DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO A LA RED DE DATOS DE ENTIDAD PRESTADORA DEL SERVICIO DE SALUD.

JADIT GUERRERO MOLINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2020

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO A LA RED DE DATOS DE ENTIDAD PRESTADORA DEL SERVICIO DE SALUD.

JADIT GUERRERO MOLINA

Trabajo de grado para optar el título de
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2020

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado.

_____
Firma del jurado

_____
Firma del jurado

Dedicatoria:

En primer lugar, agradezco al Dios todopoderoso por concederme la sabiduría y el privilegio de poder culminar este Posgrado, por acompañarme en los momentos de lucidez y dificultad. A mis padres, a mi Esposa y a mis Hijos, por estar ahí siempre dándome ánimo para no desmayar, enseñándome que se debe ser perseverante para lograr los objetivos que nos proponemos en la vida. También agradecer de una Manera Especial a los tutores, asesores, por su contribución y orientación para alcanzar este objetivo. A la Empresa donde laboro por su apoyo en la realización del proyecto

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

RESUMEN.

El presente proyecto, describe la importancia de mantener la información de las organizaciones protegidas bajo sistemas de monitorización, previniendo así ataques y robo de uno de los principales activos de las empresas, y desde allí proteger los datos de los usuarios y clientes. Es evidente, que muchas organizaciones estatales y privadas, no tienen sistemas eficaces que permitan manejar y/o manipular de manera organizada y segura los datos ofrecidos o recogidos de sus usuarios y clientes; siendo esté uno de los principales factores de riesgo que presentan las organizaciones en la actualidad.

La necesidad de monitorizar y proteger la información nace al evidenciar algunas deficiencias que presenta el sistema que almacena las bases de datos de los usuarios de un hospital estatal (Colombia), donde en ciertas ocasiones ha habido pérdida de información, y mala disposición a nivel organizativo de los datos, no cuenta con un sistema que supervise el tráfico en la red, en algunas oportunidades hay saturación en la red de datos. Es por eso que este proyecto está enfocado en mejorar y salvaguardar la información que se transmite en la red.

ABSTRACT

The present investigation describes the importance of keeping the information of protected organizations under monitoring systems, thus preventing attacks and theft of one of the main assets of the companies, and from there protecting the data of users and customers. It is evident that many state and private organizations do not have effective systems that allow to handle and / or manipulate in an organized and safe way the data offered or collected from their users and clients; being one of the main risk factors that organizations presently present.

The need to monitor and protect the information is born by evidencing some deficiencies presented by the system that stores the databases of the users of a state hospital (Colombia), where on certain occasions there has been loss of information, and poor disposition at the organizational level of the data, it does not have a system that monitors the traffic on the network, sometimes there is saturation in the data network. That is why this project is focused on improving and safeguarding the information transmitted on the network.

INTRODUCCIÓN.

Mantener la información segura ha sido el compromiso más importante que han asumido las organizaciones de los diferentes sectores económicos, ya que está se ha convertido en un activo importante de las organizaciones en la era digital; de igual manera aún existen empresas que conociendo la exposición a la que se ven expuestos sus activos tecnológicos no han tomado medidas pertinentes que mitiguen el riesgo. La mayoría de las organizaciones no cuentan con un sistema de gestión de seguridad de la información, que preserve y garantice un idóneo manejo de este activo, exponiendo de manera exponencial a los usuarios y/o clientes y a las organizaciones a procesos legales.

El desarrollo y ejecución de un sistema de monitoreo de una red de información que adquiere y posee una organización y en este caso el hospital está enmarcado en la norma ISO/IEC 27001 basado en la metodología de Sistemas de detención de Intruso (en adelante IDS), que busca optimizar los procesos de protección de datos, pretende determinar e identificar posibles amenazas y elementos de naturaleza hostil a los que se encuentran expuestos los datos de una empresa prestadora del servicio de salud, para determinar controles que le permitan a la organización tomar medidas de seguridad y evitar pérdidas de información.

Para la realización del presente proyecto aplicado, es necesario traer a colación la siguiente información; la institución cuenta con dos estaciones de trabajo una ubicada en el barrio Olaya del mismo municipio, la cual está conectada a través de radio enlace y la otra ubicada en la Ciudad de Cartagena conectada a través de *Virtual Private Networ* o Red Privada Virtual según su traducción al español (en adelante VPN). El análisis de la situación actual de la organización, señala que los proveedores del software con los que cuenta actualmente, se conectan a través de escritorio remoto, VPN o a través del software informático llamdo TEAMWIEVER, cuando se presenta algún tipo de inconveniente.

La organización maneja a gran escala información delicada y detallada en la gestión normal operativa. A pesar de la gran cantidad de información que se almacena en la empresa, se evidencia que no cumple con los protocolos básicos de seguridad de la información; la confidencialidad, integridad y disponibilidad. El presente proyecto busca reducir la actividad hostil que afecta al sistema de infraestructura informático en la empresa de salud, a través del diseño de un sistema de monitoreo que mitigue los riesgos y proteja la información que se almacena. Una de las

principales finalidades del presente proyecto es implementar de manera conveniente y óptima un sistema de monitoreo de red de datos, generando seguridad en la infraestructura informática de la empresa, que minimice cualquier tipo de riesgo referente al acceso de información por parte de personas inescrupulosas o no autorizadas para su propio interés incurriendo en faltas hacía la ley de HABEAS DATA.

1. DEFINICIÓN DEL PROBLEMA

El presente proyecto describe en detalle el proceso de diseño de la ruta de implementación del sistema de monitoreo y control, describiendo a nivel teórico - práctico los beneficios alcanzados con la puesta en marcha del mismo, con el fin de construir indicadores de gestión que garanticen un adecuado funcionamiento e identifiquen las vulnerabilidades existentes en la red de la Empresa Prestadora de Salud. El diseño, desarrollo y ejecución del proyecto se realizará en un periodo determinado en seis meses (180 días). De acuerdo a lo anterior, surge la siguiente pregunta que orienta al proyecto: ¿De qué manera la Entidad Prestadora del Servicio de Salud puede conocer estadísticas de tráfico y seguridad de su red de datos?

1.1 JUSTIFICACIÓN

El mundo actualmente se enfrenta a diversos ataques informáticos que atentan contra la integridad de la información de organizaciones gubernamentales y privadas, entonces, es necesario tomar medidas de control que salvaguarden la información y las redes. La información se ha convertido en un activo esencial de las organizaciones, por eso es imprescindible implementar controles rigurosos que permitan proteger la infraestructura tecnológica de la empresa y la seguridad de los datos, que optimicen la disponibilidad, accesibilidad, veracidad, confiabilidad e integridad de la red de datos y la información presente en esta, desde procesos de gestión de calidad.

La Empresa Prestadora del Servicio de Salud, donde se diseñará y ejecutará el siguiente proyecto, no cuenta aún con políticas, controles y protocolos de seguridad que mitiguen y minimicen los riesgos de amenazas informáticas que puedan incidir

en el adecuado manejo de la información de los usuarios. Por este motivo es necesaria la implementación de un sistema de monitoreo y control, basado en la ISO 2700; esta es la norma que estructura el diseño de métodos, sistemas que permitan implementar medidas de seguridad a nivel informático que generen confianza para los usuarios y las organizaciones.

El siguiente proyecto está centrado en diseñar una ruta de implementación para mitigar los riesgos por medio de protocolos de seguridad a los que está expuesta la red informática que a groso modo es la que permite por medio de una serie de dispositivos tecnológicos estar interconectados entre sí para intercambiar información y compartir recursos.

1.2 OBJETIVOS

1.2.1 Objetivo general.

Diseñar la ruta de implementación del sistema de monitoreo del tráfico de la red de datos de una Empresa Prestadora de Servicio para garantizar la integridad de la información enviada, implementando protocolos de seguridad y control, según las recomendaciones de la norma ISO/IEC 27001:2013.

1.2.2 Objetivos específicos.

- Identificar los activos de información que interactúan con la red de datos de la Empresa Prestadora de Servicio.

- Diagramar la red de datos actual de la Empresa Prestadora de Servicios de Salud.

- Exponer, los riesgos y amenzas que se pueden presentar en el sistema informático de la Empresa Prestadora del Servicio de Salud.

- Implementacion de un Sistema de Monitoreo.

- Diseñar, medidas y protocolos para proteger el sistema la red de datos de la Empresa Prestadora de Servicio de Salud, según las recomendaciones de la Norma.

1.3 ALCANCES Y LIMITACIONES

Diseñar y elaborar una ruta de implementación donde se especifique los procedimientos para salvaguardar la red de datos de acuerdo a los riesgos de vulnerabilidad encontrados en el tráfico de la información que se almacena localmente en un programa que asocia la información, para su posterior análisis y de allí tomar decisiones. Esta herramienta es conocida como PANDORA FMS. El proyecto se aplicará de manera específica sobre el área de infraestructura informática de la organización de salud. La implementación del sistema de monitoreo iniciará durante el segundo semestre del 2019, en un periodo de tiempo de tres meses

2. MARCO REFERENCIAL.

2.1 MARCO TEORICO.

Durante los orígenes de la era de la información, las redes de datos eran consideradas como un insumo simple; como tecnologías de bajo impacto, a raíz de que no eran tomadas como un elemento fundamental de las empresas y organizacione, al trasegar el tiempo las organizaciones fueron implementados en sus diferentes sistemas de gestión las redes de información, para almacenar información valiosa y sensible de sus diferentes procesos y operaciones; el monitoreo de seguridad de red en las organizaciones se convirtió en una tarea vital en el momento de detectar ataques de malware y problemas en la red. Al analizar los eventos de seguridad se puede dar una pronta respuesta ante amenazas y así de proteger los activos de información. Junco & Rabelo afirma que:

> La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar su comportamiento mediante el análisis y recolección de tráfico. En el presente trabajo se aborda el monitoreo de redes, describiendo los diferentes enfoques y técnicas que se deben tener en consideración para implementar este servicio, los elementos a tomar en cuenta en un esquema de monitoreo, así como un resumen de algunas herramientas para su implementación[1].

El monitoreo de redes en las Empresas Prestadoras de Salud, es tal vez, la actividad que menos se desarrolla, en parte por la escasez de recursos, la ausencia de sistemas de información que permitan soportar dicha tarea y ¿por qué no?, por la falta de una cultura preventiva. ISO/IEC 27001:2013, es una de las principales normas a nivel mundial emitida por la Organización Internacional de Normalización que describe cómo desarrollar la seguridad de la información en las empresas; muchas organizaciones han certificado su cumplimiento y eficacia.

Ejecutar procesos preventivos, es sin duda alguna un desarrollo que se debe hacer constantemente, es concebir la idea de que los proyectos (en este caso de implementación de un sistema de monitoreo de red) no finaliza al ejecutar las

[1] JUNCO ROMERO, Gerarod; RABELO PADUA Sonia. Los recursos de red y su Monitoreo. Cuba: Revista Cubana de Informática Cubana Médica, 2018. p. 76

estrategias planteadas tras distribuir los recursos financieros destinados a un proyecto, sino que por el contrario, un análisis de los resultados de dicha implementación son insumos que permiten retroalimentar, trasformar, mejorar y optimizar el funcionamiento del sistema de monitoreo de red. De acuerdo a lo anterior, desarrollar un diagnostico preventivo en las organizaciones, permite replantear y reestructurar las políticas del Sistema de Monitoreo en atención a los problemas que se pueden presentar en un futuro en la red, es decir, procesos de evaluación, monitorización y control de los sistemas informáticos. Por su parte Junco & Rabelo señalan que: "el proceso de monitorización testea continuamente la red con el fin de encontrar problemas causados por cualquier tipo de factores; si encuentra algún tipo de fallo, el sistema notificará al administrador, de tal manera que se pueda actuar eficazmente ante el evento"[2].

La finalidad del presente proyecto; es que la entidad prestadora del servicio de salud donde se implementará la prueba piloto, tenga un Sistema de Monitorización de la Red, que le permita tener una administración segura de sus datos y demás activos de manera completa e íntegra. Para ello, es necesario diseñar y establecer una ruta de implementación de procedimientos que potencie los procesos de retroalimentación de la organización desde el monitoreo y su respectiva gestión, permitiendo configurar, evaluar, analizar y controlar los recursos destinados.

Los indicadores de gestión que se formulen del presente proyecto, permitirán mantener niveles de trabajo y de servicio adecuados, conforme a las políticas y objetivos planteados por la alta gerencia, dado que del buen funcionamiento de la red dependerá de que se pueda controlar la vulnerabilidad de acceso no autorizados y la confidencialidad de los datos. Junco & Rabelo[3] señalan que este control se puede realizar por medio de métricas; en las redes de información estas métricas son conocidas como alarmas, que sencillamente lo que buscan es identificar patrones anómalos al interior de una red de datos; las alarmas más utilizadas comúnmente son las alarmas de procesamiento, alarmas de conectividad, alarmas ambientales, alarmas de utilización y alarmas de disponibilidad.

De este modo, el monitoreo de redes en las organizaciones es muy importante, ya que permite regular la organización y su infraestructura informática y brinda más autonomía al Departamento de Tecnología de la Información TI, detectando con facilidad la vulnerabilidad presente en la red de datos, desarrollando controles oportunos en tiempo real e implementar políticas estándares de gestión de calidad. La revista Celsia en su documento Política de Tecnologías de Información y

[2] Ibid. p. 77
[3] Ibid. p. 79

comunicación TIC, señala que “Cuando un área requiera implementar software, plataforma tecnológica o sistemas de información, debe diligenciar el respectivo formato de requerimientos y asignar a una persona responsable para liderar la implementación solicitada” [4], siendo este un ejemplo macro del orden que establece el Departamento de Tecnología e Informática sobre los procesos informáticos de las organizaciones.

2.1.1 Infraestructura de red.

Znet it solutions[5], señala que la infraestructura de red está constituida por elementos esenciales e importantes para cualquier institución u organización pública o privada (empresa, oficinas) que precise todos o algunos de los siguientes servicios de telecomunicaciones: teléfono, computadores, escáner, impresoras, cámaras de control y vigilancia, control de accesos, datafonos, etcétera, de esta manera, una red Informativa hace referencia a un conjunto de nodos y dispositivos informáticos conectados entre sí por algún medio de transmisión; cable coaxial, cable *Unshielded Twisted Pair* (en adelante UTP) o traducido al español cable par trenzado no blindado, fibra óptica u ondas de radio, con el objetivo de transmitir datos y compartir recursos e información, se clasifican según su alcance. Son diferentes los equipos implementados para lograr dicho fin, a continuación, se explicarán las diferentes y existentes topologías tipificadas en el diseño e implementación de una infraestructura de red.

2.1.1.1 Topología en bus.

La topología de bus permite que los dispositivos estén conectados por un único canal físico, normalmente es un cable (Backbone). La implementación de este tipo de red es efectiva por medio de un cable coaxial, el cual transmite y distribuye. La Topología en Bus es la forma más sencilla, común y económica de implementar una red. Sin embargo, esta topología es poco confiable, porque si una de las conexiones falla afectara toda la red. La topología de red en bus es multipunto, en ese orden el rendimiento de la red se verá afectada por el número de nodos conectados al backbone. Un cable actúa como una red troncal que interconecta todos los ordenadores en la red, se coloca un terminador, en los extremos del cable para evitar el eco o el rebote de la señal, según lo señalado por Cisco Networking Academy Program [6]. En la figura 1. se detalla el funcionamiento de la red.

---

[4] CELSIA. Política de Tecnologías de información y Comunicación TIC. 2013. p. 3
[5] ZNET IT SOLUTIONS. Infrastructura y redes. s,f. Blog
[6] Cisco Networking Academy Program. 2003. p. 13

Figura 1.Topología de una red Bus.

Fuente: Topologías de Red. Página web. Recuperado de: https://sites.google.com/site/wikitopored/topologias-fisicas/ventajas-y-desventajas

2.1.1.2 Topología en estrella.

Cisco Networking Academy Program[7] señala que la característica de esta topología radica en que los dispositivos se conectan a un punto central, que puede ser un switch, Hub, entre otros, las redes con topología en estrella son mucho más fiables que las redes de topología en Bus, ya que si un nodo se avería no afectara a la red ya que todos los nodos funcionan de manera independiente, siendo el swicth el que distribuye la "señal". De igual manera la topología en estrella permite agrupar los recursos y la gestión, cabe anotar que si el switch o el hub presenta fallas la comunicación entre los equipos de la red se vería interrumpida. Para la implementación de este tipo de redes se usa como medio de transmisión cable par trenzado (UTP, STP, FTP). Las redes de Topología de Estrella necesitan de un hardware adicional para su completo funcionamiento. Ver Figura 2.

[7] Ibid. p. 15.

Figura 2. Topología de una red Estrella.

Fuente: Revisión de Topología. Página Web, 2012. Recuperado de: https://www.google.com.co/search?q=imagenes+de+topologia+de+estrella

2.1.1.4 Topología en árbol.

Cisco Networking Academy Program[8], señala que a diferencia de la Topología de estrella, los dispositivos no están conectados a un comunicador central; los dispositivos en la topología de árbol están conectados a un concentrador central que controla el tráfico de la red, no es necesario que estos nodos estén conectados de manera directa al concentrador central; los equipos se conectan a un enlace físico secundario que, a su vez, se conecta al concentrador central. Un concentrador activo contiene un repetidor, es decir, un dispositivo hardware que regenera la señal recibida antes de transmitirla de igual manera la red en árbol, jerarquiza los elementos que constituyen la topología, según la agrupación de nodos e importancia. Tal como se evidencia en la figura 3

[8] Ibid. p. 16

Figura 3. Topología red árbol.

Fuente: Paz & Silva. Topología de Red. Página Web. Recuperado de: https://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml

2.1.1.4 Topología en anillo.

En una red con Topología en Anillo cada nodo tiene un puente de conexión punto a punto solo con los equipos que se encuentran alrededor de este, la señal pasa a lo largo del anillo de manera unidireccional, siendo su destino un nodo determinado para dicho fin, lo cual exime el uso del terminador. Una de las desventajas presentadas en esta topología es la unidireccionalidad ya que cualquier anomalía presente en la estructura inhabilitaría toda la red, no habría conexión en ningún dispositivo. En la figura 4 se observa el funcionamiento de está.

Figura 4.Topología de una red de anillo.

Fuente: Paz & Silva. Topología de Red. Página Web. Recuperado de: https://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml

2.1.1.5 Topología en malla.

Es una topología en la que cada dispositivo está conectado a todos los nodos, siendo esta su principal característica, permite llevar los mensajes de un dispositivo a otro por diversas rutas. Entonces, al estar la red conectada adecuadamente, la posibilidad de alguna interrupción es mínima en cuanto a comunicación. Cada servidor es independiente en su conexión con todos los demás nodos. Para brindar un funcionamiento óptimo en los diferentes enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S). Figura 5.

Figura 5. Topología de una red en malla.

Fuente: Paz & Silva. Topología de Red. Página Web. Recuperado de: https://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml

2.1.2 Tipos de red.

Una red es la unión de dispositivos conectados entre sí. Gorgona[9], afirma que este tipo de conexión se lleva a cabo por medio de cables, ondas, señales, dispositivos, entre otros, cuya finalidad es compartir recursos e información entre usuarios, por medio de una red ya definida. A continuación, se describirán las características más importantes de los diferentes tipos de redes que existen.

[9] GORGONA, Luis. Teoría de Redes de Computadoras. p. 6.

2.1.2.1 Red de área local (en adelante LAN).

Es la unión de nodos y periféricos que se encuentran en un mismo espacio geo referencial (menor de 1 Km), o en un solo edificio mediante una red, generalmente implementan tecnología similar. La comunicación o la trasmisión de señales se da por medio de cables (telefónico, coaxial o fibra óptica). Tanenbaum & Wetherall[10] nutren el concepto anterior, afirmando que la red de área local posee características, como, que cada dispositivo tiene un modem que le sirve para establecer comunicación con otros dispositivos, tiene un protocolo estándar de naturaleza inalámbrica conocido como IEEE 802.11 o WIFI. De esta manera, si la Red es alámbrica, la transmisión se realiza normalmente por cables de cobre o fibra óptica, la mayoría de sus topologías están definidas por la conexión punto a punto, en ese orden, cada nodo se comunica mediante el protocolo Ethernet, que a su misma vez se comunica con un switch con un enlace punto a punto.

La red LAN, puede estar constituida por tan sólo dos o tres computadoras que se encuentran conectadas con el objetivo de compartir información y servicios, o también puede incluir una cantidad determinada de computadoras de diferentes tipos, es una de las redes más utilizadas en instalaciones para hogar. Sus principales ventajas y desventajas se enuncian a continuación y en la figura 6 se describe su proceso:

Ventajas

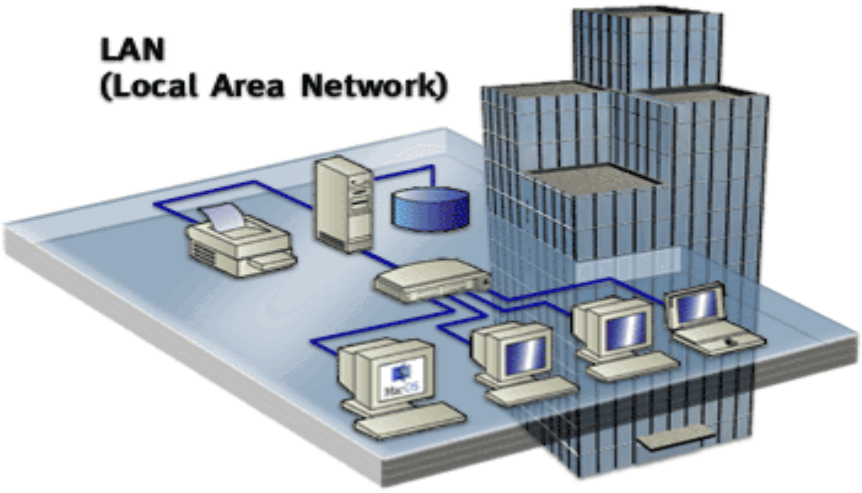
- El margen de error es mínimo, porque son redes que se caracterizan por ser seguras.
- Cada usuario posee su propio canal.
- Hay enlaces de alta velocidad. Enviar datos, y otro tipo de elementos puede ser fácil.

Desventajas

- Su tamaño es pequeño.
- La trasmisión de información ocurre cuando los dispositivos se encuentran en el mismo espacio geo referencial.

[10] TANENBAUM, Andrew, WETHERALL, David. Redes de Área Local. En Redes de computadoras. 2015. Quinta Edición. Capítulo 1. p. 18

Figura 6. Funcionamiento de una red LAN.



Fuente: López. Construcción de una Red de Área de Local. Taringa. (2014). Recuperado de: https://www.taringa.net/+info/construccion-de-una-red-de-area-local_12thr7

2.1.2.2 Red de área metropolitana (MAN).

La red la constituyen un conjunto de redes LAN que se encuentran cerca geográficamente (50 Km) siendo su alta velocidad su mayor característica. Por lo tanto, una Red de área metropolitana permite que dos dispositivos remotos se puedan comunicar como si fueran parte de la misma red de área local. Entre los usos de las redes MAN, cabe mencionar la interconexión entre oficinas que se encuentran distantes en una misma ciudad pero que pertenecen a una misma organización, a continuación, se describen las ventajas y desventajas de está y en la figura 7, se describe su funcionamiento

Ventajas

- Es más segura que una red WAN
- Este tipo de Red tiene más efectividad al transmitir paquetes de datos sin asignar un ancho de banda fijo.
- El ancho de banda es mayor a las redes WAN

Desventajas

- La regulación que presentan las redes podría limitar la compra de una red de área metropolitana.
- Su máxima cobertura son los 50 Km de diámetro.

Figura 7. Funcionamiento de una red MAN.

Fuente: Sistemas master. Recuperado de: https://sistemas.com/man.php

2.1.2.3 Red de área amplia (WAN).

Esta red está en la capacidad de enlazar un área geográfica amplia (país, continente, el mundo) utilizando con frecuencia las instalaciones de transmisión como microondas y satélites, garantizando mayor cobertura. Internet se considera como la red WAN más reconocida y usada, ya que enlaza una cantidad mayor de nodos interconectadas por redes LAN y MAN, a continuación, se describen las principales ventajas y desventajas, en la figura 8 se describe este proceso.

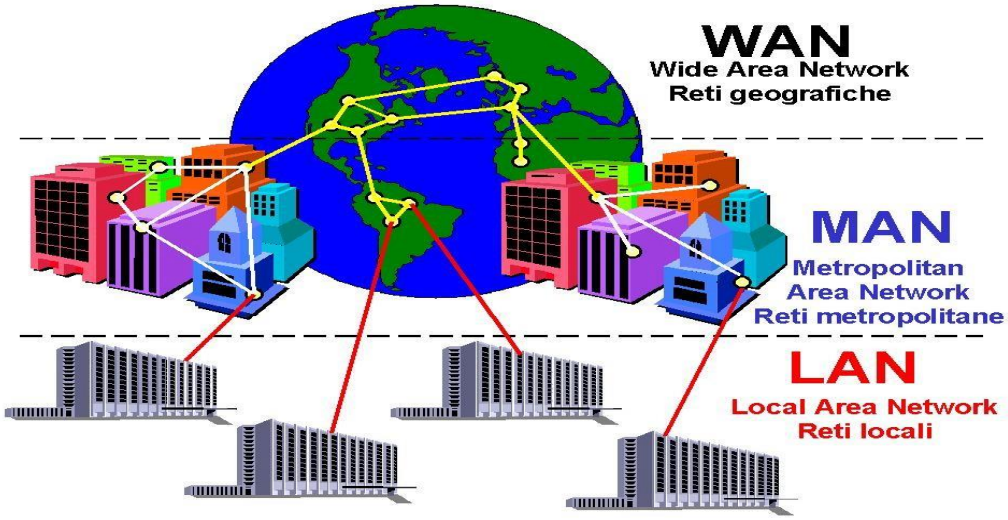
Ventajas

- Suele implementar un programa especial para abarcar mini y macro - computadores como recursos de red.
- No tiene límites geográficos.
- Entabla comunicación entre computadoras.

Desventajas

- Los dispositivos deben contar con una muy buena capacidad de memoria, de lo contrario la velocidad de transmisión es lenta o limitada.
- Los estándares de seguridad son bajos. Las vulnerabilidades y amenazas que presentan este tipo de redes son muy comunes.

Figura 8. Funcionamiento de una red WAN.



Fuente: Tipos de redes y sus características. Recuperado de: http://comunicaciongr.blogspot.com/2012/04/tipos-de-redes-y-sus-caracteristicas.html

2.1.3 Seguridad Informática.

Hablar de seguridad en los procesos informáticos en la actualidad se refiere a concentrarse y distinguir entre el concepto *safety* que aborda los riesgos asociados a eventos accidentales como lo pueden ser, los desatres naturales, fallos no intencionados, entre otros *y security,* refiriendose a los riesgos asociados a ataques con una intencipon definida, como lo pueden ser, el robo de información, sabotajes, entre otros. Para el desarrollo del presente proyecto es necesario centrarse en el segundo concepto; resolver las necesidades existentes en la red de datos, plantea abordar nuevos desafíos desde la implementación de estrategias más exigentes. La seguridad de la información en la Red se fundamenta en la protección de insumos tecnológicos tangibles e intangibles de esta. En una red se deben diseñar

estrategias que provean de seguridad al software y hardware que faciliten y optimicen el proceso de la comunicación, los usuarios y los administradores de redes

Una de las investigaciones que aporta a comprender la relevancia conceptual del siguiente proyecto es la de Maximiliano Cristia[11], el cual sugiere un ejemplo para entender la diferencia entre *safety y security;* la implementación de un programa que mejore los procesos de recolección de datos; *safety* correcto, pero *security* incorrecta. Para no incurrir en esta dicotomía y entender de manera correcta lo que el Sistema de Monitoreo de la Red necesita para funcionar correctamente es necesario traer a colación protocolos basados en técnica y desarrollados de manera metodológica que permitan diseñar y ejecutar de manera razonable estrategias que mantengan la naturaleza y seguridad de la información.

Cristia[12], señala que establecer la seguridad informática perfecta no existe, ya que siempre va a ser latente la vulnerabilidad (concepto que será explicado posteriormente), pero se puede prever los ataques de manera gradual preventiva y correctivamente, diseñando y desarrollando estrategias de seguridad eficientes, entendiendo que la seguridad informática es un proceso constante de construcción, no la finalidad en sí misma. Entender la seguridad de la información y de la red como un proceso permite entender su naturaleza: Cristia[13] en su investigación teórica señala que se puede clasificar la seguridad en interna y seguridad externa, de la primera se afirma que es la que brinda soporte y protección al software y de las herramientas del hardware que sirven para proteger la información, un ejemplo claro es la fragmentación de los discos duros; la seguridad externa provee protocolos de seguridad que el sistema no garantiza, un ejemplo claro es la seguridad física de las instalaciones, la seguridad del personal, aclarando que de la relación de los dos tipos de seguridad depende el éxito de la organización, Cristiá, aduce:

> Supongamos que instalamos en una PC el sistema operativo más seguro que se conoce (seguridad interna) pero al mismo tiempo dejamos la computadora en un pasillo público de la empresa (seguridad externa). En este caso el resultado neto será que la información allí almacenada y procesada no estará segura puesto que queda expuesta a todo tipo de ataques tales como: robo de la PC misma; robo de su disco rígido; arranque de la PC con un disco externo que permite acceder a todo el contenido del disco interno; instalación por ese mismo medio de programas de ataque; etc.[14]

[11] CRISTIA Maximiliano. Seguridad Informática. Rosario; Universidad del Rosario, 2018. P. 5
[12] Ibid., p.5.
[13] Ibid., p.6
[14] Ibid., p.8

Es desde este punto, que la información es considerada hoy por hoy como uno de los activos más importantes de cualquier entidad, y el buen tratamiento de esta es indispensable. El proceso de transmisión de información mediante la red, debe cumplir con ciertos estandares de seguridad que protejan la información, desde los siguientes aspectos; exactitud, el alcance de los usuarios, sin modificación alguna y, ante todo, sin ser manipulada por personas no autorizadas.

2.1.4 Características de la seguridad informática.

Para diseñar y ejecutar un sistema de monitoreo efectivo y eficaz que cumpla con el objetivo principal del siguiente proyecto y en ese orden los objetivos corporativos de la organización, es necesario tener en cuenta protocolos de seguridad, estos han sido definidos a nivel general como los estándares a cumplir por parte de cualquier organización con respecto a la seguridad de la información, su veracidad, confiabilidad y demás atributos que serán explicados posteriormente.

2.1.4.1 Autenticación

La creación de este sistema de Monitoreo se fundamenta en el proceso histórico de reconocimiento que ha llevado a cabo la humanidad y sus diferentes civilizaciones, donde han sido las diferentes características del cuerpo humano un elemento clave para identificarse dentro de la sociedad, por ejemplo, el reconocimiento por medio de la voz, del rostro, del tacto, entre otros. En la era de la información este tipo de reconocimiento corporal obedece a un modelo aplicable a redes o sistemas Unix, donde el agente de reconocimiento es un dispositivo.

La autenticación en un sistema de red, tiene como objetivo reconocer al usuario al momento de ingresar a una plataforma digital, de esta manera se corrobora la identificación del usuario en la red. La confianza y el principio de la buena fe desempeñan un rol importante en este atributo, ya que lo que se pretende es que la información esté disponible por el usuario que requiere el ingreso. De esta manera Cristia en la investigación titulada seguridad informática aduce:

> El ejemplo canónico de identificación y autenticación es el mecanismo de *login* que utilizan los usuarios para ingresar a un sistema. Cuando el usuario provee su 'nombre de usuario' o *'login'* se está realizando la identificación; cuando el sistema comprueba

> que la contraseña provista es la que corresponde a la cuenta de usuario, el usuario ha sido correctamente autenticado.[15]

Los métodos de autenticación se estructuran y segmentan según el tipo de sistema que se quiera proteger (interno, externo), por medio de métodos de verificación. La protección de la información está definida por dos criterios: El modelo basado en pruebas de validación escrita como lo son un *password* o *passphrase*. Los modelos basados en la validación física como lo son una *smartcard* o sistemas basados en una característica física. La investigación titulada sistemas de autenticación[16], señala que uno de los sistemas más implementados para proteger el sistema externo, es la autenticación biométrica, debido a su eficiencia y eficacia, se ha pensado que estos sistemas son los que se van a imponer en la mayoría de las situaciones en las que se haga autentificar a un usuario. Este tipo de sistemas de autenticación biométrica, presentan ciertas ventajas en cuanto a otros métodos; son más adaptables para los usuarios, ya que no necesita recordar una contraseña de acceso, esto representa una ventaja hacía otros métodos de autenticación, ya que es más fácil reconocer una parte del cuerpo, que estar recordando contraseñas. Otra ventaja que sobresale de este sistema es la dificultad para ser suplantada, al contrario de una contraseña que puede ser descubierta o descifrada.

Aunque, el sistema de autenticación biométrica presenta mayor seguridad, el acceso a esté en la actualidad se encuentra limitado, debido a sus altos costos. La investigación Sistemas de autenticación[17], señala que son denominados biométricos debido a que su diseño se basa en inspeccionar las formas, y el avance tecnológico, facilitan que este sistema pueda identificar de manera exacta las características físicas de los usuarios a identificar, según lo señalado por la investigación sistemas de autenticación.

En la **tabla 1**, se describe los diferentes tipos de métodos de autenticación biométrica que utilizan e implementan las organizaciones actualmente desde el reconocimiento de características físicas de los humanos, señalando sus características específicas.

[15] CRISTIA Maximiliano. Seguridad Informática. Rosario; Universidad del Rosario, 2018. P. 5
[16] SISTEMAS DE AUTENTICACIÓN, s,f. p. 2
[17] Ibid. p. 2

Tabla 1. Comparación de métodos biométricos.

Variable evaluada	Ojo Iris	Ojo Retina	Huellas	Geometría de la mano	Escritura firme	Voz
			Nivel de Eficiencia			
Fiabilidad	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta
Facilidad de Uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de Ataques	Muy Alta	Muy Alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Alta	Alta	Muy Alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y Autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándars	-	-	ANS1/ NIST	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad	Artritis	Firmas fáciles	Ruido

Fuente: Elaboración Autor. @ Copyright. Sistemas de autenticación (s, f).

Los sistemas de reconocimiento de voz buscan, reconocer una serie de patrones particulares de sonidos vocales del individuo que permita identificar a este usuario en una red, para aplicar este sistema correctamente se debe disponer de condiciones que no emitan ruidos, ecos, entre otros. La investigación Sistemas de Autenticación[18] aduce que cuando un usuario quiere acceder a un sistema pronuncia frases en las cuales reside la mayor parte del protocolo de seguridad, habitualmente se escogen palabras con diferentes características (entonación, diptongos, entre otros), mientras habla el usuario el sistema va registrando la información.

Una de las principales desventajas de este sistema biométrico de reconocimiento de voz es la poca repuesta efectiva que se le ha prestado al replay *attacks* (ataque de repetición),

[18] Ibid. p.5.

este tipo de ataques se producen por medio de un magnetófono, y otros mecanismos utilizados donde se reproducen las frases o palabras que el usuario pronuncia a la hora de entrar a un sistema.

Otro método de autenticación descrito en la investigación Sistemas de autenticación[19] es el reconocimiento que realiza un usuario mediante la escritura, que, aunque no es un elemento de constitución 100% biométrica, se suele agrupar en esta categoría dado sus beneficios y desarrollos informáticos. El sistema pretende reconocer las características específicas de la escritura, tales como el grado de inclinación de los grafemas, el trazo, entre otros. Por último, se encuentra el método que permite verificar la identidad de un usuario en la red, por medio del reconocimiento de la huella dactilar; lo cual ha mejorado la eficacia al momento de verificar al ususario; indiscutiblemente nunca dos dedos van a poseer las mismas características dactilares, este tipo de sistema reconoce las particularidades de cada huella.

Contraseñas: Su traducción en inglés es *password*, este tipo de sistema de autenticación, utiliza información personal y secreta de un usuario para permitir o negar el acceso a una red o recurso, este sistema ha potenciado la seguridad de los sistemas internos informáticos. La investigación Sistemas de Autenticación[20], señala que el antecedente histórico de este método data de la época medieval: “donde los centinelas que vigilaban una posición solicitaban el «santo y seña» al que quisiera pasar, solamente le permiten el acceso a aquella persona que conoce la señal. En la actualidad son utilizadas para dar acceso a la información y sus recursos.

La lengua inglesa presenta dos definiciones de este concepto: en un primer lugar se encuentra la palabra *password,* que hace referencia a la utilización de códigos alfa – numéricos, normalmente son palabras de fácil recordación, la segunda definición la *pass code* (código de acceso) que hace referencia a códigos numéricos, según lo señala la investigación Sistemas de Autenticación[21]. El control más efectivo para evitar que un tercero cifre las contraseñas, consta de proveer un determinado límite de tiempo para ingresar a la red o al sistema; de igual manera, al proporcionar varias claves fallidas bloquean posteriormente el acceso, de esta forma la única persona que puede desbloquear la cuenta es el administrador; en conclusión, es relativamente seguro el sistema mientras el usuario cree contraseñas seguras.

El cambio esporádico de las contraseñas es una recomendación a seguir para mantener la información segura de los usuarios; se han diseñado diferentes formas de cambiar

[19] Ibid. p.7.
[20] Ibid., p. 9.
[21] Ibid., p. 9.

contraseñas, algunos administradores tienen como opción suministrar la contraseña de una manera no cifrada vía e-mail. Los Sistemas de Administración de Identidad solicitan preguntas ya predeterminadas que den garantía de la identidad del usuario.

Sistemas de Autentificación en Sistemas Operativos: El primero se llama Autenticación Clásica, este es un sistema Unix, donde, según la investigación Sistemas de Autenticación "cada usuario posee un nombre de entrada al sistema o *login* y una clave *password*, ambos datos se almacenan generalmente en ficheros"[22].

En ese orden, cabe aclarar que este Sistema Operativo distingue de un usuario a otro por medio del *UID* (Identificación Usuario), y esto lo organiza por medio del *login*, ya que es más fácil recordar un nombre que una combinación numérica; de igual manera, cabe aclarar que un nombre de usuario es asignado a un *UID.*

Shadow Password: Este método es implementado para brindar protección a las contraseñas de los usuarios y su traducción al español es oscurecimiento de contraseñas, Según la investigación Sistemas de Autenticación [23], la finalidad de este mecanismo es no permitir el acceso ilimitado a usuarios que no tengan este permiso protegiendo así a los ficheros donde se almacenan las contraseñas cifradas.

2.1.4.2 Integridad.

Soriano[24], aduce que Requiere de un proceso riguroso en el que los recursos sean manipulados exclusivamente por quienes han sido autorizados y que los métodos y los procesamientos de la información sean salvados y guardaos en su totalidad. Varios son los conceptos que se acuñan de manera análoga a este factor de seguridad informática: precisión *(accuracy)* integridad *(integrity),* autenticidad *(autenticity)*; estos conceptos que abordan la definición de integridad es la que garantiza que la información no sea modificada.

Esta característica de la seguridad, asegura que no se falsifique, modifique o pierda la información. A groso modo: cuando se presentan perdidas de información el aspecto de integridad en una red de datos debe garantizar que al ser recuperada la información sea la misma con la que se contaba antes del incidente sin que se haya alterado o modificado esta. En ese orden, el problema de la integridad no solo se

[22] Ibid., p. 16.
[23] Ibid., p. 17.
[24] SORIANO, Miguel. Seguridad en Redes y Seguridad de la Información. Praga. Fakulta elektrotechnická,

refiere a la modificación a la que se puede llegar a someter la información de manera intencional, sino, también de las alteraciones que se presentan de manera accidental o no intencionada.

Tanto autenticidad e integridad trabajan conjuntamente, ya que proporcionan los medios para verificar que el origen de los datos sean correctos o confiables desde un protocolo establecido: la primera parte de este pnrotocolo es identificar el origen (emisor), quienes envían y reciben la información, el canal por donde llega esta, en pocas palabras analiza todo el proceso comunicativo de trasmisión de datos. Soriano[25], aduce, que donde se implementan constantemente los aspectos de integridad y autenticidad es en las organizaciones financieras y bancarias; en estas entidades es necesario validar la información de los usuarios y mantener la integridad de esta al momento de hacer una transacción, predominando la integralidad de la información sobre la confidencialidad

2.1.4.3. Confidencialidad.

La confidencialidad como aspecto informático es la garantía que se debe proveer a un usuario de que la información es accesible solo para quienes están debidamente autorizados para su modificación, lectura, impresión y formas de revelación, esto permite salvaguardar los datos. La confidencialidad se relaciona directamente con la capacidad que tiene las organizaciones en sus sistemas informáticos de evitar que personas mal intencionadas puedan acceder a la información de la Empresa.

Un ejemplo claro donde se implementan altos niveles de confidencialidad en los sistemas operativos, son los presentes en las organizaciones gubernamentales, donde se limita o se da acceso a la información según los rangos u oficios que ocupen los funcionarios dentro de la organización. Cristia[26] señala que los protocolos son necesarios desarrollarlos e implementarlos según las recomendaciones y normas vigentes que protejan la información, de esta manera Soriano, aduce que “la protección de la información o la red con base a disposiciones legales o criterios estratégicos a nivel privado, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc”[27].

[25] Ibid., p. 33
[26] Cristía, Op, cit., p. 7
[27] Soriano, Op, cit., p. 34

Algunos de los mecanismos que se implementan de manera constante para proteger los datos a nivel de confidencialidad son, entre otros: el uso de técnicas de control de acceso a los sistemas, el cifrado de la información confidencial o de las comunicaciones, entre otras.

2.1.4.4 Disponibilidad.

Este factor debe garantizar que la información esté a disposición en el momento exacto y requerido por las organizaciones o personas que estén autorizadas para acceder a ella y así cumplir los objetivos institucionales, basadas en la efectividad y eficacia de los sistemas de gestión de la información. En ese orden tanto el software, el hardware y la red deben estar siempre trabajando en óptimas condiciones. En palabras de Soriano: "la disponibilidad significa que tanto el hardware y el software; se mantengan de manera eficiente, siendo capáz de recuperarse de manera eficiente y rápida en caso de cualquier fallo"[28].

2.1.4.5 Consistencia.

La consistencia es la capacidad que tiene un sistema para asegurar que este se comporte como debe comportarse con los usuarios autorizados. Un ejemplo claro antagónico de la función de seguridad de la consistencia es cuando el hardware o software de un sistema, se comporta de manera inesperada.

2.1.4.6 Aislamiento.

Es la capacidad de un sistema para limitar el acceso a personas no autorizadas o inescrupulosas. En palabras de Soriano: "Regula el acceso al sistema, impidiendo que personas no autorizadas tengan acceso. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema hardware y software que a la información que contiene[29]".

2.1.4.7 Auditoria.

[28] Cristía, Op, cit., p. 7.
[29] Ibid., p .10

Se refiere a la capacidad, que tiene una organización para determinar, definir, clasificar los diferentes procesos que se hacen parte del sistema de gestión de la información, la forma para realizar este proceso es registrando las actividades del sistema.

2.1.5 Tipos de Ataques.

El no cumplimiento de los anteriores factores que constituyen el protocolo de un Sistema de Gestión de la información en una red, permite clasificar y determinar los diferentes tipos de ataques a la seguridad de la red de transmisión de datos dentro del proceso de comunicación (trasmisión y emisión). Estos ataques pueden darse o clasificarse en dos tipos:

2.1.5.1 Ataques pasivos.

Se caracterizan por monitorear la transmisión de datos por parte de agentes externos no autorizados. El objetivo de los atacantes es sustraer la información trasmitida con el fin de hacer público el contenido de un mensaje; una de las formas más comunes de este ataque es escuchar una llamada telefónica, leer un correo electrónico abierto o analizar el tráfico de datos para determinar la localización e identidad de quienes se están comunicando.

2.1.5.2 Ataques activos.

Este tipo de ataque pone en evidencia y altera los procesos informáticos y tecnológicos de una organización; supone modificar y manipular la información o crear flujos de datos falsos. Estos se clasifican en:

Enmascaramiento (*IP Spoofing*): Es un ataque que se da cuando un agente pretende suplantar a una entidad para obtener información susceptible; es un tipo de ataque donde se suplanta la identidad, el atacante consigue modificar el asunto de los paquetes enviados. La investigación titulada: tipo de ataques e intrusos en las redes informáticas, realizada por Gómez[30], define este tipo de ataques, señalando que son realizados cuando el atacante trata de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al

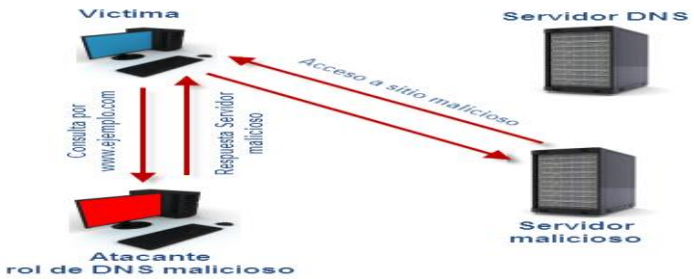
[30] GÓMEZ VEITIS, Alvaro. Tipo de ataques e intrusos en las redes informáticas. Profesor de la Escuela de Negocios Caixanova. s, f. p. 2

sistema que pretende ser engañado, este tipo de fraudes podría ser prevenido implementando filtros para que todo el tráfico se asocie a un Protocolo de Internet (en adelante IP).

Otro tipo de ataque, utilizando este método es el conocido como el *hijacking*, donde el atacante trata de suplantar la dirección IP de la víctima y el número de la secuencia del próximo paquete de datos que va a transmitir, a groso modo, es conocido como el secuestro de datos con un nombre de usuario que se mantenga activo.

DNS *Spoofing:* Son ataques que falsifican el Domain Name System (en adelante DNS), o sistema de nombres de dominio por su traducción al español y su objetivo es direccionar erróneamente los datos de los dispositivos afectados, es posible por medio de una traducción falsa de los nombres de dominio; redirecciona a los usuarios a páginas falsas para sustraer nombres de usuario y contraseñas, Gómez[31] señala que la manipulación de los DNS, también podría estar detrás de algunos casos de pishing; estos buscan redireccionar a usuarios hacia páginas Web falsas, y desde allí obtener información susceptible como nombres de usuarios y contraseñas, este tipo de ataque es considerado como un fraude, ya que busca la suplantación de identidad de un agente en la red. De igual manera cuando se es víctima de este tipo de ataques, aunque se piense que el servidor que se está consultando es el correcto muchas veces no lo es. Es importante recordar que para navegar en internet es necesario contar con los servidores DNS, ya que las paginas web se encuentran bajo una dirección IP, que coloquialmente sun números de identificación otorgados al nodo para navegar, en ese orden, los DNS traducen nombres inteligibles para las personas que están conectados a la red facilitando el direccionamiento y la localización de los equipos, ya que es más fácil recordar nombres que números. El ataque se encuentra representado en la figura 9.

Figura 9. Ataque a ARP por DNS Spoofing



Fuente: Equipo Editorial (2019).

[31] Ibid,. p. 2

SMTP *Spoofing:* consiste en enviar contenidos por medio de mensajes con remitentes falsos *masquerading*, para timar al destinatario o dañar la imagen del remitente, es un ataque común entre los tantos que hay de suplantación de identidad, muchos de los virus utilizan este mecanismo para propagarse en los sistemas informativos. Gómez [32], señala que, en la actualidad, plagiar los e- mails es sencillo ya que el protocolo utilizado es el Simple Mail Transfer Protocol (en adelante SMTP) o Protocolo Simple de Trasferencia de Correo, por su traducción al Español; tiene ausencia de procesos de autenticación, este tipo de método es de fácil manipulación ya que cualquier persona ajena a la organización puede ingresar al protocolo SMTP.

Modificaciones del tráfico y de las tablas de enrutamiento: La finalidad es desviar los paquetes de datos originales a través de Internet, para que atraviesen por dispositivos antes de llegar al destino establecido captando e interceptando los datos. Este tipo de ataques permite que el atacante puede determinar el enrutamiento de transferencia de datos, antes de llegar a su destino, siendo esta la ruta de entorno y desde allí saltándose las rutas de protocolo establecidas en la red, un atacante podría hacerse pasar por un servidor generando confianza en los usuarios para recibir los datos.

Conexión no autorizada a equipos y servidores: Los métodos más comunes de este tipo de ataque son: violación de un sistema de control de acceso, explotación de agujeros de seguridad (Exploits), conjunto de instrucciones no documentadas dentro de un sistema operativo (backdoors) en cualquiera de los casos se toma el control del equipo.

Código malicioso o introducción en el sistema Malware: Es conocido como código malicioso, este puede transmitirse por un programa, documento o mensaje que pueda ocasionar daños a la red o los sistemas informáticos, un ejemplo ejemplo es cualquier tipo de virus. Gómez[33] señala que este tipo de programas malintencionados se propagan de manera rápida, por ejemplo, por medio del correo electrónico, las conexiones mediante nodos, y los nuevos servicios de intercambio de ficheros o de mensajería instantánea, según lo señala.

Ataques de "*Cross-Site Scripting*" (XSS): Consisten básicamente en la ejecución de código "Script" (como Visual Basic Script o Java Script), son ataques dirigidos a los usuarios y no al servidor Web. Gómez[34], Señala a nivel general que este tipo de

[32] Ibid., p .3
[33] Ibid.,p.5
[34] Ibid., p.5

ataque lo que busca es suplantar la identidad de los usuarios, se pueden dar cuando el servidor Web no filtra de manera correcta las peticiones del Hypertext Transfer Protocol (en adelante HTTP, o protocolo de transferencia de hipertextos por su traducción al español) de los usuarios, en este caso el atacante envia un código para lograr la suplantación.

Ataques de Inyección de Código SQL: Su nombre es *Structured Query Language* (Lenguaje de Consulta Estructurado), este tipo de lenguajes se utiliza para relacionarse con bases de datos similares. Los ataques de inyección SQL aprovechan de las fallas de diseño en las aplicaciones web convirtiéndose en un procedimiento sencillo y eficiente de ataque cibernético. En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios. El ataque por inyección de código SQL se da al no filtrar de forma adecuada la información que envía un usuario.

Ataques contra los sistemas criptográficos: Tienen como finalidad descifrar las contraseñas utilizadas que cifran datos específicos, que contienen información que se encuentran guardadas en un sistema y obtener información sobre el algoritmo criptográfico utilizado, se presentan diferentes ataques: el más común es el ataque de fuerza bruta, es un procedimiento utilizado para averiguar una clave probando todas las composiciones probables hasta dar con la exacta. Para dimensionar conceptualmente de lo que es un ataque a los sistemas criptográficos el blog informático titulado apaga y enciende[35] , señala que los ataques por fuerza bruta son uno de los métodos más comunes de robo de contraseñas en Internet debido a que no es necesario tener mucho conocimiento en seguridad informática para ejecutar uno, además existen software que se utilizan para realizar este tipo de ataque

Denegación de Servicios: El objetivo primordial de este ataque es colapsar los equipos o redes informáticas para impedir que puedan ofrecer sus servicios a los usuarios, alteran el uso normal de los servidores o de los equipos. Normalmente lo que hace este tipo de ataque es provocar la pérdida de la conectividad de la red por el consumo de la transmisión de información (ancho de banda) de la red de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el o los servidores se sobrecarguen y no puedan seguir prestando servicios, por eso se le denomina “denegación”, pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados *hackers* de sombrero negro (definido asì por las intenciones que rodean su ataque) o crackers, que son en sí *piratas* informáticos para dejar fuera de servicio a servidores objetivo

[35] APAGA Y ENCIENDE. (s, f). Blog. Que es un ataque por fuerza bruta.

2.1.6 Necesidades de seguridad

Realizado el análisis en diferentes empresas y en especial las organizaciones Prestadoras de Servicio de Salud (estos se describen posteriormente en el marco metodológico), permitió identificar que no se han establecido estándares de seguridad bien definidos para salvaguardar la información. Es evidente que la información que se maneja es bastante sensible, debido al servicio que presta esta organización a la sociedad y por eso es importante establecer controles eficientes de seguridad. Las principales eventualidades de seguridad que puede aquejar la organización, son:

- Ataques de virus.
- Inestabilidad de la energía (muchas veces se han apagado los servidores).
- Instalación de software inadecuados por partes de los usuarios.
- Perdida de información.
- Acceso no autorizado.
- Secuestro de Información.
- Falta de Capacitación de los empleados sobre seguridad informática.

2.1.7 Monitoreo de red.

2.1.7.1 Definición.

El monitoreo de red permite al administrador del sistema examinar y observar la condición en la que se encuentra la red de datos, debe permitir tomar acciones óptimas para la gestión, mitigando los problemas que pueden presentarse en las redes, brindando una visión global de todo el sistema.

Para que una Organización o Empresa pueda funcionar correctamente, se debe considerar el diseño e implementación de un sistema de seguridad de la información que contrarreste los ataques informáticos que puedan existir para violar los controles de seguridad. El sistema informático representa una gran prioridad para las Empresas. Los sistemas de protección de la información y de las redes informáticas deben tener la capacidad para responder en cualquier momento y situación, evitando incidentes que puedan generar perdida de datos.

Ofrecer un determinado servicio en una organización, convierte a las redes que trasmiten datos como uno de los componentes más primordiales. En ese orden, si

una empresa presenta incidentes en su infraestructura de red en la prestación de un servicio y no se cuenta con una solución pronta en la transmisión de los datos, clientes durante el tiempo que dure el incidente. Todo esto puede causar grandes problemas en una empresa, causando malestar en los clientes e incumpliendo con los indicadores de calidad en el servicio prestado.

De acuerdo a lo anterior, un sistema de monitoreo de red debe garantizar un óptimo rendimiento en una organización. El propósito fundamental de la persona encargada de administrar la red es constatar que las redes se encuentren funcionando a un 100% del rendimiento. Descrito lo anterior, está la elección de la herramienta de monitoreo de red permitirá descubrir posibles problemas antes de que se provoque un colapso o una caída de las redes. El monitoreo de red permite analizar y ver el estado de las redes.

Características que se deben tener presente al momento de adquirir un software de Monitoreo si es libre:

- Anunciar de manera oportuna las alertas.
- Trabajar con servidores externos.
- Exposición y descripción de los datos en el panel.
- Flexibilidad a la hora de adaptarse a herramientas o software particulares.
- API de acceso desde sistemas externos.
- Detección de dispositivos de forma automática.
- Integraciones con Bases de Datos.
- Multidispositivo.
- Escalabilidad.
- Soporte del mayor número de protocolos de adquisición de datos posible.
- Seguridad.
- Integración con máquinas virtuales.
- Integraciones hardware.
- Control remoto.
- Inventario de Hardware y Software.
- Geolocalización.
- Monitorización de la nube.

Es imprescindible tener en cuenta las herramientas que ofrece el programa de monitoreo de red para indicar al administrador de cualquier suceso que pueda afectar el correcto funcionamiento de la red de datos. La relevancia reside tanto en el formato del mensaje como en la prontitud del envío junto a su carácter multidispositivo.

Por tal motivo, el monitor de red debe generar mensajes comprensibles o claros (formato HTML), que puedan ser emitidos a distintos dispositivos, para que de esta forma se puedan tomar las medidas pertinentes, con el propósito de controlar la posible fuga de información o caída del sistema (correo electrónico, móvil u otras herramientas) y mediante diferentes protocolos (Whatsapp, SMTP, Push, etc).

Un sistema de monitoreo de red debe medir el ancho de banda y el estado de cada enlace de conexión entre nodos. Pero también es muy primordial que el software elegido sea capaz de monitorizar diferentes servidores, ya sean de aplicaciones web, de email o de aplicaciones CRM. Estas particularidades permitirán descubrir incidentes, dando una visión más global de el CPD (Centro de Proceso de Datos).

Hay que tener en cuenta que la información que va a procesar el instrumento de monitorización es relevante, en muchos casos es confidencial, previendo que la información sea obtenida por personas que no estén autorizadas. Adicionalmente, el sistema de monitoreo de red debe caracterizarse por ser seguro para que la información almacenada no se vea comprometida. Otros aspectos que cobran importancia son el almacenamiento de claves de terceros, de forma encriptada lo cual permita que la red de datos este segura.

Como se ha observado, las redes representan más que la estructura de cables, dadas entre nodos y dispositivos. En ese orden, el hardware debe ser seguro, de esta manera, se aconseja no solo monitorear la red y las aplicaciones que envían información, sino, diseñar informes que brinden el estado de las máquinas, analizando variables como la temperatura, el espacio de discos, la memoria, etcétera.

La monitorización de sistemas informáticos se ha convertido en un proceso necesario para administrar la infraestructura TI (Tecnologías de la información), que debe ser vista como herramientas que permitan optimizar el procesamiento de datos, para ello se deben centrar en conseguir los siguientes objetivos:

- Aprovechar al máximo los recursos Hardware y Software de una empresa.
- Prevención de incidencias y detección de problemas.
- Notificación de posibles problemas.
- Ahorro de costes
- Ahorro de tiempo
- Mejorar la satisfacción en atención al cliente.
- Integridad de la información
- Prevenir posibles ataques informáticos

Dichos objetivos son medibles en la cuanto se implemente un sistema de monitorización, centrado en identificar, analizar y monitorear los procesos, la memoria, el almacenamiento, la seguridad y las conexiones de red y con ello determinar en tiempo real los incidentes que se presentan a diario en la red.

2.1.7.2 Ventajas de monitorización de sistemas.

Múltiples son las razones por las cuales se deben monitorizar los sistemas de información. Las principales de estas hacen referencia a la implementación de medidas preventivas que fortalezcan los procesos de protección de datos al interior de las organizaciones, entre las principales razones, se encuentran:

- Se podrá acceder al estado del sistema informático en tiempo real.
- Localizar las causas de los incidentes.
- Suscribir información administrativa de la situación real de las instalaciones y verificar cómo están los bienes informáticos más críticos.
- Optimizar la eficacia y la eficiencia de los oficios de mantenimiento del sistema.
- Estructurar eventos y alarmas en los momentos indicados.
- Inventariar sistemas (mapas, listados).
- Proyectar el crecimiento en base al uso real de los sistemas.
- Reducir costos.

2.1.8 Herramientas de monitoreo.

Hay que tener en cuenta que no existe una herramienta que logre mitigar el 100% de las amenazas, las vulnerabilidades en un sistema de información van a existir, es por eso la importancia que los colaboradores de la Empresa tengan sentido de pertenencia, y tener mucho cuidado al momento de navegar en la red de la organización. Esto evitará minimizar los ataques cibernéticos a los cuales se está expuesto a diario, de esta forma poder salvaguardar la información. La Gestión de un Sistema de Monitoreo, no solo implica que solo el departamento TI, sea la única área funcional de la Empresa que es responsable de mitigar el riesgo de la pérdida de la información, el área administrativa esta llamada a organizar, planificar y determinar las políticas del Sistema, este diseño debe dejar en claro los objetivos específicos del monitoreo que cumpla con los principios corporativos.

2.1.8.1 PRTG.

El *PRTG Network Monitor* es un sistema de resolución de problemas desde la monitorización "Todo en Uno", combina las aptitudes profesionales de la compañía de redes informáticas *Paessler,* desde una completa serie de elementos que caracterizan la monitorización, su interfaz es instintiva y sencilla de implementar con la última tecnología. Este sistema de monitoreo es adecuado para cualquier tamaño de red PRTG, brinda la disponibilidad y mide el tráfico y el uso de los elementos de red. Reduce costos mitigando las suspensiones en el correcto funcionamiento de la red, mejorando las conexiones, la carga y calidad, ahorrando tiempo y controlando los Acuerdos de Nivel de Servicio (SLAS).

2.1.8.2 Solarwinds.

Este software de administración, permite organizar archivos de configuración de la red por medio de su Interfax web. Además, permite acceder a la configuración de los dispositivos y generar alertas de cualquier cambio que se realice. Se diferencia al resto de sistemas por su instantáneo mapeo de redes y nodos sin intervención del trabajo humano. Tiene un interfaz gráfico bastante potente en el que se puede ver de manera sencilla la topología y el estado en el que se encuentra la red. Posibilita la agrupación de máquinas virtuales en su monitorización.

2.1.8.3 Op5 Monitor.

Esta herramienta tiene como característica monitorizar varias plataformas, sistemas en la nube y contextos virtuales. Este software de monitoreo está centrado en la monitorización de hardware, tráfico de red y servicios, destacando su suficiencia para grandes entornos como entidades gubernamentales y organizaciones de alto tráfico de información

2.1.8.4 Zenoss.

Esta aplicación puede monitorizar almacenamiento, redes, servidores, aplicaciones y servidores virtuales sin necesidad de instalar software de manera directa en los nodos. Dispone de una versión "*Community*" con funcionalidades mínimas y una versión comercial con todas las funcionalidades. Es una herramienta que está orientada a la supervisión de los recursos en la red, envía notificaciones al administrador por vía de correo electrónico, mensajes de textos, entre otros,

notificando así en tiempo real cualquier tipo de daño o prejuicio en el procesamiento de datos.

2.1.8.5 Nagios.

Es una herramienta open *source* (fuente abierta), esto quiere decir que es un sistema que permite ingresar a su código de programación. Ofrece un potente sistema de monitorización de código abierto que permite monitorizar toda una infraestructura TI para asegurar que los sistemas, aplicaciones, servicios y procesos de negocio funcionan adecuadamente. Una de las funciones principales de este software es observar y verificar cómo se comportan los servicios de la red tales como, HTTP, SQL, SSH, entre otras; también analiza el comportamiento del host como router, switch y otros dispositivos físicos de los sistemas y/o equipos.

2.1.9 Pandora FMS.

Es un software de nueva generación de monitorización que contiene una gran variedad de funcionalidades para administrar la infraestructura TI. Esto incluye aprovisionamiento de red, servidores Windows y Unix, infraestructura de carácter virtualizada y todo tipo de aplicaciones. La versión libre de Pandora FMS tiene como característica monitorizar más de 10,000 nodos y cubrir sin límites el proceso de monitorización en redes, servidores y aplicaciones. Esta herramienta se selecciónó por tener funcionalidades completas de análisis para informes, alertas, integraciones, adicionalmente, el software es intuitivo en cuanto a que la identifica tempranamente los riesgos y amenazas, es de facil manejo, ofreciendo la posibilidad de ser manipulado desde una misma consola desde diferentes dispositivos identificando el estado de la red y cada uno de los nodos conectados .

Con esta herramienta se busca monitorizar toda la red de datos de la Empresa, para minimizar los riesgos de perdida de información; este software (PANDORA FMS) permite que la red informática de la Empresa Prestadora de Salud sea monitoreada las 24 horas del día los 7 días a la semana, cuyo objetivo es mejorar el servicio de conectividad de las estaciones de trabajo, para que allá un mejor funcionamiento.

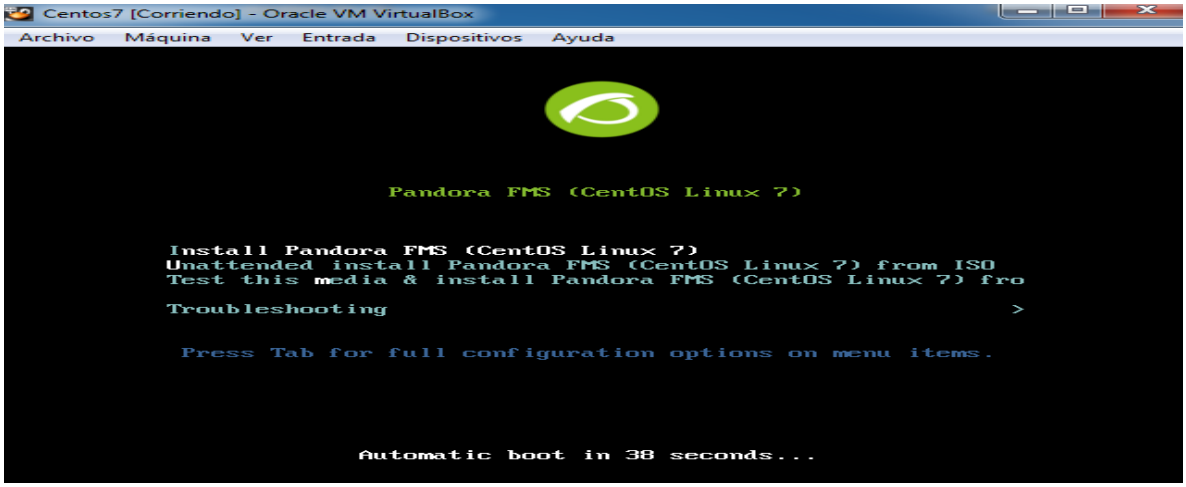
2.1.9.1 Instalación de PandoraFMS.

Se descargá la imagen ISO desde la pagina principal de PANDORA FMS se graba en un Digital Versatile Disc (en adelante DVD, o Disco Versátil Digital por su traducción al español), también se puede arrancar el sistema operativo sin

necesidad de utilizar un Compact Disc Digital Audio (en adelante CD, o disco compacto de audio digital pñor su traducción al español), si se realiza la instalación por un programa de virtualización (VMware, VirtualBox, etc). El CD o la Imagen de instalación se basa en Linux CentOS 7, y contiene preinstalados todos los componentes y dependencias necesarias para que Pandora FMS funcione, (Ver figura 9). Se debe disponer de un dispositivo con unos requisitos mínimos de hardware, un mínimo de 4GB de RAM y 20GB de disco. Cuantos más sistemas se quieran monitorizar, más medios (CPU, memoria, capacidad del disco) se deberá destinar al servidor de Pandora FMS.

Aparecerá una pantalla como la de la figura 10 al inicio de la instalación de PANDORA FMS. Si no se pulsa ninguna tecla, se iniciará en 60 segundos el Live CD, o se puede pulsar cualquier tecla, seleccionar la opción “Install Pandora FMS” y pulsar la tecla enter para comenzar la instalación.

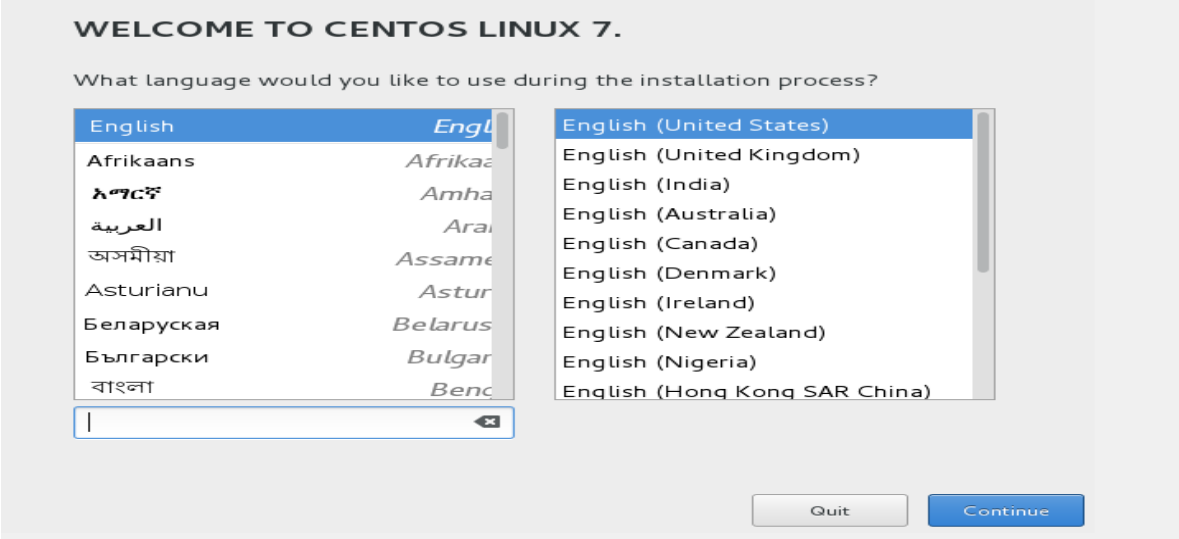
Figura 10. Instalación de Pandora FMS.



Fuente: el Autor.

El instalador gráfico orientara paso el proceso de instalación. Este instalador se puede configurar para varios idiomas y sigue un proceso de instalación estándar usado por CentOS. Es un proceso fácil, las dos secciones donde se debe prestar especial atención es cuando se pregunta por la password de superusuario (root) y cuando se pregunta acerca del particionado tal como se evidencia en la figura 11.

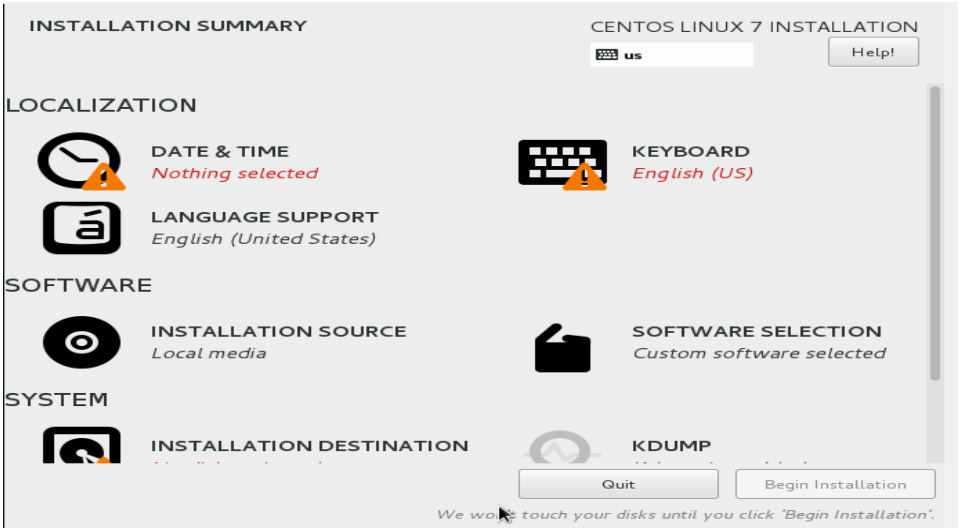
Figura 11. Instalador de gráficos.



Fuente: El Autor.

Se selecciona el idioma del país, y seguidamente continua la instalación, ver figura 12.

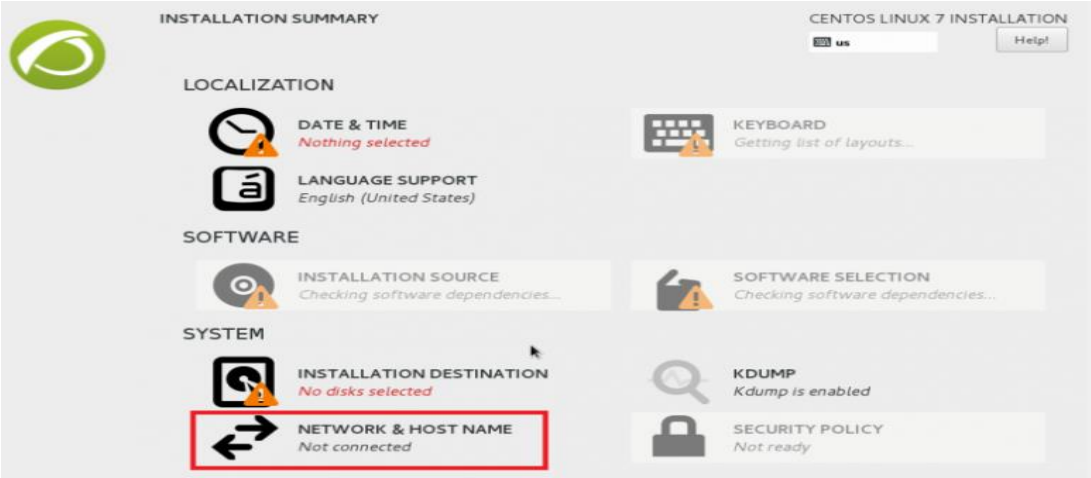
Figura 12. Selección del lenguaje para su instalación.



Fuente: El autor.

Se seleccionan y configuran las opciones solicitadas, "Fecha y Hora", "Teclado" y el "Destino de la Instalación". Se debe activar el dispositivo de red; si no, se tendrá que configurar manualmente cuando el sistema esté instalado, tal como se evidencia en la figura 13.

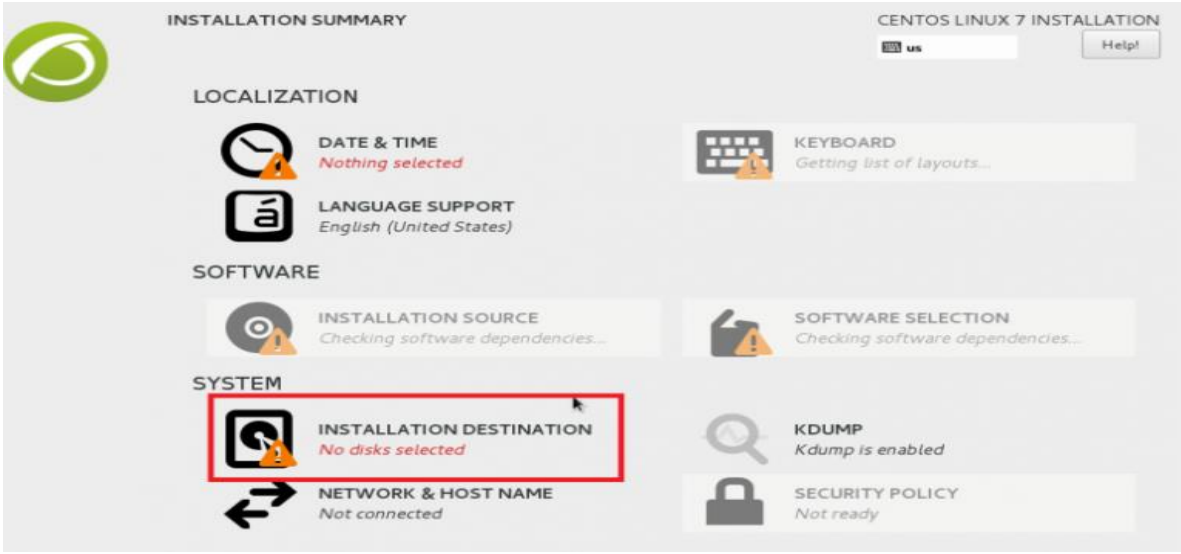
Figura 13. Configuración de las opciones.



Fuente: El autor.

Al hacer clic en destino de la instalación, se comenzará con el particionamiento del disco, en la figura 14 se representa este proceso.

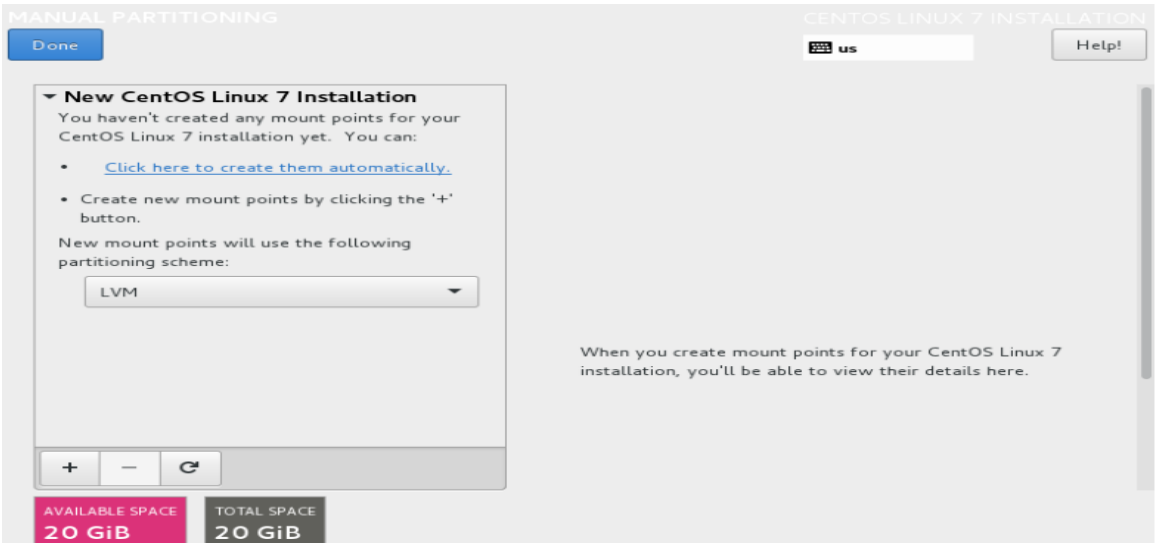
Figura 14. Particionamiento del disco.



Fuente: El autor.

Se selecciona el disco donde se va a instalar, y se cliquea en Listo, ver figura 15.

Figura 15. Proceso de instalación en el equipo.



Fuente: El autor.

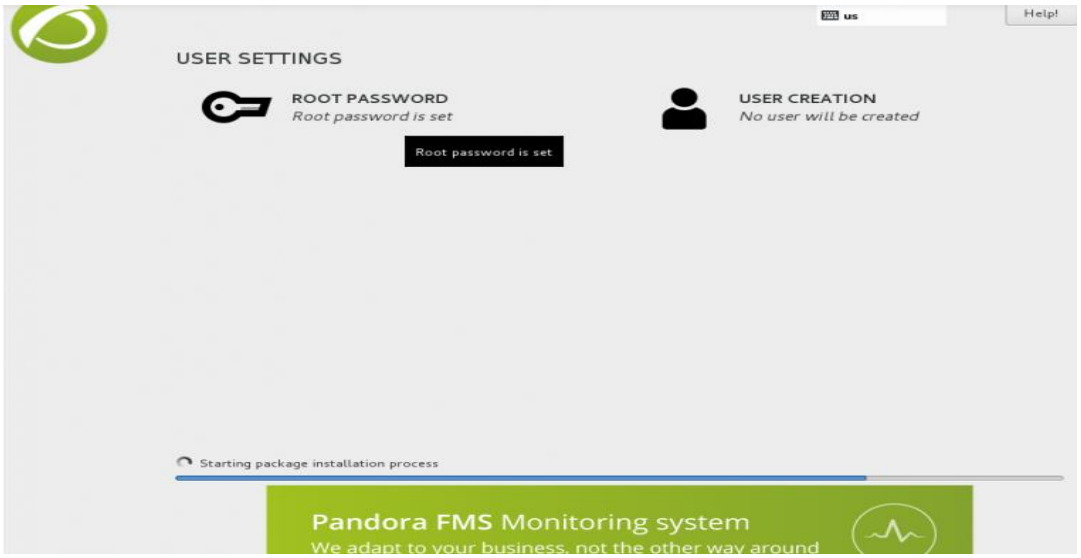
Posteriormente, se hace clic para aceptar los cambios, como se evidencia en la figura 16.

Figura 16. Cambios aceptados

Fuente: El autor.

Clic en Empezar la Instalación, tal como se representa en la figura 17.

Figura 17. Inicio de la instalación.



Fuente: El autor.

2.1.10 DLP (Prevención de Fuga de datos)

La acelerada evolución de la tecnología, ha causado que la seguridad de la información, independientemente del medio de almacenamiento o por la cual es enviada o transportada, requiera de políticas y controles más complejos y eficientes para prevenir el robo y uso inadecuado de los datos. En la actualidad las organizaciones o Empresas están enfrentando consecuencias muy graves, debido a las malas prácticas de los usuarios frente a la manipulación de datos corporativos, lo que pone en riesgo la información, la confidencialidad y la parte financiera de las organizaciones.

Para concluir, se debe tener en cuenta que no hay herramienta que logre mitigar el 100% de las amenazas, las vulnerabilidades siempre van a existir, por ende, es de mucha importancia como se ha mencionado anteriormente que los empleados tengan mucho cuidado al momento de navegar en la web o en la red de la organización. Esto evitara que las personas inescrupulosas tengan acceso a la red de la empresa, y de esta manera poder salvaguardar la información, y que esta mantenga las características y protocolos de seguridad ya mencionados con anterioridad.

3. MARCO LEGAL

Es de gran importancia describir la parte jurídica que sustenta la seguridad informática ya que permite que cada organización estructure su gestión de calidad; para la realización y sustentación del siguiente proyecto se tendrá en cuenta la siguiente normativa:

La Secretaría del Senado[36], señala que La Ley 1273 del 5 de enero de 2009 modifico el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

3.1 DELITOS CONTRA LA INTEGRIDAD Y CONFIDENCIALIDAD

Artículo 269A: La Secretaría del Senado[37], señala el acceso abusivo a un sistema informático, es el que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo

Según La Secretaría del Senado[38], A nivel penal se han articulado mecanismos de sanción, los cuales indican que la violación a la norma incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: De igual manera La Secretaría del Senado[39], aduce que la Interceptación de datos informáticos, es el que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático; prisión de treinta y seis (36) a setenta y dos (72) meses.

[36] secretariadelsenado.gov.co Diario Oficial No. 47.223 de 5 enero de 2009. Ley 1273 del 2009. Bogotá.
[37] Ibid. secretariadelsenado.gov.co
[38] Ibid. secretariadelsenado.gov.co
[39] Ibid. secretariadelsenado.gov.co

Artículo 269D: La Secretaría del Senado[40], indica que el daño informático es el que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de Información o sus partes o componentes lógicos, pena de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos.

3.2 DE LOS ATENTADOS INFORMÁTICOS Y OTRAS INFRACCIONES

Artículo 269I: La Secretaría del Señalo[41] argumenta que el hurto por medios informáticos y semejantes, es el que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

[40] Ibid. secretariadelsenado.gov.co
[41] Ibid. secretariadelsenado.gov.co

4. MARCO CONTEXTUAL

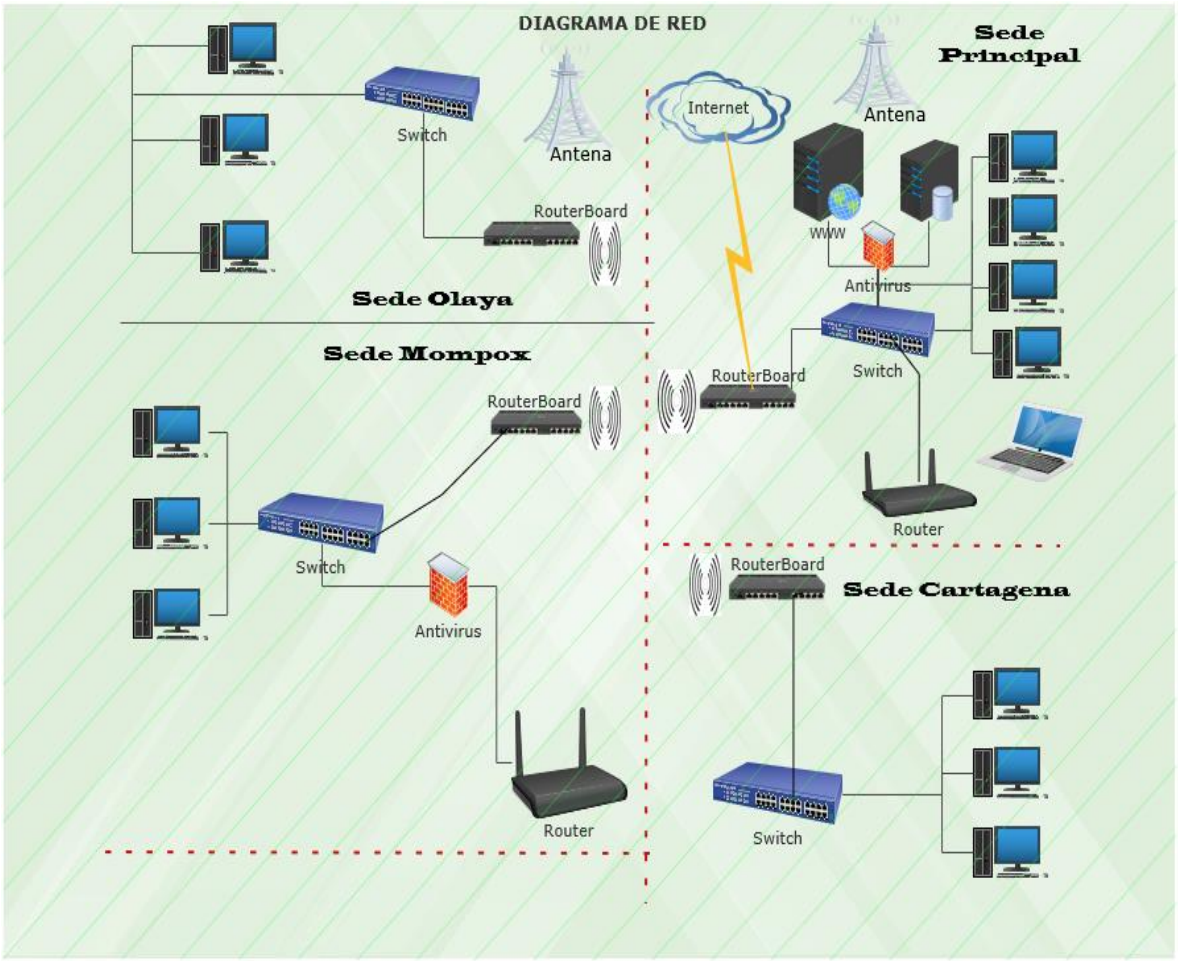
El siguiente proyecto busca implementar un sistema de monitoreo a la red de datos en la Entidad Prestadora del Servicio de Salud, se realizará desde un enfoque metodológico cualitativo desde un trabajo de campo. La Empresa brinda servicios de salud hospitalarios y ambulatorios de mediana y alta complejidad, la idea es poder diseñar e implementar un sistema de monitoreo que ayude a minimizar el riesgo de ataques informáticos que puedan poner en riesgo la integridad de los datos. Este tipo de entidades están comprometidas con el mejoramiento de la calidad de vida de sus usuarios, a través de la prestación de servicios enmarcados en criterios de seguridad del paciente, eficiencia, responsabilidad, calidad y el cuidado del medio ambiente.

El proyecto se basa en optimizar el uso de la tecnología desde una infraestructura física óptima, recursos tecnológicos de vanguardia y con equipo humano idóneo y comprometido. Es prioridad para la Empresa el mejoramiento continuo de los procesos que se realizan a diario en la institución, como seguridad del paciente, atención oportuna al usuario, etc.

4,1 DIAGRAMA DE LA RED.

La red de datos de la Empresa Prestadora de Salud está diseñada en Topología Estrella. Actualmente se cuenta con dos proveedores de internet; Telefónica con un canal dedicado de 10 Megas y Columbus, un canal dedicado de 20 Megas, cuenta con 250 estaciones de trabajo en la sede principal. La organización posee tres sucursales externas, estas conexiones se realizan por medio de VPN, es decir cada sede tiene un Mikrotik los cuales están enlazados con la estación principal; de igual manera, se estructuró un plan B, que en esencia es funcionar por medio de antenas que trabajan y operan desde radio enlace. Por medio, del presente proyecto se busca identificar en tiempo real las múltiples caídas del sistema de información, para buscar estrategias que optimicen la navegación de los usuarios y también conocer de primera mano los posibles ataques que se puedan presentar en la infraestructura informática. (Ver figura 18)

Figura 18. Diagrama de red.



Fuente: Elaboración el Autor.

4.2 CARACTERIZACIÓN DE ACTIVOS INFORMATICOS.

Son aquellos recursos de hardware y software con los que cuenta una organización para sus respectivas labores. Los activos informáticos son considerados importantes para el buen funcionamiento de las empresas, es por ello que se deben proteger con rigurosidad. Todo elemento que participa en el proceso de trasmisión de datos, parte desde la información, el emisor, el medio de transmisión y receptor, es considerado un activo informático. Ejemplo: Servidores, Bases de Datos, Routers, Racks, Programas Instaladores, Cables de Red, Computadoras, Impresoras, etc.

4.3 TIPOS DE ACTIVOS

Personalizar los activos permite identificar las características de estos y su funcionamiento, clasificando así las amenazas a los que pueden estar expuestos, salvaguardándolos de manera apropiada. Los activos se clasifican dentro de una jerarquía, estos son identificados por medio de un código que demuestra su posición en la escala jerárquica, un nombre y una breve descripción recogidos en el epígrafe. Es por ello, que la clasificación de un activo a un nivel jerárquico no lo excluye a pertenecer a otro tipo; es decir, un bien puede ser paralelo a varios tipos, ya que puede cumplir varias funciones u ocupar varias posiciones jerárquicas.

4.4 IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS Y EVALUACIÓN DEL IMPACTO

Se debe identificar los activos de la empresa para poder proceder a su clasificación. Los activos de información según la norma ISO 27005 se diferencian en dos clases. Los activos primarios que corresponde a tareas y procesos del negocio información y los activos de soporte, que representan:

- Hardware.
- Software.
- Redes.
- Personal.
- Sitio.
- Estructura de la organización.

4.5 GESTIÓN DE ACTIVOS

El presente apartado busca describir la etapa de vida de los bienes físicos de una organización con el fin de maximizar su valor, está constituido por el diseño, la construcción, explotación, mantenimiento y reemplazo de activos e infraestructuras. En la Tabla 2. (Ver anexo 1), se describen los tipos de activos.

4.6 EL ALCANCE Y LOS LÍMITES

Mediante este proyecto se busca implementar seguridad en la red para evitar ataques a la infraestructura informática de la Empresa Prestadora del Servicio de

Salud, de esta forma se busca potenciar la seguridad, protegiendo así la red y la información de la organización. Es esencial crear en la institución un sistema de monitoreo de red con el propósito de diseñar políticas, controles y protocolos de seguridad preventiva y correctiva que fortalezcan los procesos de calidad de la Empresa.

4.7 SEGURIDAD FÍSICA.

El blog guía prácticas. com[42] señala que la finalidad de la seguridad física es evitar el acceso físico de personas no autorizadas por la organización, que puedan causar daño a la infraestructura informática o a la red, este tipo de amenazas son analizadas y determinadas desde diferentes variables. La Tabla 2 describe los elementos que componen la seguridad física.

Tabla 2. Variables a evaluar la Seguridad Física, según las recomendaciones de la norma ISO/IEC 27001.

Variable	Recomendación Norma ISO/IEC 27001:	Control
Controles de acceso Físico	**Planeación.**	Con el propósito de prevenir el ingreso no autorizado de personas se deben implementar perímetros seguros (puertas de acceso controladas) para salvaguardar los sectores que poseen información y procesos de información sensible.
	Acciones para abordar riesgos y oportunidades.	Controlar el acceso físico a los lugares donde se almacena la información.
	Objetivos de la seguridad de la información y cómo conseguirlos	Prevenir que ingresen personas no autorizadas, por medio de circuitos cerrados de televisión, sensores de identificación, sistemas de alarmas y detección de intrusos, etc.

[42] GUÍAS PRÁCTICAS.COM. Blog Controles de acceso. 2009.

Protección contra Amenazas		Es importante que la Empresa cuente con un sistema de alarmas contra incendio, donde se pueda detectar la presencia de fuego
2. Seguridad de oficinas, Recintos	**Operación.** Planificación Operacional. Evaluación de riesgo. Tratamiento de los riesgos	Todo Ingreso de proveedores o visitantes deberá ser registrado con el personal de seguridad, se debe revisar todo bolso o paquete a la entrada y salida del recinto. No se permite el ingreso de armas de fuego, salvo a que sea personal de la fuerza pública.

Fuente: El Autor. Sistemas de seguridad de los activos

En esta tabla 3, se analiza la seguridad de los equipos en la empresa, la importancia de ubicarlos en zonas seguras para reducir el riesgo de daños, es muy importante realizar los mantenimientos periódicamente.

Tabla 3. Variables analizadas de la seguridad de los equipos (continua).

Variable	Recomendación Norma ISO/IEC 27001:	Control
Ubicación y protección de los equipos	**Evaluación de desempeño.** Supervisión, medida, análisis y evaluación. Auditoría internas Revisiones de la gestión	Es importante ubicar los equipos en zonas protegidas para mitigar el riesgo por amenazas o peligros del contexto, las posibilidades de acceso no autorizado.

Servicios de suministro		Se deben proteger los bienes contra las deficiencias en el abastecimiento de Energía. Teniendo en cuenta que la energía es bastante inestable, se sugiere instalar ups a todos los equipos de computo
Seguridad del cableado		El cableado de energía eléctrica y telecomunicaciones que transporta datos o brinda soporte a los servicios de información deben estar protegidos contra interceptaciones o daños. Se prohíbe explícitamente retirar sin autorización del departamento de sistemas equipos, información y software
Retiro de activos		
Mantenimiento preventivo y correctivos de los equipos	**Mejora** Disconformidades y acciones correctivas	Todos los dispositivos de cómputo deben adoptar periódicamente su mantenimiento para garantizar su marcha y garantizar su continua disponibilidad e integridad.
Seguridad de los equipos fuera de las instalaciones	Mejora Continúa	Se debe proveer de seguridad para los bienes fuera de las instalaciones de la organización teniendo en cuenta los distintos peligros de operar fuera de

	las instalaciones de la empresa.
Seguridad en la reutilización o eliminación de los equipos	Por seguridad es necesario verificar las piezas del equipo que abarcan elementos de almacenamiento para asegurar que se haya eliminado cualquier software licenciado e información sensible.

Fuente: El Autor. Sistemas de seguridad de los activos

5. MARCO METODOLÓGICO.

A través de un inventario exhaustivo de todos los equipos de cómputo y software instalados que se encuentran en la entidad prestadora de servicios de salud, se verifica el estado actual de cada uno para saber sus condiciones y fiabilidad, se realizará un análisis de seguridad que permitirá identificar y estructurar historiales de incidentes informáticos de la empresa, tomando así las medidas pertinentes que ayuden a minimizar los riesgos de seguridad en la organización. Posteriormente se graficará el diagrama de la red de datos de la empresa prestadora de servicios de salud, mediante la herramienta de Packet Tracer, este programa permite simular y visibilizar la red de datos que permitan detectar posibles riesgos u ataques cibernéticos.

Implementando Pandora FMS, se determinará las medidas de control a utilizar que, garanticen la protección de la red y salvaguardar la información que a diario transita en la red, esto se llevará a cabo por medio de un sistema que permita identificar intrusos o Intrusion Detection Software (Software de detección de Intrusos en adelante IDS) que se encarguen de monitorear e informar lo que sucede en tiempo real en la red. En el desarrollo de este proyecto se expondrá las políticas, controles y protocolos de seguridad que debe contemplar una organización o empresa para prevenir los incidentes informáticos; desde la identificación de vulnerabilidades que permitan actuar de manera preventiva ante amenazas que se presenten en la red, de igual manera se busca que la información enviada sea confiable, esté disponible, sea verás e integral.

Teniendo en cuenta las características de la empresa prestadora del servicio de salud; el monitoreo de la red de datos se desarrollará a partir de la identificación de los activos informáticos, determinando las falencias que se presentan en el tráfico de información de la red.

5.1 CICLO PHVA EN EL QUE SE DESARROLLARÁ EL SISTEMA DE MONITOREO.

Para el diseño y ejecución de este Sistema de Monitoreo se tendrá en cuenta el ciclo PHVA (planificar, hacer, verificar y actuar, según sus siglas). Descrito ello, de esta manera, cada componente del ciclo PHVA tendrá un protocolo especial de evaluación.

Planificar: Para el estudio de caso en específico; en esta etapa se realizará todo el proceso de análisis de los riesgos de la seguridad y los posibles incidentes que pueden presentarse en la entidad prestadora de servicio basado en la norma ISO/IEC 27001: 2013. En esta fase de planificación se organizarán y se darán a conocer los pasos a seguir para lograr eficiencia y confiabilidad en la entrega de la información. Se establecerán compromisos con cada uno de los usuarios y directivos de la organización.

De igual manera, la finalidad de esta fase es identificar los riesgos susceptibles de mejora, se establecen los objetivos a alcanzar, se fijan los indicadores de control y se definen los métodos o herramientas para conseguir dichos objetivos. Este proceso se lleva a cabo a través de un análisis de la situación actual de la seguridad y las políticas de control en la organización prestadora del servicio de educación, con el objetivo de evaluar los riesgos y los incidentes que pueden presentarse en la red de datos de la empresa.

En el proceso de planificación se realizará una exhaustiva inspección de todas las herramientas de hardware y software que actualmente tiene la organización que determinan sus funciones, resaltando la importancia de brindar seguridad en el momento de navegar en la red.

Hacer: En este segundo momento, se lleva a cabo el plan de acción, por medio de la realización de las tareas que se planificaron en la primera fase. Inicialmente se realizará una prueba piloto para probar el funcionamiento antes de realizar cambios a gran escala. De acuerdo a lo anterior, se ejecutarán e implementarán todos los controles, protocolos y políticas que generen confianza en el momento de enviar y recibir paquetes de datos en la red, supliendo así las necesidades descritas y halladas en el diagnóstico del problema.

Verificar: Una vez ejecutada la mejora se ponen en manifiesto los logros obtenidos en relación a los objetivos que se plantearon en la primera fase del ciclo mediante herramientas de control. Previamente se definirán cuáles serán las herramientas de control y los criterios para decidir si la prueba ha funcionado o no. El análisis de los resultados se llevará a cabo a través del control de todos los servicios implementados para mejorar la seguridad de la información, se realizará periódicamente un test de penetración a la red de datos para analizar el comportamiento del sistema de gestión de seguridad informática.

El propósito es evaluar la efectividad y la eficiencia de la herramienta implementada por medio de indicadores de seguridad con base en la red datos. Es importante realizar auditorías a los procedimientos y protocolos establecidos, midiendo el rendimiento de los controles que fueron establecidos para mejorar la infraestructura informática.

Actuar: Finalmente, tras comparar el resultado obtenido con el objetivo planteado, se realizan acciones correctivas y preventivas que permitan aprovechar las áreas de mejora, así como extender y aprovechar los aprendizajes y experiencias adquiridas a otros casos y así estandarizar y consolidar las metodologías efectivas. Se ejecutan las respectivas estrategias que permitan abordar de manera efectiva y eficaz siendo estos indicadores de gestión que mitiguen los riesgos e incidentes identificados, a través de medidas proactivas y reactivas para el mejoramiento del sistema de gestión de seguridad de la información.

5.2 ACTIVOS IMPORTANTES

Existen dos activos importantes en una red de datos, estos son: la información que se maneja y se manipula en las organizaciones y los servicios que la organización o empresa presta. Dichos activos describen los requisitos de seguridad para todos los demás elementos del sistema. Dentro de los datos que se maneja, debe contemplarse los requisitos legales, o si están sometidos a alguna clasificación de seguridad, según su jerarquía.

5.3 ARQUITECTURA DEL SISTEMA

Se refiere a los bienes que permiten estructurar el sistema de información, definiendo, construyendo, caracterizando, clasificando y delimitando la arquitectura interna y sus relaciones con el exterior, desde la funcionalidad (jerarquía) y el diseño de la red.

5.3.1 [D] Datos / Información.

Los datos son la fuente que permite a una organización prestar sus servicios. La información es un bien intangible que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

5.3.2 [K] Claves criptográficas

La criptografía es utilizada para guardar el secreto o autenticar la información susceptible. Los códigos criptográficos, mezclan información susceptible, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

5.3.3 [S] Servicios.

Función que satisface una necesidad o necesidades de los usuarios del servicio, en el caso específico la salud – la optimización desde la gestión de calidad por medio de la adecuación informática para los usuarios. Esta sección contempla servicios prestados por el sistema.

5.3.4 [SW] Software - Aplicaciones informáticas

Son las aplicaciones o programas que hacen parte del sistema de información, hace alusión a actividades que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones administran, examinan y modifican los datos permitiendo la explotación de la información para la prestación de los servicios.

5.3.5 [HW] Equipamiento informático (hardware)

En este parte se habla de los canales materiales, físicos, que tienen como finalidad ser el pilar directo o indirecto de los servicios que prestan las organizaciones o las

empresas, en esta parte del proceso es donde se depositan temporal o permanente los datos.

5.3.6 [COM] Redes de comunicaciones

Esta parte incorpora tanto instalaciones dedicadas por parte de las organizaciones, como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que estos son los canales que transportan los datos de una red de un sitio a otro.

5.3.7 [AUX] Equipamiento auxiliar

En un diagrama de procesos se identifican y consideran como los otros equipos que sirven de soporte o ayuda a los sistemas de información, sin estar directamente relacionados con el proceso de relacionamiento de datos, pero que influyen en cualquier tipo de tarea preventiva o correctiva.

5.3.8 [L] Instalaciones

En este segmento se describen en planos y físicos los lugares donde se ubican los sistemas de información y comunicaciones, como torres de control, de gestión y otras que influyen en el proceso comunicativo y de tratamiento de datos de una organización.

5.4 NECESIDADES DE PROTECCIÓN

La constante insatisfacción de los usuarios por el servicio prestado vía internet, fue uno de los factores que motivo a diseñar el siguiente proyecto. Analizar y proteger la red de datos en la actualidad es una gran necesidad, por la proliferación de los ciber- delincuentes que realizan ataques a las redes informáticas. La organización que es el caso de estudio es una empresa que presta servicios de salud, y maneja un gran volumen de datos con la implementación del siguiente proyecto se busca:

- Minimizar los incidentes informáticos presentados y salvaguardar la infraestructura informática.
- Mejorar la velocidad de la conectividad de la red.
- Reducir el tiempo empleado por los usuarios para realizar transferencias de datos.
- Prevenir ataques informáticos a través de suplantación o denegación de servicios.
- Tener alertas en tiempo real de los acontecimientos en la red y así poder tomar medidas para proteger la información.
- Registrar estadísticas precisas de los percances acontecidos y observar cuáles de ellos tiene mayor incidencia y realizar los correctivos necesarios.
- Capacitar a los empleados sobre los riesgos informáticos más comunes.
- Restringir los medios externos de almacenamiento a los empleados.
- Proteger las unidades de red ya que en estas carpetas compartidas se guardan información privilegiada.
- Restringir las conexiones VPN y de escritorio remoto, se debe llevar un registro de las conexiones generadas por estos usuarios.

5.5 POLÍTICAS DE SEGURIDAD

Según lo definido en el objetivo número 5 (cinco) de la presenta investigación se diseñaron políticas o controles de Seguridad al lnterior de la organización. Tras haber realizado una investigación exhaustiva se identificaron falencias, en cuanto a la capacidad de la empresa para salvaguardar la información sensible; se pudo evidenciar que en el momento no se cuenta con políticas de seguridad claras para proteger los datos, adicionalmente no se cuenta con un programa de capacitación lo que genera que algunos usuarios (colaboradores directos e indirectos) no comprendan la importancia que tiene la seguridad Informatica para las organizaciones. El diseño de la polÍtca de seguridad se elaboró teniendo como referencia los controloes de seguridad descritos en la noma **ISO 27001.** Es por ello, que se plantean los siguientes protocolos de seguridad:

- Todos los Empleados o usuarios de los recursos TIC deben preservar, respaldar y evitar accesos a la información a personas no autorizadas; es decir son responsables de cuidar todos los activos digitales y físicos de información sean o no propiedad de la Empresa.
- Los funcionarios deben seguir los procedimientos de respaldo de la información personal y llevar una bitácora de respaldos.
- Todos los sistemas de información y recursos tecnológicos utilizados para el procesamiento deben contar con mecanismo de seguridad apropiados.

- Los usuarios de TIC son responsables de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos sensibles como Usuario y Password, entre otros. Con el propósito de proteger la integridad de la información, para que esta no sea vulnerada.
- Los usuarios deben bloquear la sesión de su computador al alejarse de su puesto de trabajo, aunque sea por poco tiempo, para que su equipo no sea usado en el tiempo de ausencia.
- Se prohíbe conectar memorias USB o discos duros externos en los equipos de la institución.
- Todos los Empleados no podrán utilizar los correos institucionales para uso personal, no deben abrir correos que su procedencia es desconocida, deben informar al departamento de sistemas para ser analizados.
- Ningún usuario de los recursos TIC debe generar, compilar, copiar, almacenar, replicar o ejecutar código de computador malicioso con la intención de causar daño, perjudicar e interferir con los servicios de cualquier recurso TIC.
- El usuario no debe visitar sitios restringidos por el departamento de Sistemas de manera explícita o implícita, o sitios que afecten la productividad en la organización; como el acceso a sitios relacionados con la pornografía, juegos, Facebook, Youtube, etc.
- Está prohibido descargar software de uso malicioso o documentos que brinden información que atente contra la seguridad de la información de la Empresa.
- Está prohibido descargar Programas de Internet bajo ninguna circunstancia y en caso de requerirlo se debe informar al grupo de soporte de la Institución.

5.5.1 Para qué sirve la política de Seguridad de la Información?

Para algunas empresas, la idea de Seguridad de la Información no ha sido definida. Por tal motivo, se ignora la relevancia del mismo, y el papel que cumple en la protección de los intereses de la organización. De esta manera, la finalidad de la política de Seguridad de la Información según ISO 27001, es transferir los objetivos que la alta gerencia pretende alcanzar con la implementación del sistema. Es necesario, desarrollar un documento que resulte fácil de comprender para las partes interesadas -sin que necesariamente ellas tengan que conocer los detalles intrínsecos del sistema, como los factores de evaluación del riesgo, o quiénes son los responsables directos del sistema. Las políticas y controles de

seguridad de una organización se deben cumplir por parte de los empleados, para que allá una armonización con los sistemas de información.

5.6 IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO

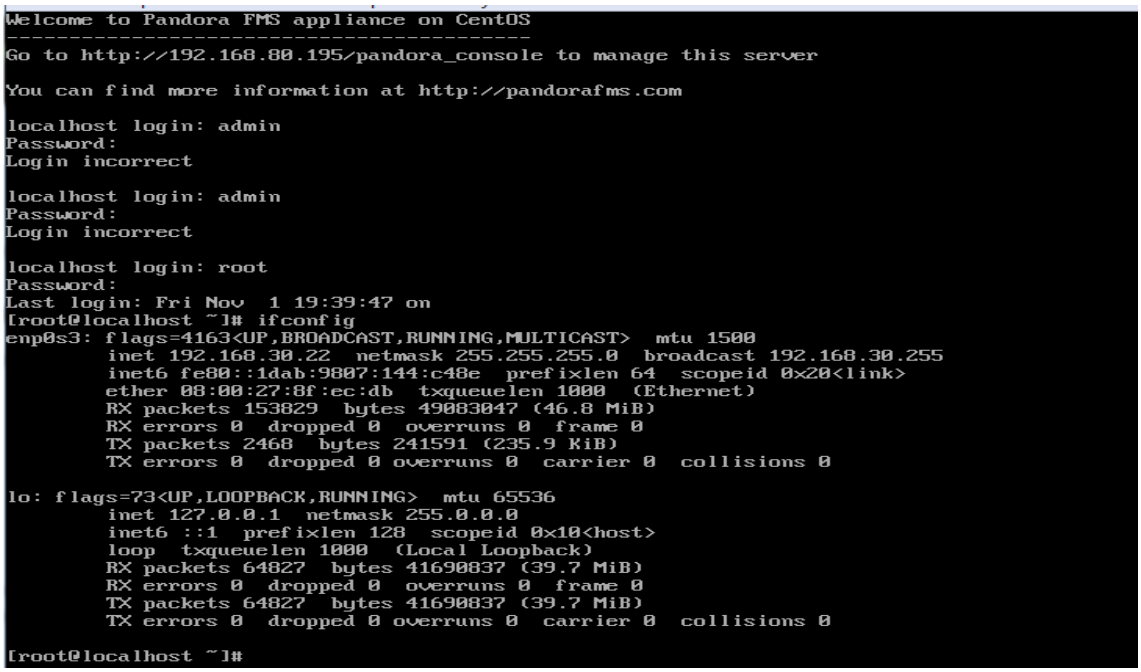
Según las falencias evidenciadas en el sistema de información actual de la organización y tras ejecutar la evaluación técnica pertinente se elige el sistema de monitoreo que supla las necesidades de seguridad de la infraestructura informática de la organización, para el presente caso se utilizará el software PANDORA FMS, por las características y controles que este posee para la realización de un eficiente monitoreo en la red.

5.6.1 IMPLEMENTACIÓN DE PANDORA FMS

El presenta acapité describe la Implementación del sistema de monitoreo de red, como se ha mencionado el software a utilizar será PANDORA FMS en su versión *OPEN SOURCE*, se puede descargar la ISO del siguiente sitio web https://pandorafms.org/es/, una vez descargado se procede a la instalación de un amaquina virtual para realizar las respectivas configuraciones de este software, si la empresa quiere seguir con el proceso de mejoramiento en su red de datos está en todo su derecho de escoger en comprar la licencia del programa o no.

Una vez instalado, el sistema debería arrancar y, tras unos segundos, mostrar el terminal donde el usuario puede ingresar sus credenciales para iniciar el servidor de PANDORA FMS. El primer paso es conocer la IP del servidor de PANDORA FMS Para poder conectarse al servidor desde fuera. Para ello, en el terminal se escribe el siguiente comando: IFCONFIG, que mostrara la IP asignada, tal como se evidencia en la figura 19.

Figura 19. Iniciar sesión en Centos y Verificar la IP del servidor.



Fuente: el autor

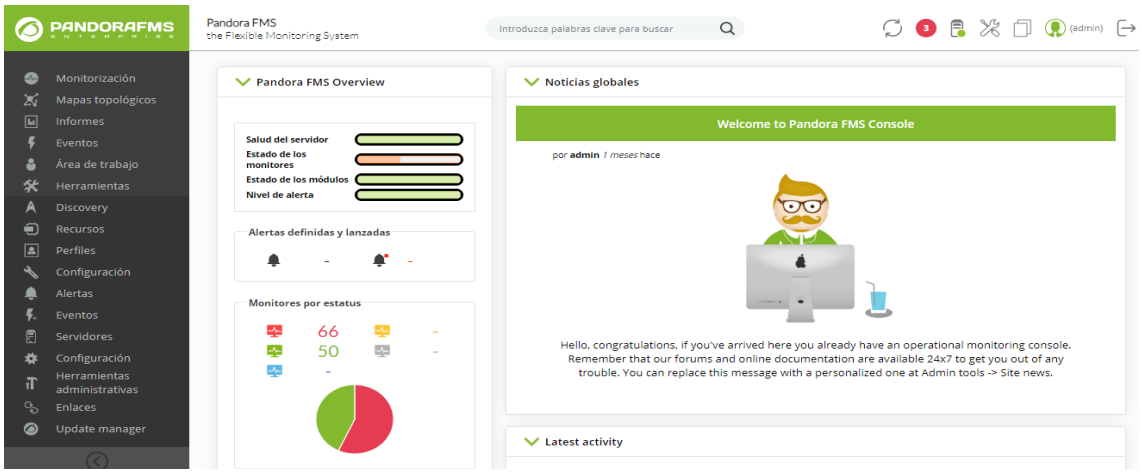
Una vez conocida la dirección IP del sistema de Pandora FMS, se puede ingresar desde fuera de la máquina virtual. Se puede hacer vía SSH o vía HTTP. Tener presente el password de root (superusuario) que se estableció en la configuración. Seguidamente se abrirá el navegador y se escribirá en él la siguiente dirección http://192.168.30.22/pandora_console que se ha obtenido en el servidor:
De esta manera se accede a la pantalla de bienvenida. Se utilizan las credenciales por defecto: usuario admin y password: pandora, como se muestra en la figura 20.

Figura 20. Inicio de sección en Pandora FMS

Fuente: el autor

Cuando se ingresan las credenciales PANDORA FMS mostrara el panel de control o los ítems que tiene el programa para su navegabilidad, tal como se evidencia en la figura 21.

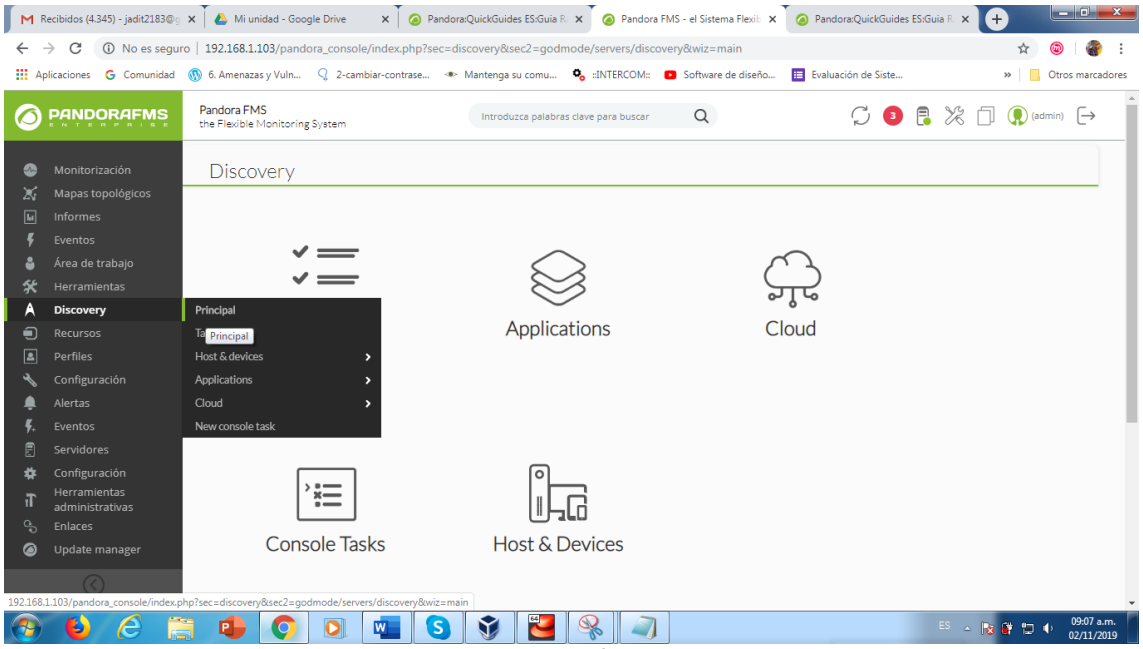
Figura 21 Panel de Control



Fuente: el autor

Creando una tarea de reconocimiento, se deben seguir los siguientes pasos. En el menú lateral se irá a la sección de “Discovery -> Principal” tal y como se muestra en la imagen. Una vez dentro, se dirige a “Host&Devices” y se hará clic en el botón “Net Scan”. Tal como se evidencia en la figura 22.

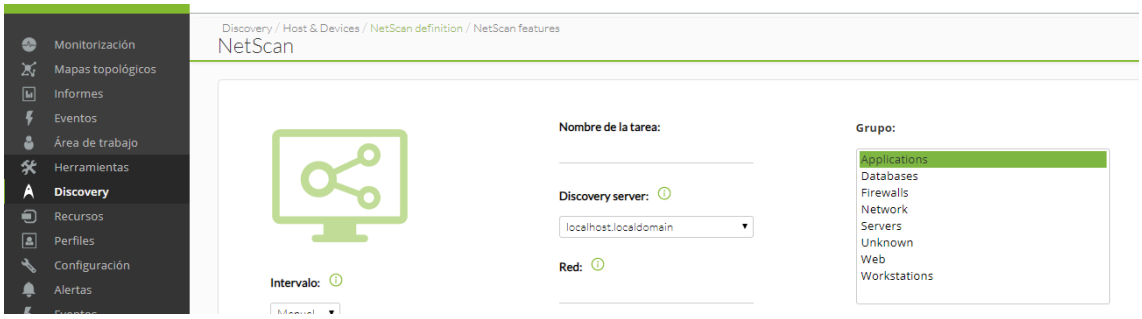
Figura 22. Crear tarea de reconocimiento.



Fuente: el autor

Se va a monitorizar el segmento 2 de la red, en esta sección se puede visualizar los dispositivos que se encuentran conectados en este segmento. Se crea la tarea para explorar, en este caso es 192.168.2.1/24, significa que todos los hosts del segmento 192.168.2.2 serán explorados. Se utilizará aquí la máscara apropiada para definir la red. Seleccionando el grupo “Applications”, que se usará para contener los dispositivos que se detectaron. A partir de ahora se llamarán de forma genérica "agentes" a los dispositivos gestionados y/o monitorizados por Pandora FMS. Ver figura 23.

Figura 23. Creación de Tarea



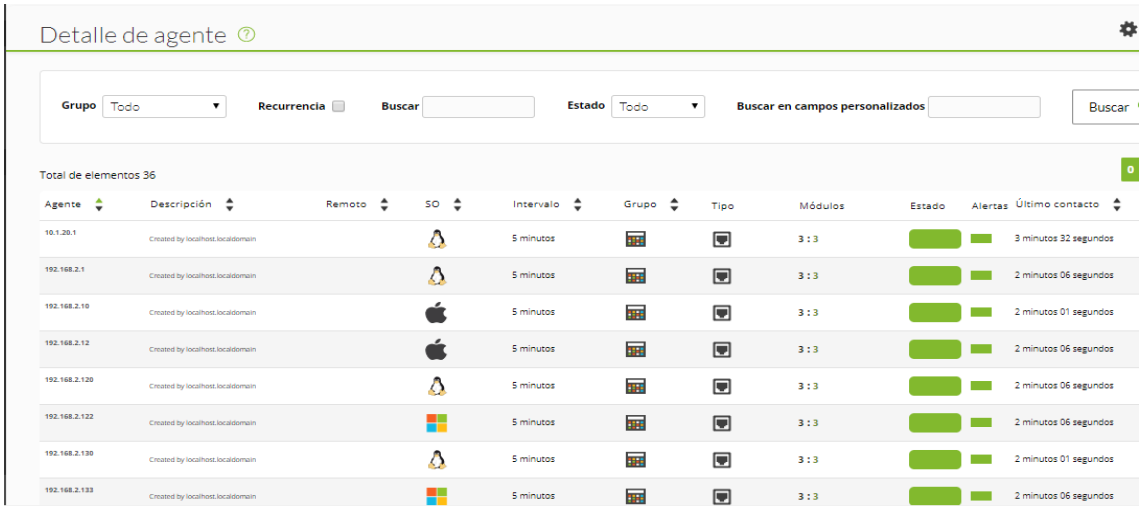
Fuente: el autor

Se ha seleccionado la plantilla de red (module template) "Basic monitoring", que cubre únicamente chequeos de latencia y disponibilidad de red. Se podrán seleccionar otro tipo de chequeos, como SNMP o WMI, a realizar durante el reconocimiento.

5.7 REVISANDO LOS SISTEMAS DETECTADOS

En este punto es mejor que se espere a que toda la red haya sido detectada. Cuando se haya terminado, se accederá a la vista de detalle de agentes para ver todos los sistemas detectados. Menú "Monitoring" > "Views" > " "Agent detail", tal como se ve en la figura 24.

Figura 24. Host Detectado



Fuente: el autor

Aquí se puede observar varios agentes que han sido correctamente detectados por Pandora FMS. En algunos casos se habrá resuelto el nombre del sistema (si por DNS era posible) y en otros habrá detectado el Sistema Operativo. Al hacer clic en el nombre (en este caso, el primero de la captura) se irá a la vista de detalle del agente, que mostrará toda la información de ese sistema, tal como se representa en la figura 24 a.

Figura 24 a. Información del sistema detectado

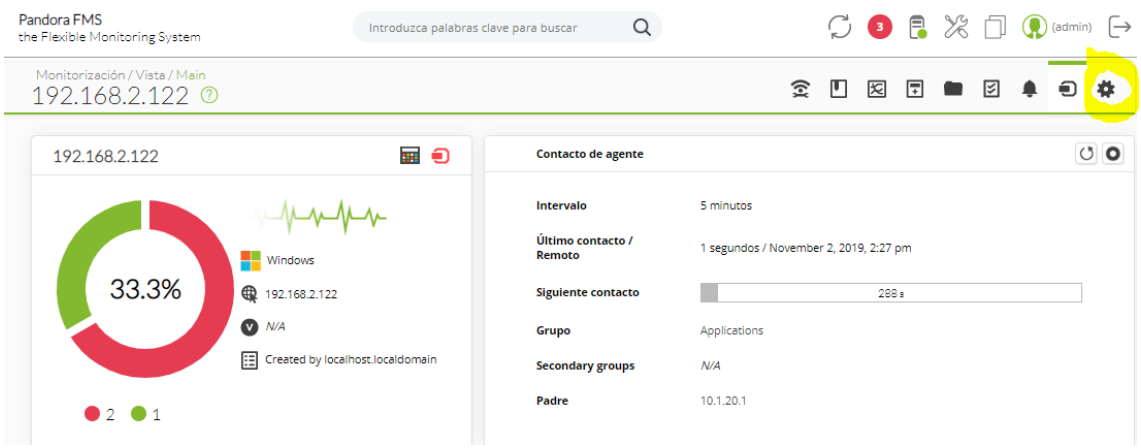
Fuente: el autor

5.8 TRÁFICO DE RED EN INTERFAZ

Para ello es esencial que el SNMP esté configurado en el dispositivo remoto. Esto generalmente necesita activarse, y una configuración mínima que permita consultar datos. Los dispositivos SNMP permiten configurar las IP que pueden hacer consultas y con qué comunidad, que a todos los efectos es una especie de password.

Primero se ubicará el agente de donde se quiere conseguir el tráfico de red; en este caso es 192.168.2.122. Siguiendo el mismo proceso (Monitoring > Views > Agent detail) se llega a la vista principal del agente que se quiere configurar y se hará clic en la última pestaña de la derecha, que llevará a la vista de edición de ese agente. (Gestionar). Ver figura 25.

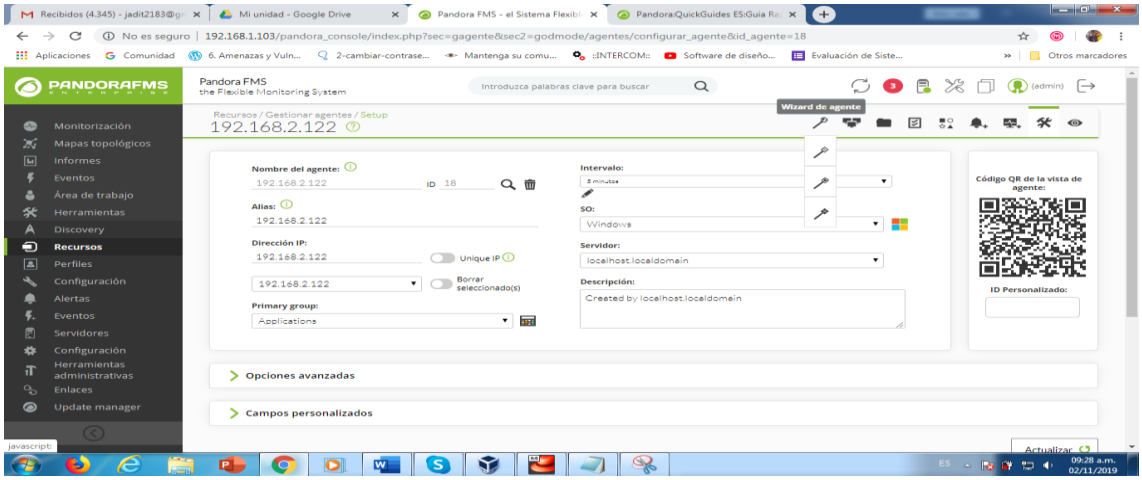
Figura 24. Tráfico de red.



Fuente: el auto

Se pasará a la vista principal de edición del agente. Aquí se mostrará el submenú de "Wizards" de configuración para este agente, donde se escogerá el Wizard de Interface SNMP, tal como se ve en la figura 26.

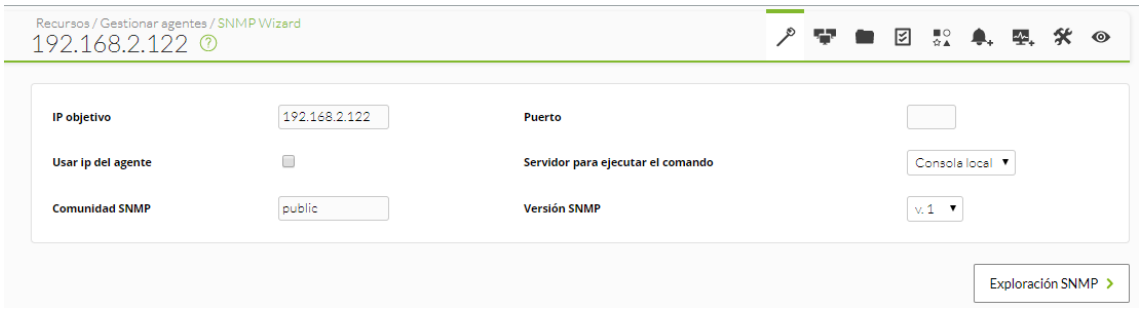
Figura 25. Wizards



Fuente: el autor

En este punto se debe facilitar la comunidad SNMP que tiene configurada el equipo, y asegurarse que el sistema tolera consultas SNMP habilitadas en la IP que se muestra en la pantalla. Se puede cambiar la IP y la comunidad SNMP por defecto, que es pública. Una vez esté relleno, se le dará al botón "SNMP Walk, tal como se evidencia en la figura 27.

Figura 26. Exploración de SNMP



Fuente: el autor

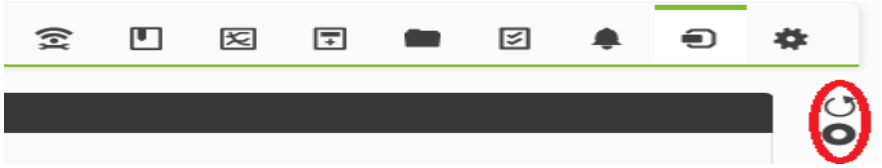
Se pulsa en el botón "Create modules" y una pantalla debe informar que los módulos se han creado.

Hay que tener en cuenta que los módulos de tráfico de red son de tipo incremental, es decir, que su valor es la diferencia entre la muestra de información que se acaba de recoger y la anterior. Muestra una "tasa" (en este caso en bytes/sec), de forma que necesita un tiempo (entre 5 y 10 minutos) antes de mostrar nada.

Se hace clic en la pestaña "View" para volver a la vista del agente y se espera 5 minutos hasta que ya se tengan datos de tráfico, actualizando o haciendo clic en la pestaña "View". Después de un tiempo se debería tener una pantalla similar a esta, donde ya se tienen datos de los módulos de tráfico (entrada y salida, por separado) y una nueva sección en el agente, que muestra información de las interfaces con un acceso directo a una gráfica agregada con el tráfico de salida y entrada superpuesto (si se hace clic en el título donde dice "Interface information (SNMP)").

Si no se quiere esperar más o se quiere "forzar" la ejecución de los módulos de red, se puede utilizar el icono de forzar chequeo remoto (no funcionará con los módulos locales, o recogidos en local por un agente software). En función de la carga del servidor, puede tardar entre 2 y 15 segundos en ejecutar la prueba de red, tal como se evidencia en la figura 28.

Figura 27. Actualización para recibir los datos del tráfico.



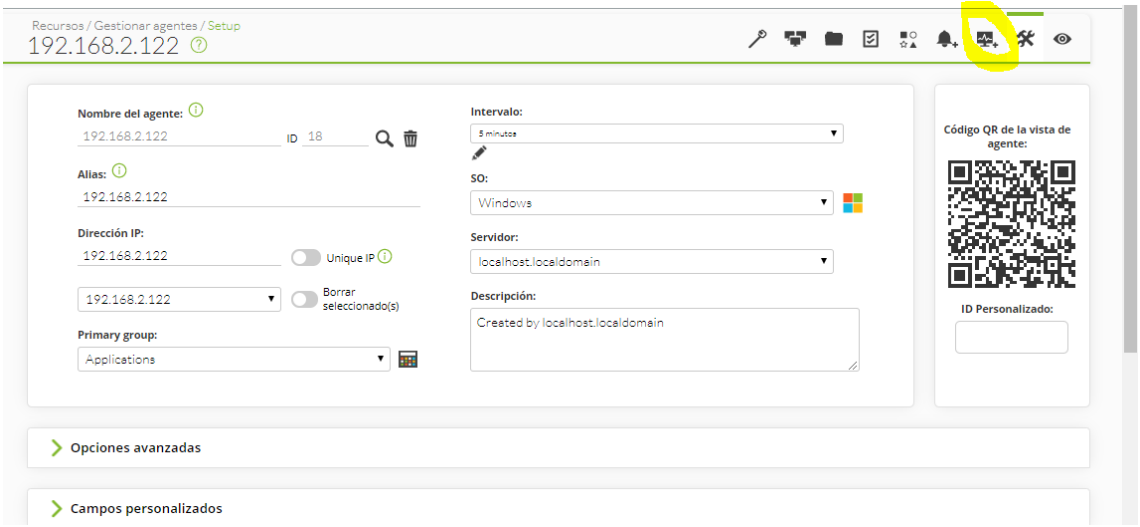
Fuente el autor

La información de los módulos de tráfico se verá de esta manera, y las gráficas para cada métrica, pulsando en el icono de gráfica  mostrará una ventana con la gráfica de ese monitor y al pulsar en el icono de datos  , una tabla con los datos.

5.9 PÉRDIDA DE PAQUETES EN LA RED

Se quiere agregar un plugin remoto pre configurado en Pandora FMS. Los plugins remotos son chequeos definidos por el usuario que emplean un script o un programa que se ha desplegado en el servidor de Pandora FMS, de forma que este pueda utilizarlo para monitorizar, ampliando el conjunto de cosas que puede hacer. Se usará un plugin de serie; para ello, se dirige a la vista de edición del agente y luego a la solapa de configuración de módulos. Tal como se evidencia en la figura 29

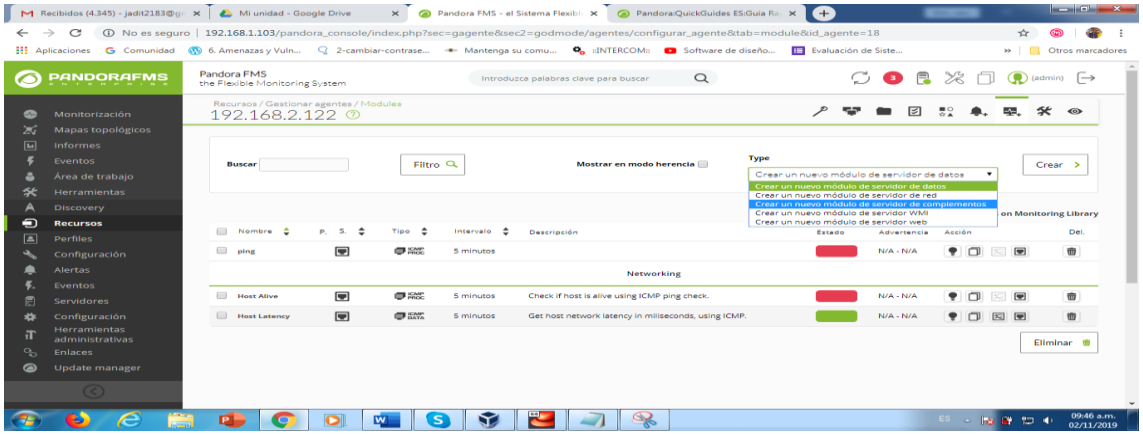
Figura 28. Vista de edición.



Fuente: el autor

Se escoge un módulo de tipo plugin y se le da al botón de "crear", que llevará a la interfaz de configuración de módulos de tipo "Plugin remoto". Tal como se evidencia en la figura 30.

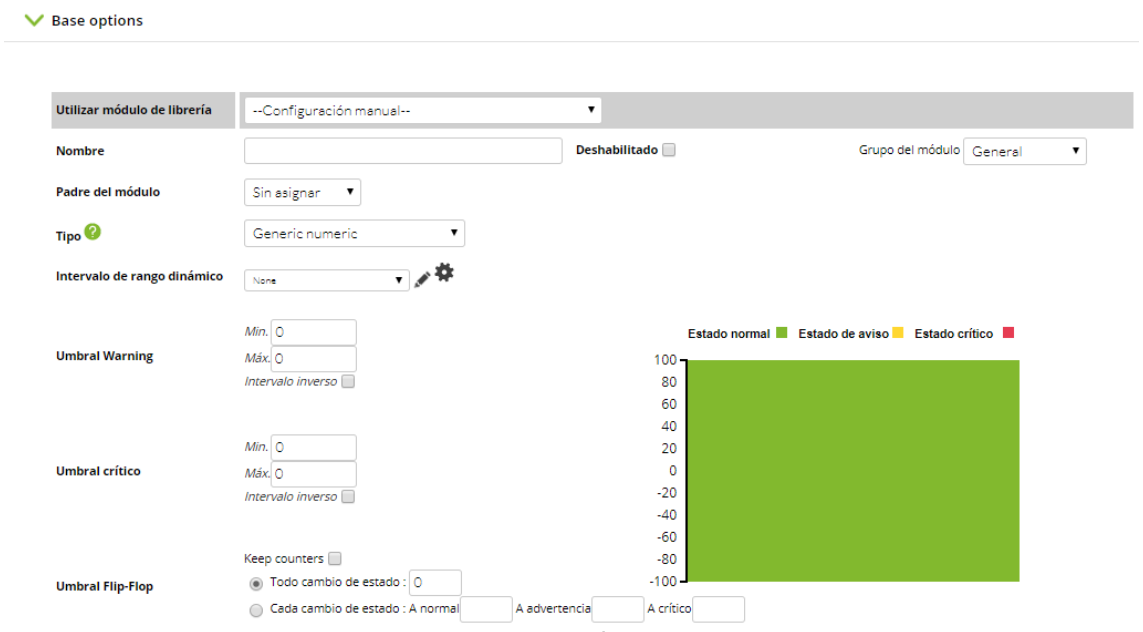
Figura 29. Tipo de Plugin



Fuente: el autor

Se escoge el plugin "Package loss" utilizando los desplegables, y finalmente se pondrá la IP sobre la que se quiere lanzar el chequeo. El resto de campos se dejan como están. Ver figura 31

Figura 30. Configuración de la IP



Fuente: el autor

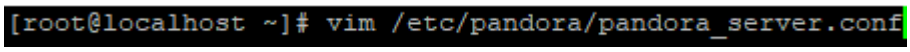
Se hace clic en el botón "Crear" y se vuelve a la vista de operación, como en el caso anterior. Se actualiza un par de veces la pantalla, hasta que el nuevo módulo aparezca en la lista.

5.10 AÑADIR UNA ALERTA (ENVÍO DE EMAIL) ANTE UN PROBLEMA

La primera alerta que se va a ejecutar consiste simplemente en enviar un email cuando se caiga una de las máquinas que ya se están monitorizando (con el módulo Host alive). Las alertas en Pandora FMS están compuestas por tres elementos: Comando, Acción y Plantilla. En este caso concreto se va a utilizar un comando predefinido (envío de emails), se va a modificar una acción que ya existe (Mail to ejemplo123@gmail.com) se utilizara una plantilla que también existe ya, la plantilla Critical condition, que ejecutará la alerta cuando el módulo en cuestión aparezca en estado crítico.

Para el correcto funcionamiento del comando email se debe configurar en el fichero pandora_server.conf un servidor de correo que permita hacer relay. En el ejemplo, el servidor de correo situado en el localhost mediante postfix. Se debe poner la IP del servidor de correo local, o uno en Internet (configurando para ello la autenticación). Para modificar el fichero de configuración del servidor se debe acceder a él, situado en /etc/pandora/pandora_server.conf como usuario root, por lo que antes de hacerlo se debe hacer root con sudo su. Ver figura 32.

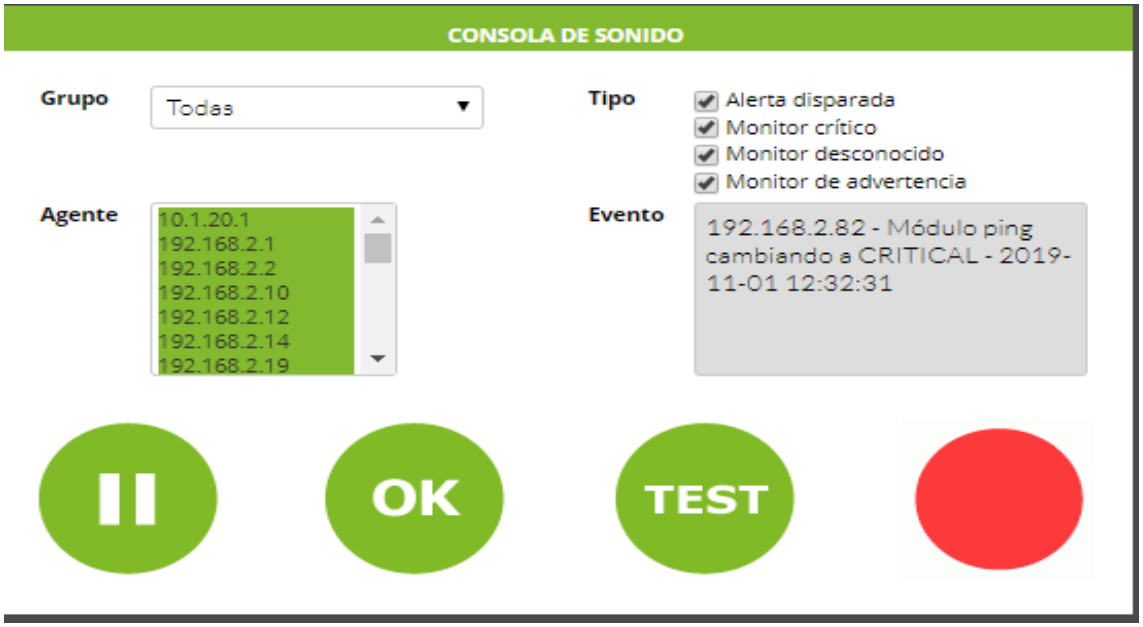
Figura 31. Añadir Alerta



Fuente: el autor

En la consola de sonido se escuchar los eventos o incidentes que hay en los dispositivos, ya que comienza a emitir un sonido como especie de una alarma y el botón rojo se pone en movimiento. Ver figura 33.

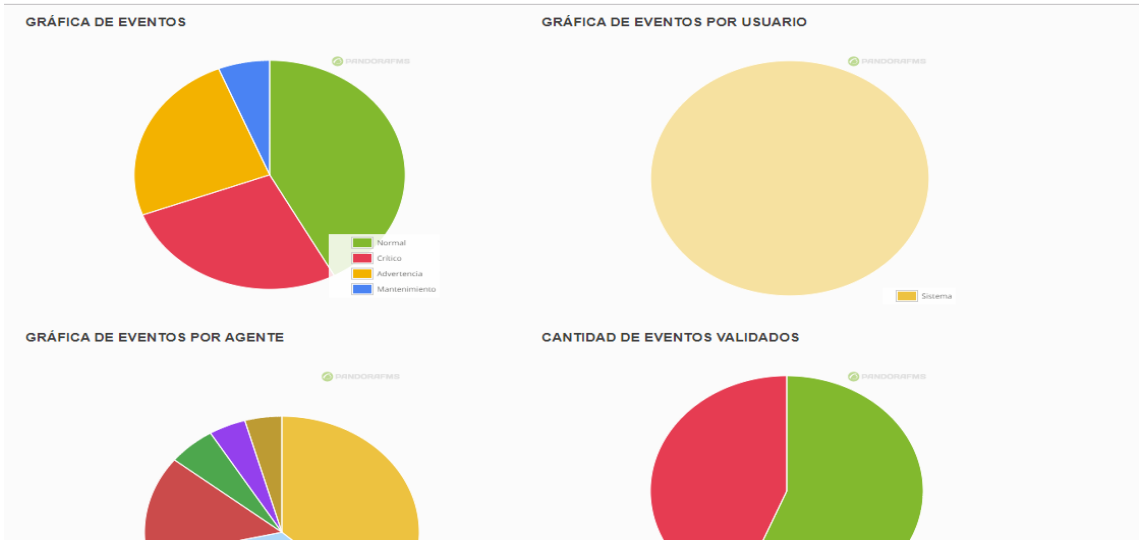
Figura 32. Sonido de incidente



Fuente: el autor

En la figura 34, se puede observar las estadísticas de los agentes.

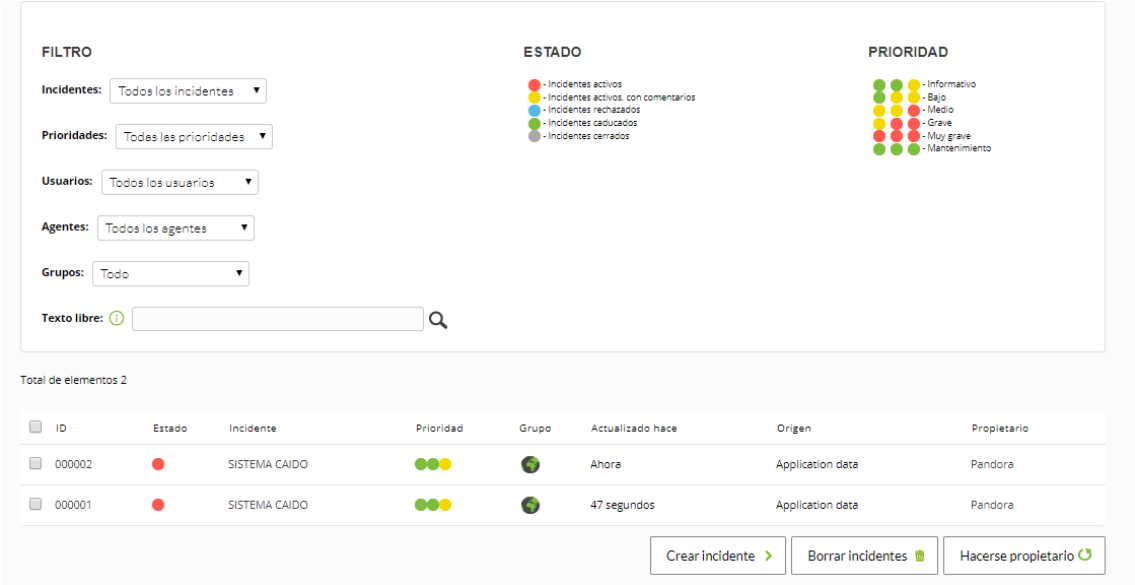
Figura 33. Estadística. Fuente y elaboración el autor



Fuente: el autor

En la figura 35 se observa el estado y la Prioridad de los Incidentes.

Figura 34. Gestión de incidentes.



Fuente: el autor

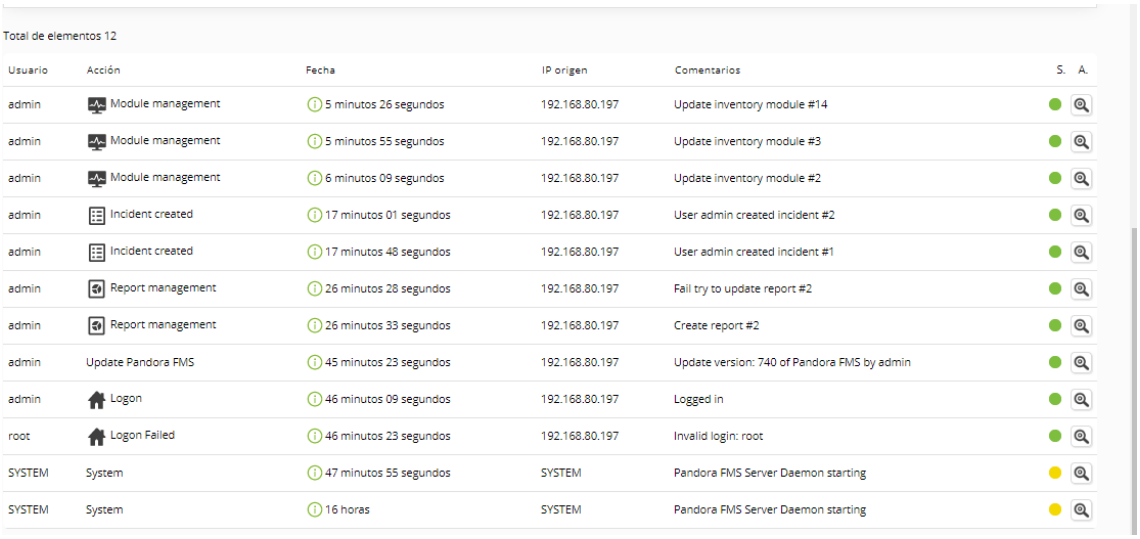
Estadísticas de Incidentes, se debe hacer clic en una de las gráficas, se puede observar cuantos incidentes por usuarios o por grupo se tuvieron de manera porcentual, tal como se evidencia en la figura 36

Figura 35. Estadísticas de Incidentes

Fuente: el autor

En la figura 37 se describen los informes que realiza el mismo sistema.

Figura 36. Auditoria



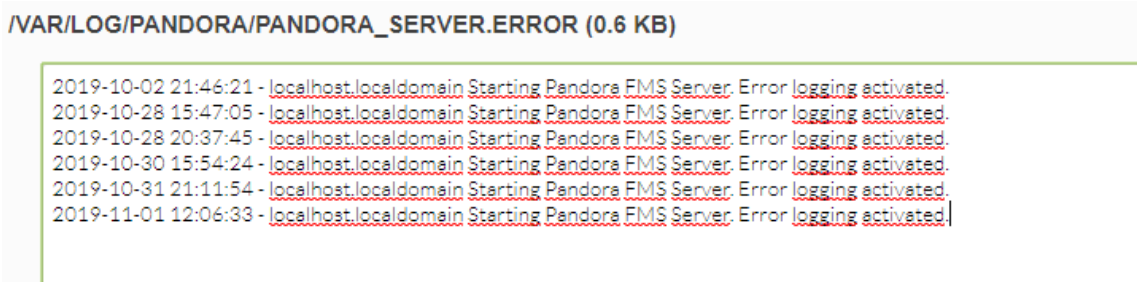
Total de elementos 12

Usuario	Acción	Fecha	IP origen	Comentarios	S.	A.
admin	Module management	5 minutos 26 segundos	192.168.80.197	Update inventory module #14		
admin	Module management	5 minutos 55 segundos	192.168.80.197	Update inventory module #3		
admin	Module management	6 minutos 09 segundos	192.168.80.197	Update inventory module #2		
admin	Incident created	17 minutos 01 segundos	192.168.80.197	User admin created incident #2		
admin	Incident created	17 minutos 48 segundos	192.168.80.197	User admin created incident #1		
admin	Report management	26 minutos 28 segundos	192.168.80.197	Fail try to update report #2		
admin	Report management	26 minutos 33 segundos	192.168.80.197	Create report #2		
admin	Update Pandora FMS	45 minutos 23 segundos	192.168.80.197	Update version: 740 of Pandora FMS by admin		
admin	Logon	46 minutos 09 segundos	192.168.80.197	Logged in		
root	Logon Failed	46 minutos 23 segundos	192.168.80.197	Invalid login: root		
SYSTEM	System	47 minutos 55 segundos	SYSTEM	Pandora FMS Server Daemon starting		
SYSTEM	System	16 horas	SYSTEM	Pandora FMS Server Daemon starting		

Fuente: el autor.

En la figura se evidencia el Visor de archivos de log del sistema

Figura 37. Visor



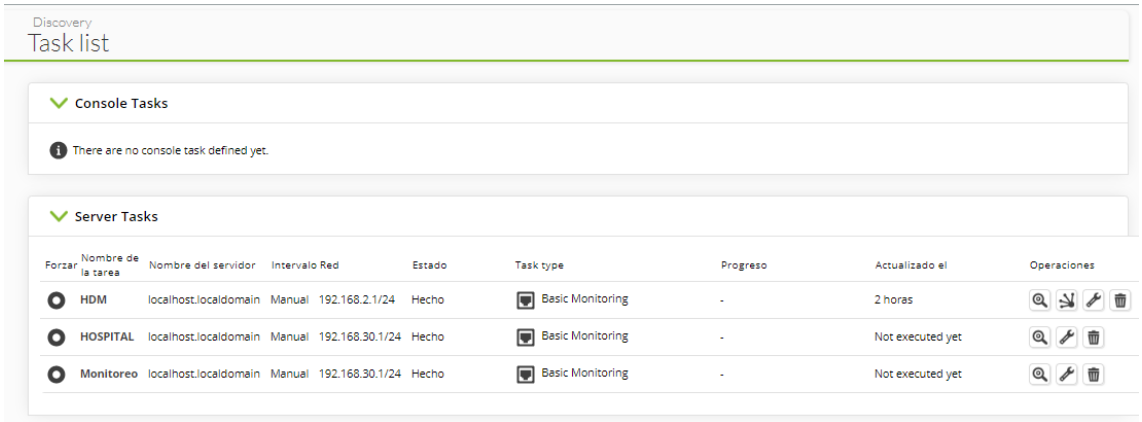
Fuente: el autor

Se procede a realizar un escaneo para verificar los puertos que se encuentran abierto, ver figura 39.

Figura 38. Puertos abiertos

La clasificación y segmentación de la lista de los segmentos de red agregado al software se describen en la figura 40

Figura 39. Red



Fuente: el autor

Una de las ventajas que ofrece Pandora FMS, es que se puede verificar el estado de los agentes desde cualquier lugar si tiene una conexión a internet, también se tiene información al instante cuando suceda algún incidente en los dispositivos.

6. CONCLUSIONES

En la actualidad las Empresas modernas han centrado en gran parte de su actividad económica a través de internet, es por ello que existe la necesidad de dotar la infraestructura informática de las medidas y políticas que protejan adecuadamente y garanticen el desarrollo constante y sostenible de las actividades que se realizan a diario. En este orden de ideas, se hace necesario que las organizaciones cuenten con profesionales especialistas en las nuevas tecnologías de la seguridad informática, para que se pueda implementar y gestionar controles y medidas de seguridad efectivas.

Es de conocimiento que la información se ha convertido en uno de los activos de muchísimo valor, el cual se debe resguardar o proteger y asegurar para garantizar su integridad, disponibilidad y confidencialidad.

Después de haber hecho el análisis de la red de datos se concluye que dado el número de equipos y servicios de red es de suma importancia que la persona encargada de administrar la red cuente con el acceso total de monitorizar la red y de manera indispensable para que de esta forma se pueda desarrollar una labor más efectiva de prevención y corrección; con el propósito de salvaguardar la información que a diario circula por la red y de esta manera controlar eficazmente el tráfico de datos para que estos o sean alterados o modificados por intrusos.

Utilizar Pandora FMS como herramienta principal de monitoreo proporciona cubrir la mayoría de las necesidades de monitoreo y requerimientos de red planteados por la empresa, existen otras herramientas que pueden ayudar a complementar las bondades que ofrece el software en mención, como Nagios, que también es una herramienta bastante utilizada para realizar esta actividad, al ser todas ellas software libre permiten abaratar costos en la implementación del sistema de monitoreo de la red.

Con la implementación de este sistema de monitoreo se mejorará el número de incidencias y la repuesta a los incidentes será casi que inmediata, ya que el administrador será notificado a través de correo electrónico, para que toma las medidas pertinentes para no permitir que los incidentes pasen a un problema mayor, esto con la finalidad de mantener la infraestructura informática protegida y que la información sea integra y esté disponible para las personas autorizadas.

7. RECOMENDACIONES

Capacitar al personal que labora en la Empresa sobre la importancia de proteger los activos de información con la finalidad de evitar acceso no autorizado al sistema. Es necesario realizar periódicamente, según los objetivos corporativos una retroalimentación para ir afianzando los conceptos de seguridad de la información y evitar caer en prácticas inadecuadas que afecte el funcionamiento de la red y de la información que a diario transita por esta. El personal encargado de administrar la red realizará periódicamente revisiones del funcionamiento de la aplicación que se está utilizando para el monitoreo de la red (PANDORA FMS). De igual manera, se tendrán en cuenta las alertas generadas por el programa para mitigar el riesgo y de inmediato tomar las correcciones necesarias para salvaguardar la integridad y disponibilidad de la información.

Es recomendable hacer las actualizaciones del software siempre que haya una disponible, porque a través de las actualizaciones muchas veces se corrigen errores de seguridad. Ejecutar constantemente el análisis de vulnerabilidad con el fin de tener claro dónde están las brechas que pueden afectar el sistema de información e instalar antimalware en todos los Equipos.

8. RESULTADO

Con la implementación del sistema de monitoreo de red en la Empresa se evidencian con facilidad las alertas en tiempo real, de las amenazas informáticas que se gestan en la red, esto lleva al administrador del sistema a tomar los correctivos para que estas amenazas no surjan efectos adversos en el sistema de información de la organización. Se observa el cambio de actitud de los empleados acogiendo el buen hábito al momento de utilizar las herramientas de información de la Institución.

Anexos

Anexo 1

Tabla 4. Inventario de Activos.

Tipos de Activos	Nombres	Características	Control
COMUNICACIONES [COM]	Mikrotik RB1100AHx2	Es de gran rendimiento y con un CPU Dual hasta un millón de paquetes por segundo 2 GB de RAM SODIMM, tiene una ranura para micro SD, un beeper y un puerto serial, viene instalado con un radio de aluminio.13 puertos, cantidad 3	Controla el tráfico del ancho de banda. Se recomienda realizar periódicamente mantenimiento preventivo y correctivo
	Switches hp	Switches HP de 48 puertos, capa 3 Cantidad: 6	Para su buen funcionamiento y protección deben estar conectados a la corriente regulada y tener buena ventilación.
	Router	Se conectan a la red LAN por	Para la seguridad de la

		medio de un cable UTP, difunde conexión inalámbrica a través de una red WIFI.	red se debe asignar una contraseña y colocarle una IP estática
	Transceiver	Es un dispositivo que se encarga de realizar funciones de recepción de una comunicación, contando con un Circuito Eléctrico. Cantidad:4	+13
I	Router Inalámbrico Rompe muros, 3BUMEN	Cuenta con dos antenas de 5dBi cada una y su alcance con línea de vista es de aproximadamente 1000 m, pueden alcanzar velocidades de trasmisión de hasta 300Mbps. Cantidad: 3	Periódicamente se le debe realizar actualización del software.
HARDWARE [HW]	Impresoras Ricoh Multifuncionales	Impresoras Ricoh Multifuncional Cantidad 35.	Están distribuidas en los siguientes servicios, facturación, hospitalización, pediatría, quirúrgica, urgencia adulto, urgencia triage, medicina interna, ginecología,

			cirugía, consulta externa, cada tres meses se le realiza mantenimiento preventivo y correctivo
	Impresoras HP	Las impresoras HP son utilizadas en los consultorios de consulta externa y de TRIAGE Urgencias, con el fin de imprimir las ordenes y la historia clínica del paciente. Cantidad 45	Las referencias de los equipos son HP mp 1102, mp 1212 y mp 127, cada tres meses se les debe hacer mantenimiento, la persona encargada de estos equipos debe estar pendiente y reportar en el sistema de información que se maneja en la empresa lo que se le realizo a cada máquina.
	Computadoras de Escritorio	Las computadoras de escritorio se utilizan para facturar y realizar las historias de los pacientes. Cantidad 250	Están distribuidos en las siguientes áreas, urgencias, admisiones, laboratorio, banco de sangre, pediatría hospitalización, quirúrgica, UCI

			adulto, UCI intermedio, sala de capacitación, medicina interna, administración, gerencia. Cada coordinador de área es responsable de cada computador y reportar al área de sistemas que hay alguna afectación en el equipo.
	Computadores Portátiles	Los portátiles se utilizan para realizar la ronda, que los médicos hacen todos los días en los servicios. Cantidad 8	El coordinador médico es la persona responsable de estos equipos, reportara al área de sistemas cualquier inconsistencia con los equipos, cada tres meses se les deben realizar sus respectivos mantenimientos
	Office	Office 2010	Se utiliza el 2010, se les ha indicada a los colaboradores

			utilizar Google drive.
I	E-MAIL	Todos los colaboradores deben tener correo institucional	Los correos electrónicos se crean en Bogotá, y es obligatorio que todo empleado lo tenga.
	SIOS	Es el sistema de información que se utiliza para la realización de facturación e Historia clínica de los pacientes, tiene versión web y escritorio.	Es imprescindible adoptar medidas de seguridad para el sistema para prevenir ataques. Nivel de acceso de usuarios, antivirus licenciado, etc
	ANNARLAB	Sistema de información para la validación de laboratorios, se comunica con SIOS a través de webservice, tiene versión escritorio y web.	La versión del Sistema operativo es Linux Centos 5, se debe actualizar el sistema operativo, ya que la versión 7 de CENTOS tiene un nivel de seguridad más alto.

	OCULUS	Software que se utiliza para la realización de RX o imágenes diagnosticas	Trabaja sobre Windows Server r2
	ITOOL	Sistema que se utiliza para la recepción de las ordenes, entrega y facturación de medicamentos.	A través de este software se lleva el control de los medicamentos entregados y la existencia que hay en bodega
ACCIÓN FÍSICA	ARCHIVO	A través de este software se lleva el control de los medicamentos entregados y la existencia que hay en bodega	No dejar acceder a persona ajena al servicio, tener la precaución de no encender elementos en esa área.
	Activos de Información Digital	Los backup de las bases de datos se encuentran en discos duros externo	Es responsabilidad de la persona encargada de los respaldos de las bases de datos de ubicar estos discos en un lugar seguro.
	Funcionarios	Aproximadamente la empresa cuenta con 500 colaboradores	Los colaboradores deben registrar su huella a la hora de entrada y salida del trabajo.

	Usuarios externos	Existen dos sedes que se conectan a través de VPN y radioenlace	Llevar un registro de las personas que se conectan por VPN y por escritorio remoto
DIGITAL [D]	Administradores de base de datos	Persona encargada de realizar mantenimiento y los backup de las bases de datos	Los procedimientos de los respaldos se debe realizar todos los días y salvaguardar los medios donde se almacena la información

Fuente: Autor. Inventario de una Empresa Prestadora de Servicio

RESUMEN ANALITICO EDUCATIVO – RAE

INFORMACIÓN GENERAL

Título del texto	**Diseño e implementación de un sistema de monitoreo a la red de datos del sistema hospitalario.**
Autor	Jadit Guerrero Molina
Edición	**Universidad Nacional Abierta y a Distancia**
Fecha elaboración	08 de Diciembre de 2018

Palabras Claves

Activo, bases de datos, amenaza, auditoria, cifrado, clave encriptada, contraseña, criptografía, declaración de aplicabilidad, impacto, política, riesgo, salvaguarda, seguridad, vulnerabilidad.

Descripción: Proyecto aplicado para optar por el título de Especialista en seguridad informática de la Universidad Nacional Abierta y a Distancia. El proyecto tiene como propósito diseñar un Sistema de Monitoreo de red informática de la Empresa Prestadora del Servicio de Salud garantizando un óptimo funcionamiento de la red informática.

El monitoreo de seguridad de red en las organizaciones es una tarea vital a la hora de detectar ataques de malware y problemas en la red. Al analizar los protocolos de seguridad se puede dar una pronta respuesta ante amenazas y así de proteger los activos de información.
.

La gestión de la seguridad es un proceso complejo de mejora continua y de constante adaptación a los cambios del entorno. Las tres dimensiones principales son: La confidencialidad entendida como garantía del acceso a la información únicamente de usuarios autorizados; integridad, como la preservación de la información de forma completa y exacta y disponibilidad como el respaldo de acceso a la información en el instante en que el usuario la necesita.

En el desarrollo de la presente propuesta, se aprecian los resultados producto del desarrollo de las etapas de Planificación, Ejecución,

Seguimiento y Mantenimiento y se formulan varias oportunidades de mejora, dentro de las cuales se destacan como estrategias de continuidad del proyecto el autodiagnóstico, el cumplimiento de compromisos, simulacros de materialización de riesgos y contratación de consultorías para realizar mediciones objetivas de la ejecución del sistema. Lo que se pretende es que la organización prestadora del Servicio de Salud tenga una red de datos a la altura de una administración segura, completa e íntegra, que se establezca una ruta de implementación de procedimientos capaces de ayudar a mejorar en el monitoreo y gestión de la misma, permitiendo no solo monitorear, si no evaluar, analizar y controlar sus recursos, con el fin de lograr mantener niveles de trabajo y de servicio adecuados, dado que del buen funcionamiento de la red dependerá que se pueda controlar la vulnerabilidad y la confidencialidad de los datos.

Fuentes bibliograficas:

[1] MARTIN, sara. Monitorización de Sistemas Informáticos. Pandorafms (Monitoring Blog) [online], 21 Agosto 2017. Encontrado en: https://blog.pandorafms.org/es/monitorizacion-de-sistemas/

[2] MARQUETING. Las 10 mejores herramientas de Monitoreo de Redes del 2017. Apen 25 (Soluciones Globales en Informática y Tecnología) [online], 2017. Encontrado en: https://apen.es/2017/03/10/las-10-mejores-herramientas-de-monitoreo-de-redes-del-2017/

[3] ESTRELLA, Jorge. Tipos de topología. [online]. Encontrado en: http://jorge-star.galeon.com/INDICE.html

[4] ANANGUREN, amarilis_204A1. Clasificación de Redes según el tamaño. (Redes de Computadora). [online], 30 Junio 2017. Encontrado en: https://redcomputadora.wordpress.com/2016/06/30/tipos-de-redes-segun-el-tamano/

[5] ISOTools. Qué debe incluir la Política de Seguridad de la Información según ISO 27001. (Blog calidad y excelencia). [online], 9 Abril 2017. Encontrado en: https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/

[6] AVANCE, jurídico. Ley 1273 de 2009. (Casa Editorial Avance Jurídico Ltda). [online]. 5 Enero 2009. Encontrado en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[7] GÓMEZ VEITIS, alvaro. Tipo de ataques e intrusos en las redes informáticas. [en línea]. [Caixanova, Madrid]: s, f. Disponible en Internet:

https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

[8]. JUNCO ROMERO, Gerardo y RABELO PAUDA, Sonia. Los Recursos de Red y su Monitoreo. [en línea]. Texinfo, 1 ed. [Cuba]. Revista Cubana de Informática Médica. 1 Octubre 2018 [citado 25 Agosto 2019]. Disponible en Internet en: https://www.javerianacali.edu.co/sites/ujc/files/normas_icontec.pdf

[9]. HEINEHKEN, team. Introducción a la problemática de la seguridad informática. [en línea]. Seguridad y Protección de la Información [citado 25 Agosto 2019]. Disponible en Internet: http://www0.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf

[10]. CRISTIA, Máximiliano. Seguridad Informática. [en línea]. [Rosario, Argentina] 2018, [citado 25 Agosto 2019], Disponible en Internet: https://www.fceia.unr.edu.ar/~mcristia/apunte-si.pdf

[11] Sistemas de Autenticación. Disponible en Internet: http://seguridadensistemascomputacionales.zonalibre.org/Sistemas%20de%20Autenticaci%C3%B3n.pdf

Contenidos

Metodología:

Se toma como base la norma NTC-ISO-IEC 27001, la que utiliza el ciclo PDCA: Planear – Hacer- Verificar - Actuar. Dividido en las siguientes etapas: Planificación, Ejecución, Seguimiento, Mantenimiento y Mejora y la metodología a emplear para realizar el análisis y formular un plan para gestionar los riesgos.

Seguimiento:
marc
Proponer procedimientos de monitorización y revisión, mantenimiento y Mejora Sugerir acciones preventivas y correctivas sobre la red informática del sistema hospitalario.

La seguridad informática es un campo bastante amplio y en constante cambio y evolución, sobre el cual, no se ha dicho la última palabra; por lo anterior, el ambicionar la implementación de un sistema de monitorización de la red para cualquier entidad requiere de esfuerzo e inversión.
.
En la presente propuesta, se realizó un levantamiento de activos con que cuenta el HDM, un reconocimiento de las amenazas, el plan de tratamiento de riesgos y la definición de los responsables de las tareas entre otros, sin embargo, constituye solamente la piedra angular para la construcción de un sistema de monitoreo de la red hospitalaria.
Es vital aprovechar los resultados de este Plan, con miras a generar una cultura de control y seguridad, permitiendo que cada empleado/usuario sea consciente de las amenazas a que está expuesta la entidad por ésta razón se dejan definidos: los comités, sus funciones, los documentos, el plan de capacitación, las actividades, los procedimientos, y una metodología para las pruebas a realizar.

Conclusiones:

Diariamente aparecen nuevos y complejos tipos de incidentes informáticos y se registran fallas de seguridad de fácil resolución técnica, en ocasiones ocurren algunos casos por falta de conocimientos de los empleados sobre los riesgos informáticos más comunes. Los incidentes de seguridad están impactando de forma cada vez más directa sobre los seres humanos. Es por ello que se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas, para prevenir esta clase de incidentes repentinos por parte del personal. Es necesario realizar retroalimentación periódicamente para proveer y eludir dichos ataques informáticos.

Es importante que la red de información de la organización prestadora del servicio de salud mantenga un estado de alerta y de actualización permanente: la seguridad es un proceso continuo que demanda aprender sobre las propias experiencias.

Las organizaciones o empresas no deben considerar la seguridad de la información como un proceso o un activo aislado de los demás. La seguridad informática debe formar parte fundamental de las organizaciones. Por esta razón se hará un trabajo de concientización cuidadoso y reflexivo.

Debido a las constantes amenazas en que se encuentran los sistemas, es esencial que los usuarios y las organizaciones, ya sean privadas o del Estado enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

Los ataques informáticos están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso las persona, por esto toda empresa se debe comprometer a capacitar a todo el personal que labora en una organización, para que se tenga pleno conocimiento de los riesgos que existen, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios y de las personas encargadas o administrador de la red.

El sistema hospitalario maneja muchísima información confidencial o sensible que debe ser protegida por la alta gerencia y por el personal encargado de la administración de la información, y a su vez por cada empleado.

Autor del RAE: Jadit Guerrero Molina

REFERENCIAS

ANANGUREN, amarilis_204A1. Clasificación de Redes según el tamaño. (Redes de Computadora). [online], 30 Junio 2017. Encontrado en: https://redcomputadora.wordpress.com/2016/06/30/tipos-de-redes-segun-el-tamano/

AVANCE, jurídico. Ley 1273 de 2009. (Casa Editorial Avance Jurídico Ltda). [online]. 5 Enero 2009. Encontrado en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CATOIRA, Fernando. DNS Spoofing, ¿en qué consiste? [online], 18 junio 2012. Encontrado en: https://www.welivesecurity.com/la-es/2012/06/18/dns-spoofing/

CRISTIA, Máximiliano. Seguridad Informática. [en línea]. [Rosario, Argentina] 2018, [citado 25 Agosto 2019], Disponible en Internet: https://www.fceia.unr.edu.ar/~mcristia/apunte-si.pdf

ESTRELLA, Jorge. Tipos de topología. [online]. Encontrado en: http://jorge-star.galeon.com/INDICE.html

GÓMEZ VEITIS, Alvaro. Tipo de ataques e intrusos en las redes informáticas. [en línea]. [Caixanova, Madrid]: s, f. Disponible en Internet: https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

HEINEHKEN, team. Introducción a la problemática de la seguridad informática. [en línea]. Seguridad y Protección de la Información [citado 25 Agosto 2019]. Disponible en Internet: http://www0.unsl.edu.ar/~tecno/redes%202008/seguridadinformatica.pdf

Hostalía. Ataques de inyección SQL: qué son y cómo protegerse. (2013). Blog [abierto en 01 de febrero de 2020]. Recuperado de: https://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql/

Internet Soluciones Ya. ¿Qué es un ataque de denegación de servicios DDoS? (2018). Blog [abierto en 01 de febrero de 2020]. Recuperado de: https://www.internetya.co/ataques-de-denegacion-de-servicio-ddos-un-riesgo-real/

ISOTools. Qué debe incluir la Política de Seguridad de la Información según ISO 27001. (Blog calidad y excelencia). [online], 9 Abril 2017. Encontrado en: https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/

JUNCO ROMERO, Gerardo y RABELO PAUDA, Sonia. Los Recursos de Red y su Monitoreo. [en línea]. Texinfo, 1 ed. [Cuba]. Revista Cubana de Informática Médica. 1 Octubre 2018 [citado 25 Agosto 2019]. Disponible en Internet en: https://www.javerianacali.edu.co/sites/ujc/files/normas_icontec.pdf

LAZARO, Diego. Ataques XSS: Cross-Site Scripting en PHP. [en línea]: 2018. Disponible en Internet: https://diego.com.es/ataques-xss-cross-site-scripting-en-php

MARQUETING. Las 10 mejores herramientas de Monitoreo de Redes del 2017. Apen 25 (Soluciones Globales en Informática y Tecnología) [online], 2017. Encontrado en: https://apen.es/2017/03/10/las-10-mejores-herramientas-de-monitoreo-de-redes-del-2017/

MARTIN, Sara. Monitorización de Sistemas Informáticos. Pandorafms (Monitoring Blog) [online], 21 Agosto 2017. Encontrado en: https://blog.pandorafms.org/es/monitorizacion-de-sistemas/

MEDINA, Joaquin. Introducción al Malware. [en línea]. [Madrid]: 2008. Disponible en Internet: http://www.joaquin.medina.name/web2008/documentos/informatica/documentacion/seguridad/virus/2007_09_05_IntroduccionAlMalware.html

NAGIOS. ¿Qué es Nagios? (2017). Blog [abierto en 01 de febrero de 2020]. Recuperado de: https://www.north-networks.com/fabricante/que-es-nagios/

Pandora FMS 5.0 Manual de Usuario. (2013). 1º Edición (España). Recuperado de: https://pandorafms.com/downloads/PDF/PandoraFMS_5.0_Manual_ES.pdf

Pandora. QuickGuides ES: Guia Rapida General. (s, f). Blog [abierto en 01 de febrero de 2020]. Recuperado de: https://pandorafms.com/docs/index.php?title=Pandora:QuickGuides_ES:Guia_Rapida_General

PAESSLER. Software de monitoreo de VoIP PRTG (2020). Blog [abierto en 01 de febrero de 2020]. Recuperado de: https://www.paessler.com/voip_monitoring_software?gclid=CjwKCAiA1rPyBRAREiwA1UIy8P47Z4at5QZkI2T-aMUkxdijgI3pb6yTfQc_DDlYPM57UI8OkzaMlxoC370QAvD_BwE&utm_adgroup=it-monitoring-tools&utm_adgroupid=64650660683&utm_adnum=324488756610&utm_campaign=ALL_EN_TEST_Search-NonBrand_broad_3&utm_campaignid=1674172061&utm_device=c&utm_keyword=it+monitoring+tools&utm_location=1029349&utm_medium=cpc&utm_source=google&utm_targetid=aud-320225222828%3Akwd-953701782

Sistemas de Autenticación. Disponible en Internet: http://seguridadensistemascomputacionales.zonalibre.org/Sistemas%20de%20Autenticaci%C3%B3n.pdf

“Spoofing” o “suplantación de identidad”. Que es el email Spoofing y cómo evitarlo con el registro SPF. [online], 13 de diciembre 2017. Encontrado en: https://www.acens.com/comunicacion/white-papers/email-spoofing-como-evitarlo-registro-spf/