Se evidencia que los certificados SSL no son confiables no están firmados por una entidad de certificación reconocida si los host son de acceso público esto deshabilita completamente el uso de SSL ya que permite un ataque tipo " man-in-the-middle" se recomienda adquirir un certificado adecuado para estos componentes

- Se entrega una modelo de plantilla de seguridad para Windows Server 2016 en la cual se mencionan una serie de controles que se recomienda aplicar en los servidores. (Ver Anexo.15.3)

- Los dispositivos de red como lo es (**Switches, Controladora Wi-Fi, Switch Core y Firewall**) se encuentran por debajo de varias versiones de firmware por lo cual recomendamos en la siguiente tabla la actualización a últimas versiones estables.

EQUIPO	FIRMWARE ACTUAL	FIRMWARE RECOMENDADO	FECHA DE LIBERACION	ESTADO
Controladora Cisco	8.2.151.0	8.5.161	20-feb-20	Desactualizado
Firewall	6.5.2.3-4n	6.5.4.6-79n	29-may-20	Desactualizado
Switch HP 5130	5130_EI_7.10.R3208P03	5130_EI_7.10_R3506P02	14-ene-20	Desactualizado
Switch DELL N1500	6.6.0.2	6.6.0.2	3-jun-19	Actualizado
Switch Core DELL N4000	6.5.2.18	6.5.6.3	22-mar-19	Desactualizado

Tabla 5: Versiones de Firmware Dispositivos De Red

- Dentro del análisis recolectadas a los dispositivos de red se evidencia que está habilitado el acceso a los dispositivos por los puertos y protocolos Telnet, HTTP y SMTP v1 por lo cual se recomienda deshabilitarlos y habilitar el acceso por SSH, HTTPS y protocolo SMTP v2 y/o v3.

- Durante el levantamiento de información preliminar se evidencia que existen varios SSID publicados con el nombre de la empresa por lo cual es recomendable que sea cambiado el nombre de la red Wi-Fi para evitar ataques dirigidos.

- Realizar el cambio de la autenticación WEP por WPA2 de los SSID que lo tienen habilitado, ya que son las redes supremamente vulnerables en la actualidad.

- Implementar y habilitar la autenticación por RADIUS con el fin de controlar el acceso a la red.

- Se evidencia que los puestos que se encuentran en sitos de acceso a público general o que no estén en uso sean deshabilitados.

- Para la administración de los dispositivos se recomienda generar listas de acceso con el fin de que solo puedan accederse desde una red o equipo en específico.

- Con el fin de garantizar una administración más centralizada y un mejor control ir generando una unificación de marcas en cuanto a Switches, dispositivos inalámbricos y demás equipos de red.

- Se entrega un modelo de plantilla de aseguramiento de Switches el cual puede ser utilizado en los dispositivos actuales y próximas adquisiciones dependiendo de las particularidades de configuración o marcas según la necesidad de la empresa.

- Es de vital importancia eliminar cualquier tipo de dispositivo que realice extensiones de la red LAN y WLAN no controlados que afecten el rendimiento del tráfico de red en general como lo son (Hub y Routers no corporativo o de uso casero).

- Generar control y restricción de conexiones de dispositivos que sean de uso personal a través de bloqueo de dirección Mac.

- Teniendo en cuenta las bondades que ofrece la herramienta de vulnerabilidades Nessus utilizada en este proyecto la empresa tiene la libertad de adquirirla para realizar un control continuo de sus estándares de seguridad informática, se anexa cotización del valor de la Herramienta.

- Con la cantidad de dispositivos que tiene la empresa estarían en la necesidad de realizar un despliegue de una herramienta de monitoreo que le permita tener una mayor visibilidad de la disponibilidad de la infraestructura para lo cual se genera un prototipo de monitoreo utilizando la herramienta ZABBIX la cual es Gratuita.

12.2 Buenas Practicas

- Se recomienda utilizar como referencia los estándares de ciberseguridad proporcionados por la norma ISO 27000 Versión 2013 como guía de aseguramiento de la información; se recomienda aplicar solo los controles que sean requeridos o necesarios por la empresa, no es obligatorio aplicar todos los controles.

    - ISO 27001 - Norma principal de toda la serie ya que incluye todos los requisitos del Sistema de Gestión de Seguridad de la Información en las organizaciones.
    - ISO 27002 - Manual de buenas prácticas en la que se describen los objetivos de control y las evaluaciones recomendables en cuanto a la seguridad de la información.
    - ISO 27003 - Manual para implementar un Sistema de Gestión de Seguridad de la Información.
    - ISO 27004 - Técnicas de medida y las métricas que son aplicables a la determinación de la eficacia de un Sistema de Gestión de Seguridad de la Información y los controles relacionados.
    - ISO 27005 – Norma que establece las diferentes directrices para la gestión de los Riesgos en la Seguridad de la Información.
    - ISO 27006 - Estándar que específica todos los requisitos para lograr la acreditación de las entidades de auditoría y certificación de Sistema de Gestión de Seguridad de la Información.
    - ISO 27007 - Manual de auditoría de un Sistema de Gestión de Seguridad de la Información.
    - ISO 27011 - Guía de gestión de seguridad de la información específica para telecomunicaciones
    - ISO 27031 - Guía de continuidad de negocio basada en las tecnologías de la información y las comunicaciones
    - ISO 27032 - Texto relativo a la ciber-seguridad.
    - ISO 27799 - Estándar de Gestión de Seguridad de la Información dentro del sector sanitario.
    - ISO 27033 -Norma da una visión general de seguridad de la red y de los conceptos asociados

  - ISO 37034 - Guía de seguridad en aplicaciones.

- Se recomienda tomar como referencia el uso de buenas prácticas de ITIL Versión 4

- Se sugiere guiarse con las recomendaciones proporcionadas por cada fabricante de dispositivos de red (Hewlett Packard, Dell, Sonic Wall y Cisco) en cuanto a configuraciones y prácticas de aseguramiento.

13. Conclusiones

Teniendo en cuenta los resultados obtenidos a través del levantamiento de información se logra generar un inventario de los dispositivos de red e infraestructura tecnológica de la compañía para identificar su grado de criticidad

Del análisis de vulnerabilidades se obtiene información de gran importancia que permite establecer un plan de mitigación.

Con la evaluación de los componentes críticos de la compañía se logra identificar, analizar y evaluar el nivel de aseguramiento de la infraestructura permitiendo entregar una serie de recomendaciones y buenas prácticas en pro de mejorar la disponibilidad, integridad y confidencialidad de la empresa.

No se cuenta con información que presente estadísticas de disponibilidad de los equipos en la red por lo cual la implementación del prototipo de sistema de monitoreo permite optimizar el tiempo de respuesta ante la caída de uno de estos dispositivos o plataformas y la monitorización y estadísticas que se requieran.

El no contar con procedimientos de aseguramiento y herramientas de análisis de seguridad en conjunto con tener sistemas operativos y firmware desactualizados genera brechas de seguridad que ponen en riesgo los sistemas de información y plataforma tecnológica de la

compañía del sector industrial.

14. Documentación de Referencia

Bibliografía

Cisco – 1920 - Guía de Buenas Prácticas en Seguridad de Cisco Systems
https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/160-guia-de-buenas-practicas-en-

Isotools – 2015 - Norma Iso 27000 Version 2013

https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

Mintic – 2016 – Articulo Guía para la Implementación de Seguridad de la Información en una MIPYME

https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Universidad Estatal del Sur de Manabi, Autores: Martha Irene Romero Castro, Grace Liliana Figueroa Moràn, Denisse Soraya Vera Navarrete, José Efraín Álava Cruzatty, Galo Roberto Parrales Anzúles, Christian José Álava Mero, Ángel Leonardo Murillo Quimiz, Miriam Adriana Castillo Merino – 2018 - Introducción A La Seguridad Informática Y El Análisis De Vulnerabilidades

https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Instituto Nacional de Ciberseguridad – 2014 – Decálogo de Buenas Practicas de Seguridad

https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-departamento-informatica

Acronis - Alexey Sotnikov – 2019 - Las 10 mejores herramientas para monitorizar

https://www.acronis.com/es-es/articles/monitoring-tools/

Tenable Nessus – 2019 - Web Oficial Herramienta Nessus

https://es-la.tenable.com/products/nessus

Gartner – 2019 - Gartner Nagios Vs Zabbix

https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools/compare/nagios-vs-zabbix

Telemática y educación: expectativas y desafíos Jesus Salinas 1997

http://www.lmi.ub.es/te/any96/salinas_chile/

La ventaja de mover primero en la industria: Valor empresarial con fábricas digitales - Mckinsey & Company - 2020

https://www.mckinsey.com/business-functions/operations/our-insights/industrys-fast-mover-advantage-enterprise-value-from-digital-factories/es-es#

15. Anexos

- Anexo 1: Acta De Calificación Y Aprobación De Trabajo De Grado
- Anexo 2: Carta Presentación Estudiantes PGC-F1
- Anexo 3: Carta Aceptación Propuesta De Proyecto De Grado PGC-F2
- Anexo 4: Carta Aprobación Del Trabajo De Grado PGC-F3
- Anexo 5: Carta Sobre Derechos De Autor PGC-F5
- Anexo 6: Plantilla de Aseguramiento de Switch
- Anexo 7: Plantilla de Aseguramiento de Servidores
- Anexo 8: Carta de Recomendaciones de Seguridad
- Anexo 9: Prototipo de Sistema De Monitoreo Zabbix
- Anexo 10: Cotización Herramienta Nessus
- Anexo 11: Reporte Nmap de Escaneo de Puertos
- Anexo 12: Reporte General Nessus de Vulnerabilidades
- Anexo 13: Reporte Nessus de Vulnerabilidades por Plugin