SOLUCIONES DE MONITORIZACIÓN DE RED COMO ELEMENTOS CLAVE PARA LA DETECCIÓN DE AMENAZAS Y VULNERABILIDADES EN LAS INFRAESTRUCTURAS TI CON EL FIN DE REDUCIR Y GESTIONAR RIESGOS EN LAS ORGANIZACIONES.

FRANKIN STIVEN CARVAJAL PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

SOLUCIONES DE MONITORIZACIÓN DE RED COMO ELEMENTOS CLAVE PARA LA DETECCIÓN DE AMENAZAS Y VULNERABILIDADES EN LAS INFRAESTRUCTURAS TI CON EL FIN DE REDUCIR Y GESTIONAR RIESGOS EN LAS ORGANIZACIONES.

FRANKIN STIVEN CARVAJAL PÉREZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Daniel Felipe Palomo Luna
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 8 de Agosto de 2024

DEDICATORIA

Agradezco infinitamente a Dios por permitirme llegar a este camino gozando de una grandiosa salud, dándome una familia incondicional que me han apoyado a lo largo de mi carrera, dedico también a mi esposa, hija, padres y demás familiares que me han dado consejos importantes de vida para alcanzar mis metas e ideales.

AGRADECIMIENTOS

Agradezco principalmente a todos y cada uno de los docentes de la Universidad por transmitir sus conocimientos a lo largo de la carrera, exigiéndonos de acuerdo con sus metodologías dándonos un entendimiento acerca de los temas trabajados, Agradezco también al tutor Eduard Antonio Mantilla Torres por su paciencia, retroalimentaciones correspondientes, su acompañamiento constante y todo su conocimiento brindado para lograr este objetivo en mi carrera.

1 CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE ILUSTRACIONES

pág.

GLOSARIO

Amenaza: se puede considerar como un peligro que puede ser causado de forma natural o por personas para tal fin.

Arp poison routing: se utiliza para embestir una red de Ethernet, el cual pretende detectar *frameworks* de datos hacia una LAN por medio de un hacker, para que una vez obtenidos los datos sea modificado o se permita detener el tráfico por completo.

Ataques DoS (Denegación de servicio): consiste en que el usuario no pueda acceder a un equipo o red. Un avance de este tipo de ataque es la negación de servicio distribuido (DDoS) donde inducen enviar demasiados datos de información desde diversas partes con el fin que el usuario o la compañía no logren acceder a la red o al recurso necesario.

Firmware: consiste en el software o programa básico capaz de inspeccionar los circuitos electrónicos de un conector donde contiene un código que se encarga de intervenir o enviar acción para el hardware certificando el funcionamiento básico del dispositivo.

Modelo OSI: permite la comunicación entre diferentes sistemas empleando protocolos estándar, por lo cual los proveedores y/o fabricantes deben de tener en cuenta para lograr la comunicación entre estos.

Ransomware: se relaciona con un programa maligno que imposibilita el acceso ya sea a su sistema o archivos donde el hacker reclama el pago por medio de criptomonedas para devolver la información se logre acceder a los dispositivos.

Vulnerabilidad: se relaciona con el riesgo que puede llegar a tener un individuo o un sistema frente a peligros naturales, sociales, políticos, etc.

RESUMEN

En la actualidad las entidades empresariales están sujetas a una alta cantidad de ataques de seguridad que pueden llegar a ocasionar incidentes o perdidas de información que podrían afectar la continuidad del negocio, por ello se debe realizar un análisis de vulnerabilidades en los servidores tanto a nivel hardware como software (sistema operativo) así como equipos de comunicaciones, en la infraestructura TI de las compañías, con la finalidad de establecer el aseguramiento y la mitigación de dichas amenazas.

En este documento, se indican diferentes amenazas que en este momento se presentan en la infraestructura tecnológica de una compañía, dado el progreso de la tecnología y la penuria de brindar disponibilidad eficacia en los procesos de la organización.[1]

En relación, se plantea un protocolo de análisis de amenazas y vulnerabilidades que permitan a una empresa identificar, gestionar, y proteger datos y demás activos de información que puedan ser afectados por un ataque informático de cualquier tipo. Dicho análisis permite encontrar la amenaza y formular medidas eficientes de seguridad para proteger los datos de la organización y evitar que se materialice un riesgo.[2]

Palabras claves:

Amenaza, ARP *Poison Routing*, Ataques DoS, *Firmware*, Modelo OSI, *Ransomware*, Vulnerabilidad

---

1 BERMUDEZ Kelly, BAILON Edber. *Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/Iec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros.[En línea]. Bogotá:* Mayo de 2015. Disponible en https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

2 INFRAESTRUCTURA, R., & LANAMMEUCR . En 2016 Vol.1

ABSTRACT

At present, business entities are subject to a high number of security attacks that can cause incidents or loss of information that could affect business continuity, for this reason a vulnerability analysis must be carried out on servers both at the level hardware and software (operating system) as well as communications equipment, from layers 1 to 4 OSI model, in order to establish the assurance and mitigation of said threats.

This document indicates different threats that are currently present in the technological infrastructure of a company, given the progress of technology and the lack of availability in the organization's processes.

In relation, a threat and vulnerability analysis protocol is proposed that allows a company to identify, manage, and protect data and other information assets that may be affected by a computer attack of any kind. This analysis allows the threat to be found and efficient security measures to be formulated to protect the organization's data and prevent a risk from materializing.

Keywords:

ARP poison routing, Data hijacking, DoS attacks, Firmware, OSI model, Threat, Vulnerability

INTRODUCCIÓN

En la actualidad, las organizaciones enfrentan una variedad de ataques cibernéticos que pueden comprometer la continuidad del negocio al causar inconvenientes o pérdidas de información crítica. Esta situación subraya la importancia de realizar un análisis exhaustivo de vulnerabilidades en los servidores (hardware y sistema operativo) y en los equipos de comunicaciones que constituyen la infraestructura de TI. El objetivo es identificar, asegurar y mitigar posibles amenazas.

Este documento tiene como propósito definir y examinar las amenazas contemporáneas que afectan la infraestructura tecnológica de las organizaciones. El rápido avance tecnológico y la demanda de mayor disponibilidad y eficiencia en los procesos organizacionales han incrementado la exposición a riesgos de seguridad.[3]

Se propone un protocolo detallado para el estudio de amenazas y vulnerabilidades, diseñado para que las empresas puedan identificar, gestionar y proteger sus datos y otros activos de información frente a diversos tipos de ataques informáticos. Este análisis no solo permite determinar las amenazas existentes, sino también proponer medidas de seguridad eficaces para proteger la información de la organización y prevenir la materialización de los riesgos.[4]

[3] EDBER, B. M. K. G. B. Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/Iec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros. 2015

[4] INFRAESTRUCTURA, R., & LANAMMEUCR . En 2016 Vol.1

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La información de cualquier compañía, tanto comercial, como productiva, jurídica o financiera, es uno de los activos más significativos, por esta razón se hace necesario identificar la información determinante y plantear un protocolo o método para solventar cualquier amenaza que se presente a esta seguridad.

“El mayor error de muchas empresas es creer que nunca serán víctimas de un ataque cibernético, cuando en realidad ya pueden tener filtraciones de información que no serán evidentes sino después de mucho tiempo. Los *Ransomware*, por ejemplo, trabajan durante meses antes de secuestrar la información para pedir cuantiosas sumas de dinero en forma de criptomonedas con la promesa de devolverla”.[5]

En 2020, el ataque a la cadena de suministro de SolarWinds afectó a numerosas organizaciones gubernamentales y privadas. Los atacantes lograron insertar un malware en las actualizaciones de software, comprometiendo así miles de sistemas en todo el mundo[6]

En mayo de 2021, un ataque de *ransomware* afectó a Colonial Pipeline, una de las mayores redes de tuberías de combustible en Estados Unidos. Este ataque interrumpió el suministro de combustible y llevó al pago de un rescate de $4.4 millones para recuperar el control de los sistemas.[7]

El impacto de estos ciberataques no solo se limita a pérdidas financieras. Las organizaciones también enfrentan daños a su reputación, pérdida de confianza por parte de los clientes y sanciones regulatorias. La implementación de análisis de vulnerabilidades en la infraestructura de TI es esencial para mitigar estos riesgos y proteger los activos críticos de las organizaciones.

Con el fin de mitigar perdidas de información o caídas en los sistemas de información por atacantes se hace necesario analizar las causas de los riesgos y vulnerabilidades en las capas 1 al 4 del modelo OSI para observar posibles fallas o brechas de seguridad en los dispositivos.

---

[5] SGSI, ISO 27001: Los activos de información, [En Línea] 30 marzo 2015, Disponible en https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

[6] CISA, Análisis del Incidente SolarWinds, [En línea] 2021, Disponible en https://ciberseguridad.gob.cl/documents/216/10CND20-00045-01.pdf

[7] Kaspersky, Informe del Ataque de ransomware a Colonial Pipeline, [En línea] 2021, Disponible en https://www.kaspersky.es/blog/pipeline-ransomware-mitigation/25302/

De acuerdo con lo evidenciado, problemas como el aprovechamiento de vulnerabilidades existentes en la infraestructura tecnológica y los fallos relacionados a incidentes de seguridad, claramente son resultado de la utilización de sistemas operativos y aplicaciones completamente desactualizadas y a la imposibilidad de realizar detección de amenazas en tiempo real entre otros. Estos aspectos representan varios riesgos inherentes a la información vital de una compañía, para lo cual es necesario la implementación de los planes correspondientes para atacar estas amenazas y garantizar la continuidad de negocio.[8]

Se puede considerar de los activos más significativos e indispensables en toda compañía es la información la cual puede ser financiera, operacional, de uso interno, etc., por esto es indispensable identificar, priorizar, plantear un protocolo o plan de acción para prevenir cualquier inconveniente o amenaza que pueda tener.[9]

Un estudio de FireEye en 2023 reveló que el tiempo promedio para identificar y contener una brecha de seguridad es de 287 días. Este largo periodo de exposición aumenta significativamente el daño potencial causado por los atacantes.[10]

Muchas empresas llegan a pensar que no pueden ser víctimas de un ataque cibernético, sin embargo toda organización está expuesta a estas intrusiones, incluso muchas infiltraciones pueden llegar a ser evidentes luego de un tiempo e incluso cuando ya son atacados; como por ejemplo los Ransomware muchas veces están filtrados durante un largo tiempo analizando la información a secuestrar para así poder exigir cierta cantidad de dinero de tipo criptomoneda para no ser descubiertos y devolver la información, sin embargo esto no es ninguna garantía, de hecho en algunas ocasiones no devuelven la información o la entregan cifrada o de forma parcial.[11]

---

[8] LOZANO Michael, CORREA Miguel, ANÁLISIS DE LAS VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA MEDIANTE TESTING DE CAJA BLANCA, BAJO LA NORMA ISO 27005 EN LA COMPAÑÍA CARACOL RADIO, NODO PRINCIPAL BOGOTÁ. [En Línea] Bogotá, 2020 Disponible en https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

[9] LOPEZ, María Teresa, Universidad de Murcia, Departamento de Sociología, [En Línea] 2013, Disponible en https://www.tdx.cat/bitstream/handle/10803/117203/TESIS.pdf?sequence=

[10] FireEye, Informe de respuesta a incidentes 2023, [En línea] 2023, https://docs.trellix.com/es-ES/bundle/fireeye-documentation-landing/page/GUID-AA0E08E3-E71E-4197-98C4-0A0BCBE80A65.html

[11] AMBIT TEAM, ambit-bst Tipos de Vulnerabilidades y Amenazas informáticas [En Línea] 10 noviembre 2020, Disponible en https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

El estudio anual de IBM y el Instituto Ponemon estimó que el costo promedio de una violación de datos es de $4.24 millones. Este costo incluye la pérdida de ingresos, la reparación de los daños y las sanciones regulatorias.[12]

Como propuesta para mitigar ataques de pérdidas de información es indispensable analizar las posibles causas de riesgos y vulnerabilidades de dispositivos situados en las capas 1 a 4 del Modelo OSI correspondientes a la infraestructura de TI con el fin de visualizar las brechas de seguridad en dichos dispositivos. Muchas de las vulnerabilidades evidenciadas en los incidentes de seguridad se deben a aplicaciones o sistemas operativos desactualizados que en ocasiones no son capaces de detectar amenazas o ataques en tiempo real, por lo cual simboliza riesgos inherentes de información para la organización, es por ello por lo que se hace necesario la ejecución de planes para abarcar las amenazas detectadas y evitar posibles ataques cibernéticos garantizando la continuidad de negocio.

1.2 FORMULACIÓN DEL PROBLEMA

Tomando como punto de partida la pandemia vivida por el Covid-19 donde las organizaciones se vieron obligadas a cambiar sus modalidades de trabajo y donde los ciberdelincuentes del mundo aprovecharon la situación para exponer todas las vulnerabilidades posibles en las infraestructuras de las organizaciones, teniendo en cuenta esto la seguridad informática ha tomado mayor fuerza ya que las entidades malignas buscan atacar las compañías y sacar provecho de toda información confidencial que logren obtener, es por esto que también vemos como los ciberdelincuentes engañan a personas naturales por medio de correos electrónicos falsos, llamadas o mensajes de texto engañosos para obtener información confidencial como claves de cuentas bancarias o tarjetas de crédito , hurtando a las personas que en ocasiones no se dan cuenta de cómo los robaron. Teniendo en cuenta la problemática y resaltando que cuenta con crecimiento exponencial desde la pandemia, las organizaciones se vieron obligadas a tomar acciones de respuesta inmediatas contra los ataques de los ciberdelincuentes es por esto por lo que hoy en día se evidencian malas prácticas en la seguridad de la infraestructura de las compañías y es así como continúan presentando riesgos y vulnerabilidades en sus redes, por lo que se planeta la siguiente pregunta problema. ¿Cuáles serían las soluciones ideales de monitorización de red que permitan detectar amenazas y vulnerabilidades en las infraestructuras TI, con el fin de reducir y gestionar riesgos en las organizaciones?

[12] IBM y el Instituto Ponemon, Informe sobre el coste de una vulneración de datos en 2023 [En línea] 2023, https://www.ibm.com/es-es/reports/data-breach

2 JUSTIFICACIÓN

Teniendo en cuenta la contingencia mundial que se vivió a lo largo de los últimos años a causa de la pandemia, muchas de las compañías de Colombia y del mundo tuvieron que reformar la operación o forma de trabajo de sus empleados, con esto fue necesario generar o configurar VPN de tipo Client-to-site, Site to Site, SSL, etc. para que sus trabajadores pudieran trabajar desde el hogar para evitar contagios del COVID-19, para lo cual fue necesario generar apertura de puertos y otras configuraciones en los equipos de infraestructura sobre las capas 1 a 4 del modelo OSI; sin embargo se hace necesario que se delimiten y/o revisen las configuraciones generadas en el momento de la implementación para evitar posibles brechas de seguridad que se tienen en la compañía.

Por lo anterior, y dado que la información se considera como uno de los activos más trascendentales de las compañías y que más se encuentran expuestos en la red a nivel mundial, es necesario protegerla de posibles amenazas sin que esta sufra ningún tipo de modificaciones o alteraciones en los datos que contengan.
El dueño de las tecnologías que se manipulan dentro de una compañía debe de tener el conocimiento suficiente de las plataformas tecnológicas que se utilizan para generar controles de seguridad y seguimiento que permitan detectar y atacar amenazas y vulnerabilidad halladas evitando un riesgo que puede llegar a ser mayor en la compañía por la no detección de la amenaza.

Para aminorar posibles riesgos residuales, se manejarán los análisis de las amenazas de forma constante que favorezcan el amortiguamiento del riesgo encontrado, donde se aplican los controles de seguridad para solventar brechas de seguridad dado que muchas de las plataformas o sistemas operativos pueden tener vulnerabilidades poco conocidas que alguna persona pueda llegar a explotarla para obtener beneficio de estas.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Examinar las soluciones de monitorización de red disponibles como elementos clave para la detección de amenazas y vulnerabilidades en las infraestructuras TI con el fin de reducir y gestionar riesgos en las organizaciones a partir de la consulta documental.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar cuáles son los vectores de ataque más comunes con sus diferentes técnicas de intrusión utilizados para vulnerar sistemas de red de las organizaciones a partir del material bibliográfico, indicaciones de los fabricantes de seguridad perimetral y boletines de ciberseguridad con el fin de brindar sugerencias a nivel de seguridad en las organizaciones.
- Evaluar las diferentes soluciones más eficientes de hardware y software para la detección de amenazas y vulnerabilidades en las infraestructuras TI por medio de un análisis de los diferentes softwares existentes en el mercado.
- Proponer procedimientos que contribuyan a la detección de amenazas y vulnerabilidades en las infraestructuras TI a partir de las diferentes metodologías de intrusión y comparativa de los procesos para minimizar y gestionar riesgos en las organizaciones.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Hoy en día, muchas brechas de seguridad ocurren en la infraestructura de red, más que en los dispositivos conectados a ella. Estas brechas pueden evitarse mediante la implementación de equipos y configuraciones de última tecnología. Es indispensable incluir medidas de seguridad en todos los componentes de la red, como firewalls, switches y routers, para mantener los pilares de la seguridad: disponibilidad, integridad y confidencialidad. Esto requiere prácticas como el encriptado de información, la autenticación de doble factor, el uso de datos biométricos, y el mantenimiento preventivo y correctivo de hardware y software.[13].

La arquitectura OSI, basada en el RFC 2828, distingue entre amenazas y ataques. Las amenazas son eventos latentes que pueden violar la seguridad de los datos, mientras que los ataques son eventos que ya han ocurrido, como el ransomware, donde se accede a la información y se exige un rescate. Los atacantes suelen infiltrarse en los sistemas y esperar antes de lanzar su ataque para identificar la información más valiosa. Por ello, es crucial utilizar software de calidad y actualizado.[14]

Para este proyecto, se considerarán únicamente las capas 1 a 4 del modelo OSI: física, enlace de datos, red y transporte. Esto ayudará a evitar errores en la comunicación mediante un correcto direccionamiento lógico de los equipos terminales y los puertos de las aplicaciones de destino. Es esencial conocer y abarcar los protocolos utilizados en cada capa, como RJ45, 802.11, RS-232 y DSL para la capa 1; Ethernet, Token Ring y VLAN para la capa 2; IPv4, IPv6, ARP e ICMP para la capa 3; y TCP/UDP para la capa 4.[15]

El análisis de la red requiere el uso de herramientas como Nessus, Wireshark, Kali Linux y Wifi Analyzer, que permiten identificar vulnerabilidades. Estudios previos indican que los ataques a la capa de enlace utilizan técnicas como spoofing, DOS, hijacking, phishing y exploits, causando pérdida de información. Los ataques

[13] DOCUSIGN. [En línea] 24 de Agosto de 2021. Disponible en https://www.docusign.mx/blog/seguridad-de-la-informacion

14 KASPERSKY. Kaspersky. [En Línea] Disponible en https://latam.kaspersky.com/resource-center/threats/ransomware

[15] LOZANO, J. R. Itadmins [En Línea] 10 de Octubre de 2019. Disponible en https://itadmins.es/networking-i-el-modelo-osi/

informáticos suelen constar de cinco fases: reconocimiento, exploración, obtención de acceso, mantenimiento del acceso y borrado de huellas.[16]

En una red corporativa típica, se pueden implementar varias capas de seguridad para proteger la infraestructura. Por ejemplo, una empresa puede utilizar firewalls de última generación para controlar el tráfico de red y prevenir accesos no autorizados. Además, se pueden configurar redes privadas virtuales (VPN) para asegurar las conexiones remotas de los empleados. La autenticación de doble factor y el uso de certificados digitales pueden fortalecer aún más la seguridad de la red. Estas medidas han demostrado ser efectivas para reducir significativamente el riesgo de ataques cibernéticos.

En 2020, SolarWinds, una empresa de software de gestión de TI, sufrió un ataque a su cadena de suministro que comprometió a miles de sus clientes, incluidos organismos gubernamentales y grandes corporaciones. Los atacantes insertaron un malware en las actualizaciones de software de SolarWinds, lo que permitió el acceso no autorizado a los sistemas de los clientes una vez que instalaron las actualizaciones. Este ataque subrayó la importancia de la seguridad en la cadena de suministro y llevó a muchas organizaciones a revisar y fortalecer sus prácticas de seguridad.

En septiembre de 2020, el Hospital de la Universidad de Düsseldorf fue víctima de un ataque de ransomware que paralizó sus sistemas informáticos, lo que resultó en la cancelación de citas médicas y cirugías. Los atacantes exigieron un rescate para devolver el acceso a los sistemas. Este incidente destaca la vulnerabilidad de las infraestructuras críticas y la importancia de contar con planes de contingencia y copias de seguridad robustas

Los ataques pueden tener varios objetivos, como la extorsión, robo o fraude de información la cual puede ser confidencial, accesos a un sistema sin previa autorización, ataque DoS, entre otros; estos ataques provienen de fuentes como usuarios autenticados (ya sean colaboradores internos o que tengan algún lazo laboral con la compañía) y atacantes con personal externo que se encuentra fuera de las instalaciones de la compañía, donde logran accesos remotamente a los equipos), para lo cual es necesario contar con un estudio de vulnerabilidades y posibles amenazas que se logren identificar en la compañía.[17]

[16]ROJAS, C. E. UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA. [En Línea] 2015 Disponible en https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/7402/Carlos_Exam.Suf.Prof_titulo_2014.pdf?sequence=1&isAllowed=y

[17] LIBRARY. Vulnerabilidades del modelo OSI [En Línea] Disponible en https://1library.co/article/vulnerabilidades-modelo-osi-seguridad-modelo-osi.z1l2ee3q

Entender los conceptos sobre la ciberdelincuencia es fundamental para comprender este fenómeno en constante evolución. La ciberdelincuencia se refiere a la realización de actividades delictivas mediante el uso de las tecnologías de la información y la comunicación (TIC). Estas actividades pueden incluir la piratería informática, el robo de datos, el fraude en línea, el acoso cibernético, la distribución de malware y otros actos ilícitos que involucran sistemas informáticos y redes.[18]

Los ciberdelincuentes pueden estar motivados por una variedad de factores, incluido el beneficio económico, la búsqueda de fama, el activismo político, el espionaje, la venganza o el simple deseo de causar daño. Es importante entender que la motivación puede ser muy diferente.

La ciberdelincuencia se puede categorizar en varias formas, como:

- Ciberdelincuencia financiera: Incluye actividades como el phishing, el fraude con tarjetas de crédito y el robo de identidad con el objetivo de obtener beneficios financieros.
- Ciberdelincuencia de acceso no autorizado: Esto implica la intrusión en sistemas informáticos o redes sin permiso, a menudo con el propósito de robar información confidencial.
- Ciberacoso y ciberbullying: Comprende comportamientos en línea que causan daño emocional, amenazas o acoso a individuos.
- Ciber espionaje: Implica la recolección de información confidencial, a menudo por gobiernos u organizaciones para fines políticos o económicos.
- Distribución de malware: Incluye la creación y propagación de software malicioso, como virus, gusanos y troyanos.

Dentro de las compañías existen diferentes infraestructuras de TI, cualquier dispositivo de red o dispositivo tecnológico puede presentar una vulnerabilidad y cierto riesgo para la compañía, comprender los riesgos y vulnerabilidades en infraestructura de Tecnologías de la Información (TI) es esencial para la gestión de la ciberseguridad y la continuidad de las operaciones.

Comprender los riesgos y vulnerabilidades en infraestructura de TI es esencial para la gestión de la ciberseguridad y la continuidad de las operaciones. Los riesgos y vulnerabilidades en infraestructura de TI se refieren a peligros potenciales y debilidades en sistemas, redes, hardware, software y datos que pueden ser explotados por amenazas cibernéticas o desastres naturales, llevando a la interrupción de operaciones y pérdida de datos.[19]

[18] BENITO Maria, Ciberdelincuencia: ¿Qué es y cómo combatirla?, 2023 [En línea] Disponible en https://blogs.uoc.edu/edcp/ciberdelincuencia-que-es-y-como-combatirla/

[19] ACRONIS, ¿Qué es la gestión de riesgo de TI?, 2021 [En línea] Disponible en https://www.acronis.com/es-mx/blog/posts/it-risk-management/

- Riesgo: Es la probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto negativo en la infraestructura TI. Los riesgos se expresan en términos de probabilidad e impacto.

- Vulnerabilidad: Es una debilidad o fallo en un sistema o proceso que podría ser explotado por una amenaza. Las vulnerabilidades pueden ser de naturaleza técnica (por ejemplo, una debilidad de seguridad en una aplicación) o no técnica (por ejemplo, la falta de políticas de seguridad).

La identificación y evaluación de riesgos y vulnerabilidades implican:

- Análisis de activos: Identificar y clasificar los activos críticos de TI, como servidores, bases de datos, aplicaciones y datos.
- Identificación de amenazas: Enumerar las amenazas potenciales que podrían afectar a los activos de TI.
- Evaluación de vulnerabilidades: Determinar las debilidades en la infraestructura que podrían ser explotadas por las amenazas.
- Análisis de riesgos: Calcular la probabilidad y el impacto de que una amenaza explote una vulnerabilidad en un activo de TI.

Gestión de Riesgos: La gestión de riesgos incluye medidas para reducir, transferir, evitar o aceptar riesgos. Esto puede incluir la implementación de controles de seguridad, la compra de seguros y la planificación de la continuidad del negocio. La gestión de riesgos es un proceso continuo que sigue un ciclo de vida que incluye identificar, evaluar, mitigar, monitorear y revisar continuamente los riesgos y vulnerabilidades.

Es importante conocer las herramientas de escaneo de vulnerabilidades, estas se centran en las aplicaciones, tecnologías y enfoques utilizados para identificar y evaluar las debilidades en sistemas, redes y aplicaciones de software.

El escaneo de vulnerabilidades es el proceso de identificar, evaluar y categorizar debilidades de seguridad en sistemas informáticos, redes o aplicaciones. Estas debilidades pueden ser puertas de entrada para ciberataques y explotaciones maliciosas.[20]

Las vulnerabilidades pueden ser de diferentes tipos, como:

- Vulnerabilidades de software: Errores en el código de aplicaciones, sistemas operativos u otros programas que pueden ser explotados por ciberdelincuentes.

[20] FORTRA, Qué es el escaneo de vulnerabilidades y cómo funciona, 2022 [En línea] Disponible en https://www.fortra.com/es/blog/escaneo-vulnerabilidades

- Vulnerabilidades de configuración: Malas configuraciones de sistemas o redes que pueden permitir el acceso no autorizado o la fuga de datos.

- Vulnerabilidades de hardware: Debilidades físicas en dispositivos, como *routers* o servidores, que pueden ser explotadas.

El escaneo de vulnerabilidades es fundamental para mantener la seguridad de los sistemas y protegerlos contra posibles amenazas cibernéticas. Ayuda a las organizaciones a identificar y abordar las debilidades antes de que sean explotadas por ciberdelincuentes.

En muchas industrias, existen normativas y estándares de seguridad que requieren la realización regular de escaneos de vulnerabilidades, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) en el caso de las transacciones con tarjetas de crédito.

4.2 MARCO CONCEPTUAL

Actualmente existen diferentes métodos de análisis de riesgos como lo es el Octave, Magerit, Mehari, Cramm, Coras, Ebios, NIST SP 800:30. A continuación, una breve explicación de cada una de las metodologías.

Octave (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) valora los peligros de seguridad de la información donde se expone un procedimiento de mitigación para una compañía. Según HOLGUIN su principal objetivo es concientizar a la compañía que la seguridad no es un proceso que es solo competente de un grupo de personas, sino que abarca todas las áreas y se puede estar expuesto a esta.[21]

Para la metodología de Magerit consiste en identificar los riesgos que puede tener un sistema de información recomendando medidas de protección las cuales pueden prevenir y reducir los riesgos de acuerdo a la norma ISO 31000 sección 4.4 por medio de instrumentales y manuales ineludibles para su implementación.[22] Esta metodología ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos

---

21 HOLGUIN Fresia, L. L. Model for measuring the maturity of the risk analysis of information assets in the context of shipping companies. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacion, [En línea] 2019 1-17pag. Disponible en https://doi.org/10.17013/risti.31.1-17

22 NOVOA, A. Vista de Metodologías para el análisis de riesgos en los sgsi Publicaciones e Investigación. Bogotá. 2010 [En línea] Disponible en https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

de evaluación, auditoría, certificación o acreditación; así mismo, una de sus mayores ventajas es que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles. Otro de sus aspectos positivos radica en que sus resultados se expresan en valores económicos lo que, a su vez, también es una desventaja por cuanto el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos, hace que la aplicación de esta metodología sea muy costosa. Mientras que la metodología de Mehari muestra una técnica armonizada de estudios de riesgos el cual suministra un plan de apreciación y responsabilidad de riesgos de seguridad de la información, manejando las exigencias ISO/IEC 27005:2008. Los aspectos esenciales de este método es el diseño de una guía de riesgo, valoración de la eficacia de las políticas de seguridad y capacidad para evaluar y representar los niveles de riesgo, con esta metodología se identifican las vulnerabilidades por medio de auditorías y valoraciones de riesgo.

Ebios (Expresión de las necesidades e identificación de los objetivos de seguridad), Es una metodología de análisis y gestión de riesgos que percibe varias guías y utillajes de código libre, encaminada a administradores del riesgo de Tecnologías de Información.[23] En el sector salud es muy indispensable mantener la confidencialidad de la información para pacientes, de acuerdo con el juramento Hipocrático realizado por los médicos, esta información es importante y exclusiva entre médico – paciente. En el mundo actual donde la información fluye de manera rápida por medios electrónicos, es muy importante mantener unas costumbres para el manejo y seguridad en los datos. Por tal razón es obligatorio conocer el tipo de amenazas que se puedan presentar para así saber cómo se pueden controlar o mitigar[24]

Coras (*Consultative Objetive Risk Analysis System*), Es una habilidad muy ventajosa para dispositivos híbridos que pretendan hallar vulnerabilidades y amenazas. Esta técnica provee una serie de modelos, que se muestran a continuación.

- Una metodología de análisis de riesgos basado en la elaboración de modelos.
- Un lenguaje gráfico basado en UML (*Unified Modelling Language*).
- Un editor gráfico para soportar la elaboración de modelos (Microsoft Visio).
- Una biblioteca de casos reutilizables.

---

[23] MONSALVE, J. . CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). [En Línea] Bogotá. *2020*. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

[24] SÁNCHEZ-Henarejos, et al. Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atencion Primaria*, [En Línea] Bogotá, 2014. p. 214–222 Disponible en https://doi.org/10.1016/j.aprim.2013.10.008

- Una herramienta de gestión de casos (gestión y reutilización de casos).
- Representación textual basada en XML (*eXtensible Mark-up Language*).
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.[25]

Otro sector económico para el que es sustancial poseer un régimen de gestión de seguridad de la información (SGSI) son las MPYMES, para las cuales muchas no se tiene un SGSI que se ajuste a sus costos, por tal razón es importante que se tenga métodos en ciberseguridad que pueda ser aplicada por esta empresas sin generar costos altos y sin necesidad de tener una certificación internacional, así podrán dar manejo seguro a su información con vistas en llegar a poder adquirir una certificación en un futuro de crecimiento[26]

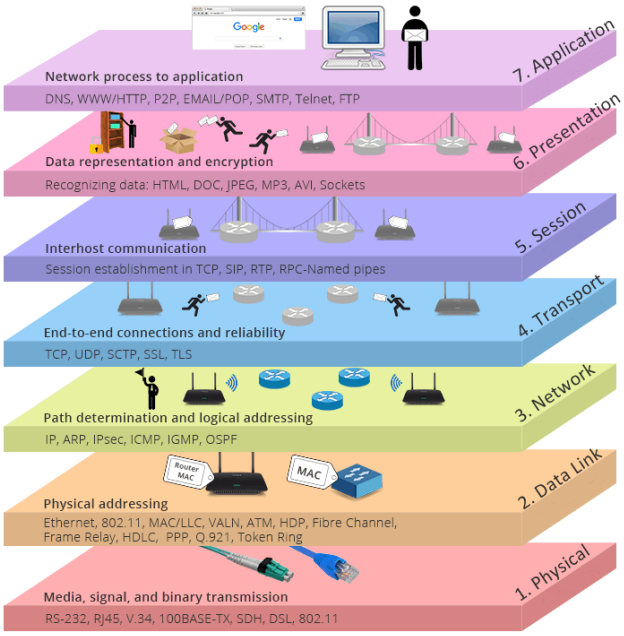
Modelo OSI: "El modelo de referencia OSI proporciona una amplia lista de funciones y servicios que pueden presentar en cada capa. Este tipo de modelo es coherente con todos los tipos de servicios y protocolos de rojo al describir qué es lo que se debe hacer en una capa determinada, pero sin regir la forma en que se debe lograr" [27]. Se representa mediante 7 capas las cuales permiten una comunicación entre sí, que corresponden a operaciones, equipos y protocolos estrictamente descritos.

Ilustración 1 - Modelo OSI

[25] ALEMÁN NOVOA, R. B. C. *Vista de Metodologías para el análisis de riesgos en los sgsi Publicaciones e Investigación*. [En Línea] Bogota. 2010. Disponible en https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

[26] CRESPO MARTÍNEZ, E. Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Ecu@Risk In *Enfoque UTE* [En Línea] 2017 Vol. 8, Issue 1. Disponible en https://doi.org/10.29019/enfoqueute.v8n1.140

[27] CLOUDFLARE. Modelo OSI *cloudflare*. Disponible en https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/



Tomado de platzi.com

Pishing: Consiste en el robo de información donde el ciberdelincuente logra obtener información personal, para lo cual usan correos electrónicos, mensajes de texto, llamadas y demás para captar la información usando la ingeniería social. [28] para lo cual es necesario revisar al detalle la información contenida en los correos electrónicos como lo es los datos del remitente, posibles archivos adjuntos o imágenes a descargar, errores ortográficos, redacción, etc.

Teniendo en cuenta el modelo OSI, es importante conocer cuáles son las herramientas de escaneo de vulnerabilidades, estas herramientas son software diseñado para identificar y evaluar debilidades. Algunas de las herramientas más comunes incluyen:

- Nmap: Una herramienta de código abierto que realiza escaneos de redes para identificar dispositivos y puertos abiertos.
- OpenVAS: Un escáner de vulnerabilidades de código abierto que realiza auditorías de seguridad y escaneos en busca de debilidades.
- Nessus: Una herramienta comercial ampliamente utilizada para escanear y evaluar vulnerabilidades en sistemas y redes.

28 MICROSOFT. [En Línea] Disponible en https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=El%20phishing%20es%20un%20ataque,que%20fingen%20ser%20sitios%20leg%C3%ADtimos.

- Qualys: Otra solución comercial que ofrece escaneos de vulnerabilidades en aplicaciones, sistemas y redes.

Conociendo las herramientas se hace fundamental conocer el proceso de escaneo de vulnerabilidades, este proceso por lo general involucra los siguientes conceptos básicos:

- Vulnerabilidad: Una vulnerabilidad es una debilidad o fallo en un sistema, red o aplicación que podría ser explotado por una amenaza para comprometer la seguridad de un sistema. Puede ser de naturaleza técnica (por ejemplo, un error de software) o no técnica (por ejemplo, una política de seguridad inadecuada).

- Amenaza: Una amenaza es cualquier evento o entidad que tiene el potencial de explotar una vulnerabilidad y causar daño a un sistema. Esto podría incluir hackers, malware, desastres naturales o incluso errores humanos.

- Escaneo de Vulnerabilidades: Es el proceso de utilizar herramientas de software para identificar y evaluar las vulnerabilidades en un sistema, red o aplicación. El escaneo de vulnerabilidades busca debilidades conocidas que podrían ser explotadas.

- Activos de TI: Los activos de Tecnologías de la Información (TI) son todos los elementos de hardware, software y datos que una organización utiliza en sus operaciones. Estos activos incluyen servidores, aplicaciones, bases de datos y más.

- Base de Datos de Vulnerabilidades: Una base de datos de vulnerabilidades es un repositorio que contiene información sobre las vulnerabilidades conocidas. Las herramientas de escaneo de vulnerabilidades utilizan esta base de datos para comparar las características de un sistema con las debilidades conocidas.

- Falso Positivo: Un falso positivo es un resultado de escaneo que indica incorrectamente la existencia de una vulnerabilidad cuando en realidad no existe. La reducción de los falsos positivos es importante para evitar la pérdida de tiempo y recursos en correcciones innecesarias.

- Riesgo: El riesgo se refiere a la probabilidad de que una amenaza explote una vulnerabilidad y cause un daño real. Los riesgos se evalúan en términos de probabilidad e impacto.

- Parche: Un parche es una actualización de software que se utiliza para corregir una vulnerabilidad conocida. La aplicación o instalación de parches es una medida fundamental para mitigar vulnerabilidades.

- Categorización de Vulnerabilidades: Las vulnerabilidades suelen clasificarse en función de su gravedad. Se utilizan categorías como "críticas," "importantes" o "menos importantes" para priorizar las correcciones.

- Informe de Vulnerabilidades: Después del escaneo, se genera un informe que enumera las vulnerabilidades encontradas, su gravedad, las recomendaciones de corrección y otros detalles importantes. Este informe guía la acción posterior.

- Gestión de Riesgos: La gestión de riesgos implica tomar decisiones informadas sobre cómo abordar las vulnerabilidades identificadas. Esto puede incluir la implementación de controles de seguridad, la asignación de recursos para correcciones y la planificación de la continuidad del negocio.

A continuación, se presentan algunas de las metodologías de intrusión y *testing* más comunes utilizadas para el hallazgo de riesgos y vulnerabilidades.

OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad**)** Esta metodología creada por ISECOM, Instituto de Seguridad y Metodologías Abiertas, tiene como fin el análisis de riesgos, para cumplir este objetivo fundamental, evalúa diferentes aspectos de los sistemas de información haciendo es posible indicar qué hacer, cómo hacerlo y cuando, ofreciendo un análisis ordenado y eficiente.

Como una metodología, está diseñada para ser consistentes y repetible. Como un proyecto de fuente abierta, permite a cualquier profesional en pruebas de seguridad contribuir con ideas para realizar pruebas de seguridad más precisas, concretas y eficientes. Además, esto permite la libre difusión de información y propiedad intelectual.[29]

Metodologías de intrusión e ingeniería social:
Esta metodología se subdivide en los aspectos más importantes de los sistemas de información: Seguridad de la información, Seguridad de los procesos, Seguridad en las Tecnologías de Internet, Seguridad en las comunicaciones, Seguridad Inalámbrica y seguridad física.

De manera sencilla se identifican una serie de actividades de testeo específicas por área, sobre las que se comprueban las especificaciones de seguridad, integradas con las verificaciones realizadas en las revisiones rutinarias. Con esta metodología, se realiza un esfuerzo para convertir en predecible QUE se debe de probar, COMO se puede hacer y CUANDO es necesario ejecutarlo. De esta manera

[29] Ciberseguridad, ¿qué es osstmm? definición, historia y características, [En línea] Disponible en https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/#Caracteristicas_de_OSSTMM

se aumenta la calidad del desarrollo, ya que la seguir esta metodología, se tiene la certeza de que se cumplen unos objetivos prefijados.[30]

OSSTMM utiliza categorizaciones estándar, las cuales permiten identificar claramente el alcance de cada una de las actividades:

Búsqueda de Vulnerabilidades: Orientado principalmente a realizar comprobaciones automáticas de un sistema o sistemas dentro de una red.

- Escaneo de la Seguridad: Orientado a las búsquedas principales de vulnerabilidades en el sistema que incluyen verificaciones manuales de falsos positivos, identificación de los puntos débiles en el sistemas y análisis individualizado.
- Test de Intrusión: Se plantean test de pruebas que se centran en romper la seguridad de un sistema determinado.
- Evaluación de Riesgo: se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.
- Auditoria de Seguridad: Se refiere a la continua inspección que sufre el sistema por parte de los administradores que controlan que se cumplan las políticas de seguridad definidas.
- Hacking Ético: Orientado a tratar de obtener, a partir de los test de intrusión, objetivos complejos dentro de la red de sistemas.[31]

NIST SP 800-115: Es una guía de evaluaciones y pruebas de Seguridad la cual fue publicada por el Instituto Nacional de Estándares y Tecnología (NIST) del gobierno de los Estados Unidos bajo la denominación SP 800-115

Esta metodología esta basada en 4 fases fundamentales:

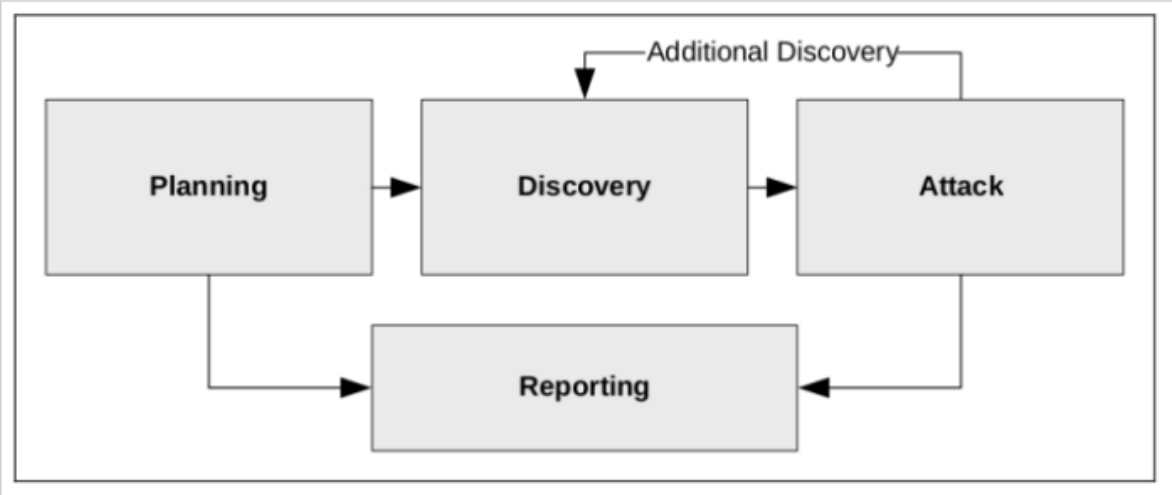
- Planeación: Allí es donde se gestionan permisos y se prepara todo lo que se requiere para llevar a cabo el análisis de seguridad.
- Descubrimiento: En esta fase se hace el reconocimiento de la infraestructura y se detectan las posibles vulnerabilidades para su posterior ataque.
- Ejecución: En esta fase se realizan las tareas de ataque para identificar si las vulnerabilidades identificadas con antelación pueden ser objeto de explotación y por ende verse afectada la organización.
- Documentación y reporte: Es la fase mas importante ante una organización ya que presenta las medidas necesarias para describir y mitigar las acciones realizadas anteriormente.[32]

[30] OSSTMM, Marco de desarrollo de la junta de Andalucía [En línea] Disponible en https://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

[31] OSSTMM, Marco de desarrollo de la junta de Andalucía [En línea] Disponible en https://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/551

[32] OVA, Metodologías de intrusión y Testing e Ingeniería social, UNAD [En línea] Disponible en https://repository.unad.edu.co/reproductor-

Ilustración 2 - Fases de una prueba de intrusión.



Tomado de NIST SP 800-115

Las pruebas de intrusión son formalizadas como las pruebas de seguridad en la cual, los evaluadores simulan ataques del mundo real en un intento de identificar modos de evadir las características de seguridad de una aplicación, sistema o red de datos.

Se menciona, además, que la mayoría de las pruebas de intrusión involucran la búsqueda de explotación combinada de vulnerabilidades en uno o más sistemas, de manera que puedan ser aprovechadas para ganar mayores privilegios de acceso que lo que pudiera haberse alcanzado a través de la explotación de una sola vulnerabilidad.[33]

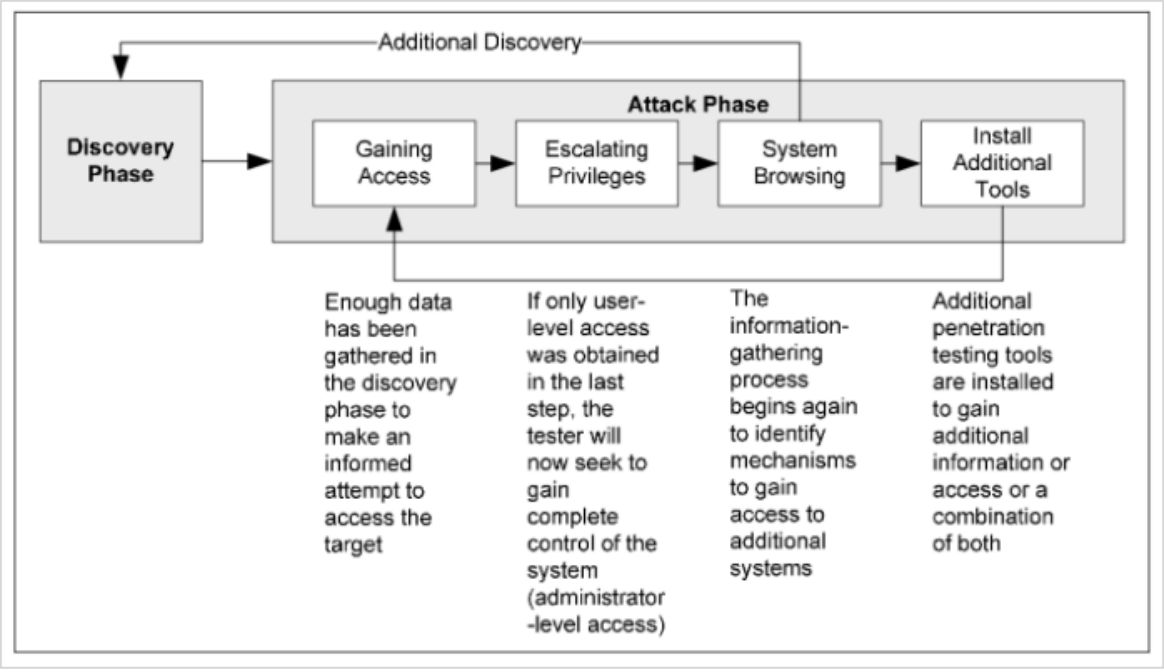
Con el fin de analizar a detalle esta metodología se especifica la fase 3 de Ejecución donde se busca explotar las vulnerabilidades y riesgos identificadas previamente, durante esta fase si algún ataque resulta ser exitoso, debe aislarse y documentarse de manera explícita además de proponer y recomendar medidas de seguridad que puedan mitigar este riesgo o vulnerabilidad, las actividades que se llevan a cabo para completar esta fase son:

ova/10596_51421/index.html#h5pbookid=322134878&section=top&chapter=h5p-interactive-book-chapter-5afd5494-9210-482a-8bd0-124f64065ad5

[33] RAUL, Henry, Mayo 2017, Metodología de Pruebas de Intrusión en la NIST SP 800-115, [En línea] Disponible en https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/

- Ganar privilegios de accesos: Si la información recopilada en la fase anterior es suficiente, durante esta actividad es posible ganar privilegios de acceso al sistema.
- Escalada de privilegios: Si en la actividad anterior solo se pudo ganar privilegios de acceso de bajo nivel (Ej. usuario básico), durante esta actividad, los evaluadores deben tratar de alcanzar el control total de sistema, semejante al que tendrían los administradores de este.
- Navegación dentro del sistema: Con el control del sistema alcanzado en la actividad anterior, los evaluadores deben buscar información adicional que les permita comprender mejor la existencia y métodos para ganar privilegios de acceso en sistemas secundarios. Si se descubren nuevos datos e informaciones, se sumarían estos a los resultados de la fase de Descubrimiento y se planificaría la explotación de las nuevas vulnerabilidades descubiertas.
- Instalación de herramientas adicionales: Durante el proceso de explotación de vulnerabilidades, puede requerirse la instalación de herramientas que permitan recopilar información adicional, ganar otros privilegios de accesos o ambas cosas a la vez.

Ilustración 3 - Actividades específicas de la Fase de Ejecución.



Tomado de NIST SP 800-115

PTES – Penetration testing Execution Estándar

Es una metodología estándar diseñada para que cualquier tipo de organización, sea grande, pequeña o mediana, pueda realizar pruebas de penetración o *pentesting*, es decir, pueden realizar auditorías técnicas de seguridad. Estas auditorias son realizadas tanto a las compañías, como a las empresas que son proveedores de servicios de seguridad debido a que utiliza un lenguaje y un ámbito de aplicaciones comunes.

Esta metodología desarrolla el proceso de un *pentesting* en 7 fases:

- Interacción previa: Consiste en especificar el alcance de la auditoria, las acciones y actividades que se van a desarrollar y otras medidas iniciales a tener en cuenta con el fin de llevar a cabo con éxito la prueba de penetración.
- Recopilación de información: Se realiza el análisis del objetivo, esto se hace consultando fuentes OSINT para recopilar información sobre los objetivos antes mencionados, realizando un examen y caracterización de los objetivos en base a toda la información recopilada, teniendo claramente en cuenta que se deben tomar las medidas defensivas necesarias para evitarlos.
- Modelado de amenazas: Analizar el entorno interno y externo para encontrar elementos que puedan ser utilizados para atacar a la organización. Esta fase caracteriza los activos a probar según su valor para la empresa y participación en los procesos organizacionales, por un lado, y la propia amenaza, por otro lado, identifica los sujetos de la amenaza que pueden intervenir y la capacidad de cada uno de ellos. De esta manera, puede delinear los tipos de ataques más probables que se utilizarán principalmente en las etapas posteriores.
- Análisis de vulnerabilidades: Proceso de descubrimiento de fallos en los sistemas de información que puedan ser aprovechados por un atacante. Pueden ir desde una mala configuración hasta un diseño inseguro, y por tanto deberán ser identificados mediante diferentes técnicas. Estas vulnerabilidades deberán ser verificadas para determinar todos aquellas que puedan ser utilizadas en la siguiente fase.
- Explotación: Considera implementar mecanismos para eludir las restricciones de seguridad en el acceso a los sistemas o recursos. En esta fase, se intenta explotar las vulnerabilidades identificadas para obtener acceso a los activos auditados, utilizando varios tipos de fuerza bruta y ataques dirigidos para explotar dichas vulnerabilidades y obtener el control del sistema.
- Post-Explotación: En esta fase, debe preparar mecanismos diseñados para garantizar los derechos de acceso continuos y realizar movimientos laterales para obtener el control de otros activos, mientras intenta obtener el máximo valor posible de los derechos de acceso que obtiene al analizar y recopilar la información más valiosa posible.

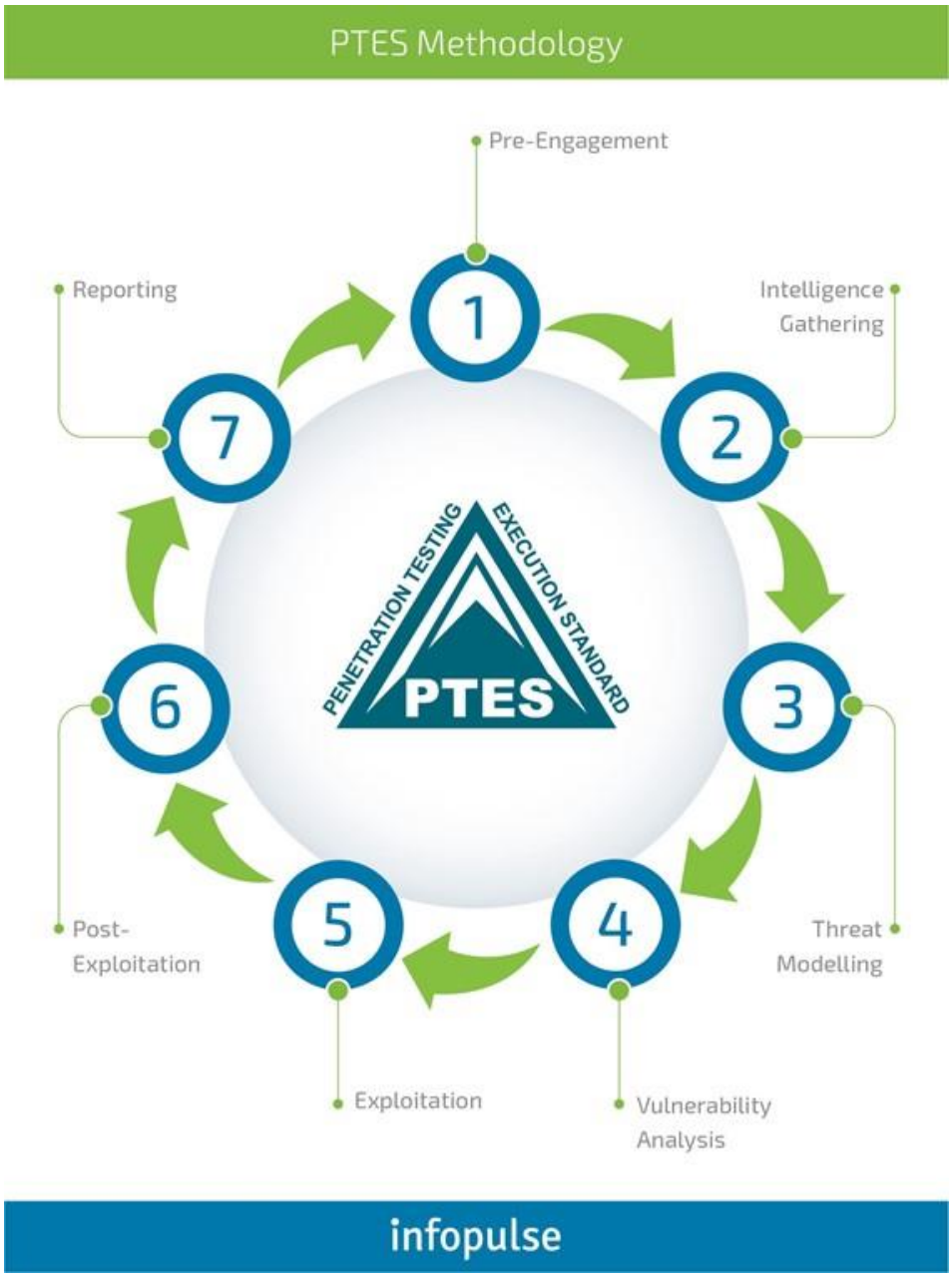
- Reporting: La última etapa consiste en la elaboración de un informe con las conclusiones del test de penetración. En esta etapa se elabora un informe de auditoría detallado, que refleja los resultados técnicos y metodológicos alcanzados, y un informe de gestión que resume los resultados alcanzados, los riesgos asociados y el plan de reducción de riesgos propuesto.[34]

Ilustración 4 - Fases de la metodología PTES

Tomado de The PTES Team Revision

[34] Basque CyberSecurity Centre, Penetration Testing Execution Standard (PTES), [En línea] Disponible en https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/penetration-testing-execution-standard-ptes

Ilustración 5 - Fases de la metodología PTES



Tomado de The PTES Team Revision

Para llevar a cabo cada una de las fases de manera satisfactoria esta metodología utiliza una guía técnica que proporciona información adicional para cada una de las etapas.

Existen diferentes tipos de metodologías para el análisis de riesgos y vulnerabilidades dentro de las compañías, donde por medio de diferentes procesos, etapas y actividades, siempre el objetivo principal es lograr identificar que vulnerabilidades o riesgos se encuentran en la infraestructura tecnológica de las

compañías, esto con el fin de que puedan ser remediadas a tiempo y así poder evitar ataques cibernéticos o ser víctimas de robo de información, también es necesario comprender la importancia del factor humano dentro de la seguridad de la información y ciberseguridad, ya que estas metodologías de *pentesting*, e intrusión son dirigidas en su mayoría a los dispositivos tecnológicos que componen la infraestructura de las compañías, las vulnerabilidades y riesgos allí encontrados es posible remediarlas para evitar futuros ataques, mientras que el factor humano es un riesgo constante para las organizaciones, ya que un descuido puede generar un ataque de grandes magnitudes para la compañía, es por esto que se considera que el factor humano se debe trabajar constantemente para fortalecer los conocimientos en seguridad informática y de esta manera proteger la organización.

4.3 MARCO HISTÓRICO

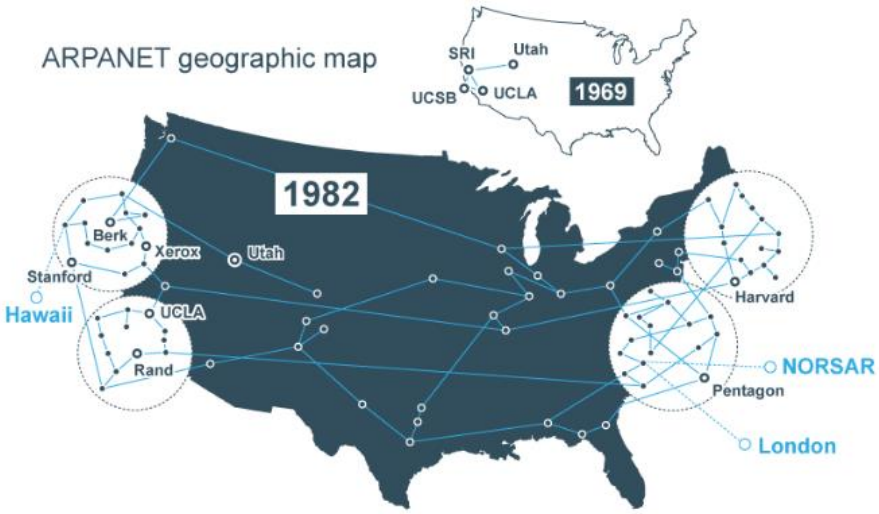
A lo largo de la vida se ha hablado de hacker, cracker y ciberdelincuente, donde se suele pensar que todos estos cumplen la misma función, pero no es así, un hacker indaga todos los fallos correspondientes a un sistema y se encarga de mejorarlo, mientras que quien los explota por un beneficio se considera ciberdelincuente, en 1903 se intercepto el telégrafo inalámbrico por el hacker Nevil Maskelyne, mientras que el primer ciberdelincuente fue John Draper quien descubrió que generando el sonido con un silbato se podían generar llamadas gratuitas.

Sobre los años 70 apareció el primer Malware con nombre Creeper creado por BBN Technologies, Bob Thomas crea un código para los sistemas conectados por ARPANET (versión básica de internet) el cual se ejecutaba solo y mostraba un mensaje de alerta,[35] a su vez, se crea el antivirus Reaper donde buscaba los equipos infectados con este virus y los eliminaba. En los años 80 se empieza a utilizar la ingeniería social para la captura de datos personales por Kevin Mitnick donde logro ganarse la confianza de personas para obtener la información necesaria para su beneficio, por lo cual es muy importante que hoy en día se generen auditorias y programas de concientización para visualizar que tan vulnerables pueden llegar a ser. [36]

Ilustración 6 - Red de Arpanet año 1969 a 1982

[35] NIVEL4 SEGURIDAD [En Línea] (14, diciembre,2020) Disponible en https://blog.nivel4.com/noticias/la-ciberseguridad-su-origen-y-la-trayectoria-que-ha-tenido-hasta-nuestros-dias/

[36] SOFISTIC CYBERSECURITY [En Línea] 30 Nov 2019 Disponible en https://www. .com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/



Tomado de sysnettechsolutions.com

OSI fue implementado en 1983 donde más que un modelo es un conjunto de protocolos que se utilizan simultáneamente donde se pueden aplicar estrategias de seguridad en todos los equipos. El modelo dispone de 7 capas, de aplicación, presentación, sesión, transporte, red, enlace y capa física; dado a su exactitud, este modelo cedió su estructura al estándar TCP/IP donde en este se utilizan únicamente 4 capas donde se incorpora la capa de aplicación, presentación y sesión en una sola llamada Aplicación, las otras 3 capas son transporte, red y Host a red (compuesto por capa Enlace y Física)[37]

4.4 ANTECEDENTES O ESTADO ACTUAL

Según el informe de la Interpol del 4 de agosto de 2020[38] "la ciberdelincuencia ha puesto de manifiesto un cambio sustancial en los objetivos de los ataques, que antes eran particulares y pequeñas empresas y ahora tienden a ser grandes multinacionales, administraciones estatales e infraestructuras esenciales" Dentro del informe de la Interpol se presentan como principales vectores de ataque el phishing, malware o ransomware, dominios y noticias falsos.

Actualmente la técnica más usada para el estudio de amenazas de riesgo es el método octave que consiste en un conjunto de criterios para establecer una evaluación de riesgos observando así los resultados obtenidos y así prevenir amenazas provenientes del exterior que se puedan materializar en un riesgo.

---

[37] GIUSTO BILIĆ, Denise, We Live Security, Seguridad de la Información Universidad Veracruzana. 02 junio 2015 [En Línea] Disponible en https://www.uv.mx/infosegura/general/noti_red-4/

[38] INTERPOL. Aumento alarmante de los ciberataques durante la epidemia de COVID-19. Agosto. 2020. [Consultado el 17 de julio de 2021]. Disponible en Internet: https://www.interpol.int/es/Noticias-y- acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los- ciberataques-durante-la-epidemia-de-COVID-19

Durante años, se ha abordado manipular diversas ideas y procesos aprovechados en la gestión de riesgos, cualesquiera circulando sobre una apariencia habitual de informar y otros en la indagación de planteamientos transformadores de tácticas para la contracción de vulnerabilidades, el amortiguamiento de pérdidas y utilizar las oportunidades que puedan llegar a acarrean los riesgos.

Así mismo, sucesos, reglas y resoluciones entablan a efectuar en las compañías previniendo que un acontecimiento peligro pueda originar quebrantos en sus intereses proyectados. Hoy en día, se conocen nuevas medidas que orientan y afrontar a los riesgos desde una perspectiva de gestión que favorece para poner en práctica en las entidades.

Indubitablemente los riesgos siempre han estado a lo largo del tiempo y han sido parte de las personas, si bien los riesgos se han ido cambiando con el progreso de las ciencias y las tecnologías. Sin embargo, la gestión de riesgos tiene demasiados inexpertos que llevan a mezclar riesgos con responsabilidad. El riesgo se considera un suceso inherente, por lo que es preciso que los expertos conozcan como identificarlo, valorarlo, y a resguardarse de estos sucesos.

En algunos momentos el riesgo está atado a la incertidumbre sobre acontecimientos futuros, y resulta improbable excluirlo. Por tanto, se debe de afrontar y administrar, diferenciando las fuentes de donde procede, calculando el valor de ostentación que ocupa y optando tácticas aprovechables para fiscalizar y estar al tanto de los valores de vulnerabilidad que se tiene.

Para conocer los riesgos y vulnerabilidades a los que se enfrentan diariamente las diferentes organizaciones se hace necesario identificar cuáles son las diferentes técnicas de ciberataques, de acuerdo con las denuncias analizadas realizadas por los colombianos, se confirma que los ciberataques más utilizados por los ciberdelincuentes son, método Phishing con un 42%, Suplantación de Identidad 28%, virus malicioso 14% y robo por medio de pago en línea con 16%.[39]

El factor más utilizado para propagar un virus como el *ransomware* es el envío de correos electrónicos masivos, estos correos suelen contener archivos adjuntos que ocultan el programa infectado del atacante, se requiere de un instalador o por lo general es un archivo tipo .exe que se ejecuta al dar doble clic para cumplir con su fraude. Para lograr obtener víctimas, el asunto del mail debe ser llamativo, con el fin de capturar la atención de los usuarios, las estrategias más comunes son las alertas,

[39] FIGUEROA CUBILLOS, Tatiana Esperanza, ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020 , UNAD, Disponible en repositorio de la Universidad.

notificaciones y citaciones judiciales además de suplantación de identidades gubernamentales.[40]

Los ataques por *ransomware* han detenido cadenas de suministros de muchas empresas en Colombia, esto ha causado impacto negativo en el comercio y la productividad, lo que significa pérdidas financieras incurridas para restablecer sistemas y datos, y daño potencial a la reputación de las empresas; el *ransomware* puede acabar con organizaciones enteras si no se cuenta protocolos de respuesta a incidentes de seguridad.[41]

La mayor parte de los ataques de tipo *ransomware* tienen como objetivo principal PC y estaciones de trabajo de *Windows* aunque algunas variantes se dirigen a Linux y macOS.

Teniendo en cuenta lo anterior es importante tener presente el crecimiento tecnológico que se evidencia año tras año, a medida que avanza el tiempo así mismo crece la tecnología e información y a su vez crecen los delitos informáticos, los ciberdelincuentes cada día preparan nuevas maneras de generar ciberataques es por esto que las organizaciones se ven obligadas a proteger su infraestructura tecnológica además de su información.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Para la seguridad informática su principal objetivo es proteger los activos consta de 3 pilares para asegurar la confidencialidad, integridad y disponibilidad de información, descritos en la siguiente manera:

Disponibilidad: Corresponde a que se obtenga la información eficaz en cualquier momento teniendo en cuenta que esta debe ser únicamente a personal autorizado, para ello los equipos de comunicación deben de estar funcionando correctamente.

Integridad: Asegura que la información que se encuentra en el momento es verídica, cierta y legitima, que no pudo ser modificada por nadie.

Confidencialidad: Corresponde a que la información únicamente debe de ser manejada por personal autorizado, no deben de tener replicas o brindar información a otras personas o entidades, puesto que no toda la información de la empresa debe

[40] FIGUEROA CUBILLOS, Tatiana Esperanza, ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020, UNAD, Disponible en repositorio de la Universidad.

[41] PINZON RUIZ, Jhon Jairo, análisis del impacto de los ataques de ransomware en las organizaciones colombianas como base de conocimiento para la determinación de nuevos mecanismos de protección y minimización de riesgos cibernéticos. UNAD, Disponible en repositorio de la Universidad.

de ser conocida por todo el mundo. Por ello los usuarios no deben de brindar accesos o prestar contraseñas para evitar intrusiones en la red.[42]

Ahora bien, es necesario identificar los tipos de virus que tanto las compañías como personas están expuestos, uno de ellos es el *phishing* donde se busca la suplantación de identidad, para ello se utilizan sitios frecuentes para capturar credenciales de accesos,[43] muchos de los ciberdelincuentes utilizan esta técnica para engañar a las personas donde exponen un sitio web falso que a simple vista es igual al original, de hecho existen formas de copiar las páginas web en tan solo 5 minutos usando programas como el *httrack* y el *Credential Harvester Attack Method* de Kali linux[44]

Actualmente muchas empresas implementan el Régimen de gestión de Información (SGSI) donde se generan planes de acción, planteamiento, implementación y gestión de procesos para disminuir posibles riesgos y vulnerabilidades que puedan tener, así mismo se plantean y realizan auditorías internas para identificar posibles fallos tanto en los sistemas de gestión como al personal de las empresas, adicionalmente se tiene en cuenta que la norma ISO 27001 posee una guía de progreso incesante mediante el método de Plan-Do-Check-Act el cual consiste en Planificar, hacer, Revisar o controlar y actuar.[45]

4.6 MARCO LEGAL

Decreto 1078 de 2015

Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones donde se compilan varias modificaciones de decretos donde se establecen las obligaciones, objetivos y funciones de acuerdo con cada uno de los sectores.[46]

Decreto 1008 de 2018

---

[42] Capítulo 1. Definiciones e historia de la seguridad informática. p.9-11 [En Línea] Disponible en http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/217/4/A4.pdf

[43] RENTERIA ECHEVERRY, Fernando Antonio, Inicio y evolución de la Seguridad Informática en el Mundo, Universidad Piloto de Colombia [En Línea] Disponible en http://polux.unipiloto.edu.co:8080/00001532.pdf

[44] CREADPAG [En Línea] (22, mayo, 2018) Disponible en https://www.creadpag.com/2018/05/clonar-un-sitio-web-en-kali-linux.html

[45] ARIAS BUENAÑO, Gabriela, MERIZALDE ALMEIDA, Nelson, y NORIEGA GARCIA, Natasha UNIVERSIDAD POLITECNICA SALESIANA, Análisis y solución de las Vulnerabilidades de la seguridad informática. Guayaquil, octubre 2013 [En Línea] Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5386/1/UPS-GT000497.pdf

[46] HOYOS TURBAY, Diana Carolina FUNCION PUBLICA Decreto 1078 de 2015 [en Línea] Bogotá. 15 mayo 2015. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

“Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”[47]

CONPES 3854 de 2016.
“Política Nacional de Seguridad Digital donde se incluyen políticas de gestión del riesgo como uno de los elementos más importantes para abordar la seguridad digital”.[48]

NTC / ISO 27001:2013
“Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI)”, donde permite que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan.[49]

NTC/ISO 31000:2009
“Gestión del Riesgo. Principios y directrices que proporciona principios y directrices sobre la gestión de riesgos, a través de un marco reconocido para los profesionales y organizaciones que emplean procesos de gestión de riesgos. La ISO 31000 proporciona directrices para planificar y ejecutar sistemas de gestión de riesgos”.[50]

Ley 1581 de 2012. Es la que se sentencia el uso de la información personal mediante el amparo de datos que se localizan en las bases de datos donde se pueden generar procesos como incluir, generar cambios, actualizaciones y/o eliminación por parte de las empresas encargadas.[51]

[47] MINISTERIO DE Tecnologías DE LA Información Y LAS COMUNICACIONES Decreto 1008 de 2018 (14, junio, 2018) p. 1 [En Línea] Disponible en http://es.presidencia.gov.co/normativa/normativa/DECRETO%201008%20DEL%2014%20DE%20JUNIO%20DE%202018.pdf

[48] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN (7, marzo, 2017) Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

[49] DEPARTAMENTO ADMINISTRATIVO DEL SERVICIO CIVIL DISTRITAL NTC / ISO 27001:2013 [En Línea] Bogotá (22, junio,2006) Disponible en https://serviciocivil.gov.co/transparencia/marco-legal/normatividad/ntc-270012013

[50] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION ICONTEC [En Línea] Bogotá. (22, febrero.2011) Disponible en http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf

[51] CONGRESO DE LA REPÚBLICA. Diario Oficial No. 48.587 de 18 de octubre de 2012.Ley estatutaria 1581 de 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html/

5 DESARROLLO DE LOS OBJETIVOS

5.1 ANALIZAR CUÁLES SON LOS VECTORES DE ATAQUE MÁS COMUNES CON SUS DIFERENTES TÉCNICAS DE INTRUSIÓN UTILIZADOS PARA VULNERAR SISTEMAS DE RED DE LAS ORGANIZACIONES A PARTIR DEL MATERIAL BIBLIOGRÁFICO, INDICACIONES DE LOS FABRICANTES DE SEGURIDAD PERIMETRAL Y BOLETINES DE CIBERSEGURIDAD CON EL FIN DE BRINDAR SUGERENCIAS A NIVEL DE SEGURIDAD EN LAS ORGANIZACIONES.

En primera instancia es importante definir que es un ciber ataque, de acuerdo con el fabricante Fortinet, un ciberataque se refiere a una acción diseñada para apuntar a una computadora o a cualquier elemento de un sistema de información computarizado para cambiar, destruir o robar datos, así como explotar o dañar una red.[52]

Fortinet define una serie de ciberataques como las comunes los cuales son: Ataques de DoS, ataques de suplantación de identidad también conocidos como phishing donde combinan la ingeniería social y la tecnología para engañar y cometer fraude, ransomware, ataque de contraseña, interpretación de URL, ataque de fuerza bruta, ataques por la web, entre otros.

Es posible ver como los ciberataques a las empresas ocurren todos los días tal como lo menciono un antiguo CEO de Cisco, John Chambers, “Existen dos tipos de empresas: aquellas que han sido atacadas y aquellas que no saben que lo han sido".[53] Según Cisco el 53% de los ciberataques dan como resultado daños por USD 500.000 o más.

Para Cisco los ciberataques mas comunes son: Malware como ransomware, suplantación de identidad (Phishing), ataque de denegación de servicio (DoS), inyección SQL, entre otros.

Durante el año 2022 se realizaron diferentes estudios para identificar si hubo un crecimiento en la cantidad de ciber ataques comparado con el año 2021, el fabricante Fortinet encontró que Colombia sufrió 6.300 millones de intentos de intrusión, lo que corresponde a un aumento del 70% comparado con el 2021, estas

[52] Fortinet, Tipos de ciberataques: ataque DDoS, ransomware y más. [En línea] Disponible en https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

[53] Cisco, ¿Con que frecuencia ocurren los ciber ataques?, [En línea] Disponible en https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html#~how-cyber-attacks-work

cifras también revelan un aumento significativo en el uso del ransomware como ciberataque principal.[54]

Colombia registró en 2022 más de 54.000 denuncias por delitos cibernéticos, superando ampliamente la cifra de 2021, Julián Buitrago, teniente de la Policía y director del centro cibernético, explico que las modalidades más comunes que utilizan los delincuentes son las de *vishing* que consiste en una llamada falsa solicitando información por medio de engaños y estafas.[55]
"Los ciberdelincuentes que están dedicados a esto tienen tiempo suficiente para estar buscando en internet los registros de las personas y están ubicándolos para que entreguen datos personales y confidenciales, ubican el banco en el cual tienen cuentas y a partir de ahí, aplican diferentes técnicas para obtener esa información privilegiada", indicó el teniente coronel Julián Buitrago, director del Centro Cibernético de la Policía.

Teniendo en cuenta lo anterior se identifican como principales vectores de ataque que a su vez son un factor clave para prevenir y defender las redes empresariales. Conocerlos y adoptar las soluciones adecuadas para protegerlos puede significar la diferencia entre la continuidad del negocio y enormes pérdidas financieras. A continuación, se describen los siguientes vectores más conocidos con sus respectivas técnicas y métodos de intrusión.

- Correo electrónico: Es el principal vector de ataque debido a que es un medio utilizado por empresas de todos los tipos y tamaños, desde pequeñas hasta grandes empresas. El correo electrónico ha sido empleado por atacantes desde hace décadas como una forma de enviar correo no deseado (Spam) suplantación de identidad (Phishing) y archivos infectados con virus (Malware). Teniendo en cuenta que esta herramienta es utilizada para diferentes propósitos se estima que, en Perú, los ataques de suplantación de identidad o también llamados phishing aumentaron a 7000 cada día durante el periodo de la cuarentena por Covid.
    - El phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía, entidades del gobierno, etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial.

[54] El tiempo, ¿Cuántos ciberataques sufrió Colombia la primera parte de 2022?, [En línea] Disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cuantos-ciberataques-sufrio-colombia-en-2022-695772
[55] Camilo Alvarez, Colombia registró un crecimiento de ataques informáticos en el ultimo año, enero 13, 2023 [En línea] Disponible en https://www.vozdeamerica.com/a/colombia-registro-crecimiento-ataques-informaticos-ultimo-ano-/6916577.html

Muchas personas incluso fuera de lo empresarial han caído en este tipo de ataque de ingeniería social, ya que ingresan sus datos personales en los links que el correo falso indica.

- Este correo electrónico incluye enlaces a un sitio web preparado por los criminales -que imita al de la empresa legítima- y en el que se invita a la víctima a introducir sus datos personales.
- El malware también conocido como programa maligno, programa malintencionado o código maligno corresponde a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario. En estos correos falsos por lo general el atacante adjunto un archivo maligno el cual el receptor resulta ejecutando sin siquiera darse cuenta.

- Drive-by compromiso: Este vector de ataque está identificado como “Amenazas avanzadas persistentes o APT” porque se mezclan diversas técnicas como la ingeniería social y exploits de vulnerabilidades para identificar comportamientos de las víctimas como las visitas frecuentes a webs o dirigiéndose a sitios con scripts que se ejecutan desde el vector del navegador para inyectar en la máquina del usuario algún malware.[56]
- Navegación por internet: Este vector de ataque se conoce por medio de realizar búsquedas en Internet y descargar accidentalmente, o por medio de engaños, códigos maliciosos como Malware, Ransomware, Spyware y cualquier otro tipo de virus con la capacidad de dañar la integridad y acceso de la información, es por esto que se recomienda tener mucha precaución a la hora de navegar en internet, solo consultar paginas web conocidas y confiables, no se recomienda realizar descargar de música o audiovisuales como películas, ya que sin darse cuenta se podría estar descargando archivos infectados o maliciosas
- Ataques de fuerza bruta: Este vector es uno de los mas utilizados por los ciberdelincuentes ya que busca explotar las vulnerabilidades de los usuarios finales como el mal uso de “nickname y passwords” este ataque tuvo mayor fuerza en la época de la pandemia, ya que muchas empresas optaron por el teletrabajo sin embargo al no estar preparados para este medio de trabajo expusieron muchas vulnerabilidades que fueron aprovechadas por los ciberdelincuentes, por ejemplo el uso de usuarios y contraseñas fáciles de adivinar y poder acceder a la información de las empresas de manera sencilla. Cambiar de la oficina al hogar hizo que se pasaran por alto muchos controles de

[56] Optical Networks, ¿Qué son los vectores de ataque en ciberseguridad?, 4 Abril 2022 [En línea] Disponible en https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/#Drive-by_compromise

seguridad, convirtiendo a las conexiones remotas en el blanco predilecto de los delincuentes por el uso de contraseñas y usuario genéricos fáciles de vulnerar por ataques de fuerza bruta.

- Aplicaciones Web: Algunas aplicaciones web plantean una serie de problemas de seguridad derivados de la codificación incorrecta y el desbaratamiento de los mecanismos de autenticación. De esta forma, vulnerabilidades explotables permiten a los atacantes ganar acceso a bases de datos administradas por aplicaciones web que contienen información valiosa y confidencial (por ejemplo, detalles personales y financieros), por lo que son un blanco frecuente de los piratas informáticos debido a los inmensos beneficios que reciben a cambio de esta información.[57]
- La red: Las grandes organizaciones como entidades de gobierno, sector educativo y el rubro de bancos, poseen grandes conexiones entre sus sedes y data center. De esta manera es necesario tomar una solución de seguridad capaz de fortificar una red empresarial de gran capacidad para evitar grandes pérdidas
- Endpoint o dispositivos finales: Este tipo de vector se refiere a estaciones de trabajo que pueden ser empleados para infectar los sistemas de la organización mediante una memoria USB o un disco duro extraíble, mediante este medio un atacante puede dañar con código malicioso un computador de trabajo o infectar una red LAN.
- Explotación de vulnerabilidades: Este ataque corresponde al uso de *software* y técnicas especiales para aprovechar las vulnerabilidades encontradas y usarlas como puerta de entrada al sistema de la víctima. Se ejecuta por medio de herramientas conocidas como *exploits*
- Insiders: También conocidos como personas con acceso que pueden exfiltrar información. Pueden ser empleados insatisfechos, exempleados que conservan por fallos de procedimiento credenciales de acceso o bien los que pudieran haberse dejado sobornar por ciberdelincuentes. Es importante los controles de seguridad de estos accesos puesto que los ciberdelincuentes podrían obtener el acceso a toda la red de la compañía de primera mano.

- Debilidades en las cadenas de suministro: Este vector de ataque hace referencia a las diferentes empresas que trabajan de manera conjunto en un tipo de negociación o sociedad, si alguna de estas compañías se ve involucrada en un ciberataque o fuga de información, si sus redes e infraestructura no cuentan con

[57] Matias Ades, 5 Abril 2018, Ataques a aplicaciones Web: Fuente mas frecuente de fuga de datos, [En línea] disponible en https://blog.smartfense.com/2018/05/ataques-aplicaciones-y-web-fuga-de-datos.html

los controles y seguridad pertinente las compañías aliadas podrían sufrir el mismo tipo de ciber ataque o fugas de información.

Teniendo en cuenta lo anterior, la mayoría de vectores de ciberataques tienen en cuenta el factor humano, por lo que algunos medios consideran el factor humano como el eslabón más débil. A medida que la tecnología entra en la vida cotidiana de las empresas y organizaciones, los desafíos de seguridad aumentan. Estos problemas están relacionados principalmente con el factor humano. Según un informe de Verizon, el 85% de las violaciones de ciberseguridad son causadas por errores humanos. Grandes empresas como Uber ya se han visto afectadas por ataques de este tipo en el pasado, por lo que es importante incorporar tecnologías de ciber resiliencia en sus dispositivos. Tomando como ejemplo la empresa estadounidense VTC, un atacante utilizó un simple WhatsApp para engañar a un empleado para que accediera al sistema. Los atacantes se hicieron pasar por personas que trabajaban en el campo de la tecnología de la información y obtuvieron credenciales para acceder a la red interna de la empresa a través de VPN..[58]

Para el año 2020 según el Centro Cibernético Policial indica que la ciberdelincuencia en todo el mundo ha crecido exponencialmente con nuevas tendencias surgiendo persistentemente. Los delincuentes informáticos dominan cada vez más, donde utilizan las tecnologías existentes para su propio beneficio, donde aplican sus ataques manejando tácticas y forman redes de reciprocidad, facilitando plasmar un ataque en poco tiempo. Con el uso frecuente de internet y las variables tecnologías se establecen oportunidades para que se acometan ataques.

Durante el año 2020 se presentaron 27734 casos de ciberataques y delitos informáticos, de las cuales 640 muestras analizadas fueron de programas malignos. Las ciudades que mayor presentaron afectación en comparación con el año 2019 fue Bogotá (37%), seguido de Medellín (10%) y Cali (7%) mediante la interceptación de datos informáticos con 235% Suplantación de sitios web 377% y espionaje informático (358% 951) [59]

[58] Interempresas Ciberseguridad. El factor humano, el eslabón débil de la ciberseguridad. 2022 [En línea] Disponible en https://www.interempresas.net/Ciberseguridad/Articulos/410723-El-factor-humano-el-eslabon-debil-de-la-ciberseguridad.html

[59] POLICIA NACIONAL. *Ciberincidentes | Centro Cibernético Policial*. 2021. [En Línea] Disponibile en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

A medida que las empresas se vuelven más digitalizadas, también lo hacen las oportunidades para los ciberdelincuentes. Pero el éxito o el fracaso de estos ciberataques a las organizaciones depende de un factor clave: el elemento humano. El factor humano se ha convertido en parte de los activos de las organizaciones que deben ser protegidos, el aumento constante de los usuarios en línea y la demanda tecnológica y el estado digital de los servicios técnicos marcan la diferencia entre el éxito o el fracaso de un ciberataque.[60]

A continuación, se describen las principales amenazas de ciberseguridad dirigidas directamente al factor humano:

- *Spear Phishing*: Tipo de ataque informático que llega al empleado a través de un correo electrónico, son mensajes muy elaborados que pueden simular perfectamente la imagen de una compañía u organización importante colocando en el cuerpo del correo un enlace malicioso.
- *Whaling*: robo de información a los altos directivos de una compañía utilizando el mismo método del correo aprovechando los perfiles que tienen los directivos para acceder a información valiosa.
- *Ransomware*: Es un software malicioso que por lo general secuestra los dispositivos con información valiosa, para que este ataque sea exitoso por lo general se requiere de alguna interacción con un usuario interno de la red.
- Ingeniera social: Diferente tipos de técnicas de manipulación utilizadas para engañar a las víctimas con el fin de obtener información confidencial.

Teniendo en cuenta los riesgos asociados al factor humano estas son algunas de las medidas que las organizaciones están optando para mitigar las brechas de seguridad producidas por el teletrabajo.

- Mantener los dispositivos corporativos actualizados con los últimos parches de seguridad.
- Implementación de servicios que protejan los dispositivos tales como antivirus.
- La organización debe contar con canales de comunicación seguros con sus respectivas licencias para evitar el uso de cuentas personales y fuga de información.
- Capacitaciones constantes de buenas practicas de seguridad de la información, con el fin de que todo el personal este al tanto de los riesgos y vulnerabilidades a las que el mundo de la tecnología se encuentra expuesto.

[60] CASTILLO, Miguel Angel, El factor humano como clave de éxito frente a los ciberataques. [En línea] Disponible en https://www.open3s.com/factor-humano-en-los-ciberataques-blog/

5.2 EVALUAR LAS DIFERENTES SOLUCIONES MÁS EFICIENTES DE HARDWARE Y SOFTWARE PARA LA DETECCIÓN DE AMENAZAS Y VULNERABILIDADES EN LAS INFRAESTRUCTURAS TI POR MEDIO DE UN ANÁLISIS DE LOS DIFERENTES SOFTWARES EXISTENTES EN EL MERCADO.

La detección se convierte en un componente muy indispensable, pues a partir de ello se empiezan a reducir las acciones que envuelve un ataque. Con un monitoreo frecuente se llegan a visualizar penetraciones en los dispositivos y así mismo poder evitarlos.

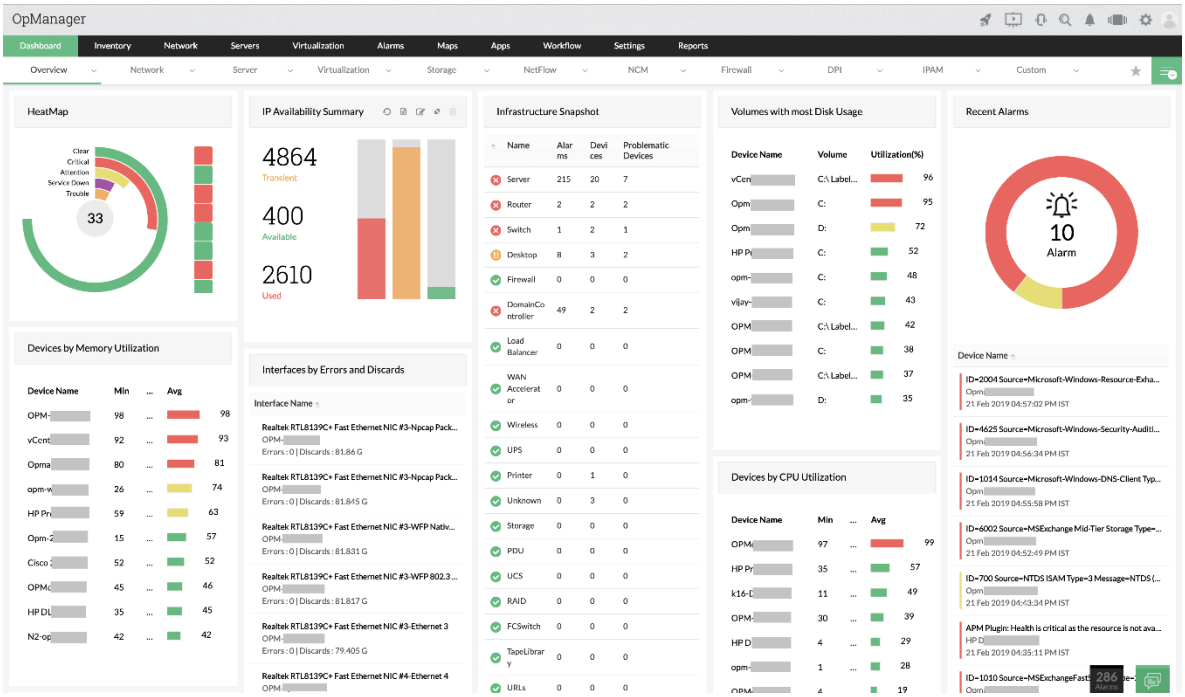
La auditoría se ha trasformado en un componente de detección muy significativo, pues se revelan las inexactitudes que puede tener una empresa, desde la indagación de los trabajadores de cómo han manejado la detección interna y externa, de acuerdo con las estadísticas, se logra detectar que la mayoría de los ataques ocurren por errores humanos.[61]

5.2.1 Herramientas de medición y detección de Amenazas en las infraestructuras TI. En la actualidad existen varias herramientas o *software* que permiten la medición y detección de amenazas y vulnerabilidades con el fin que se puedan abordar y tomar acciones para evitar ataques de ciberseguridad. Algunas de ellas son:

- ManageEngine: Herramienta SIEM para identificar operaciones y/o labores diferentes en los registros, se puede usar tanto en sistemas operativos Linux como Windows y cumple con estándares como la ISO 27001.

[61] GRIMALDO, Leidy, LA IMPORTANCIA DE LAS AUDITORIAS INTERNAS Y EXTERNAS DENTRO DE LAS ORGANIZACIONES, Documento elaborado como parte de la opción de grado para obtener el título de Contadora Pública, UNIVERSIDAD MILITAR NUEVA GRANADA, FACULTAD DE ESTUDIOS A DISTANCIA (FAEDIS) [En Línea] Bogotá 2014, Disponible en https://repository.unimilitar.edu.co/bitstream/handle/10654/13537/Importancia%20de%20las%20Auditorias.pdf;jses

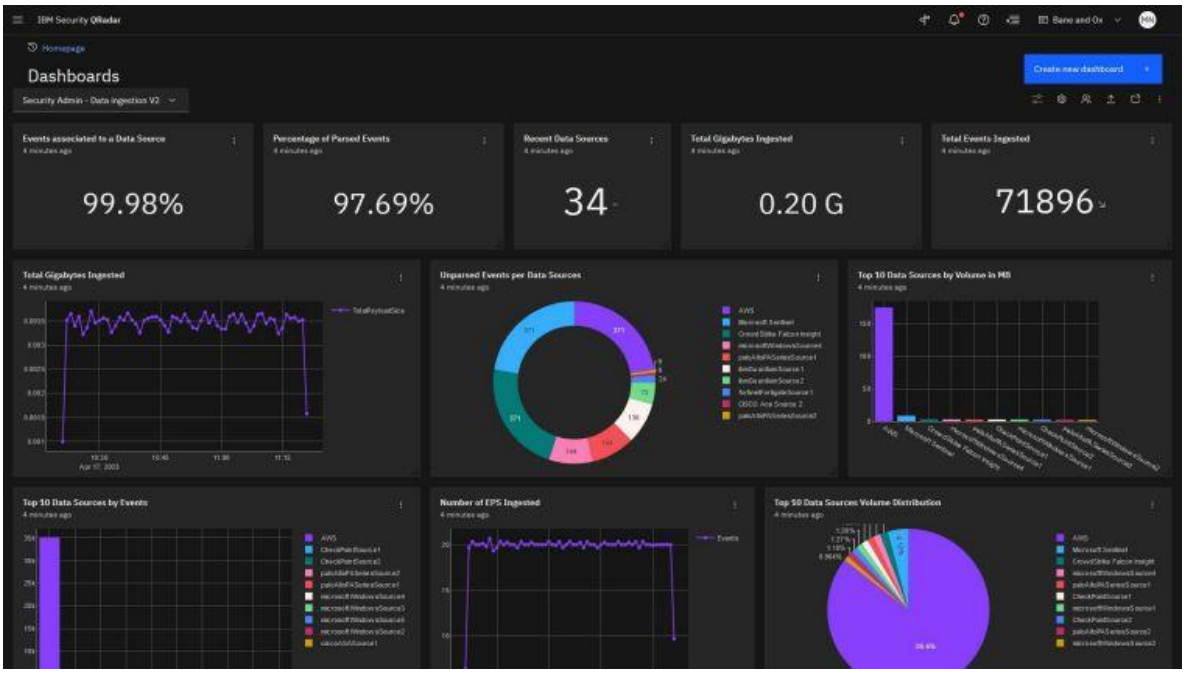
Ilustración 7 - Software de Monitoreo de red



Tomado de manageengine.com

- IBM QRadar SIEM: Además de la detección permite percibir las amenazas halladas dando una prioridad a las mismas, para ello se toman todos los datos de la compañía y se correlaciona con la base de datos de amenazas y vulnerabilidades.

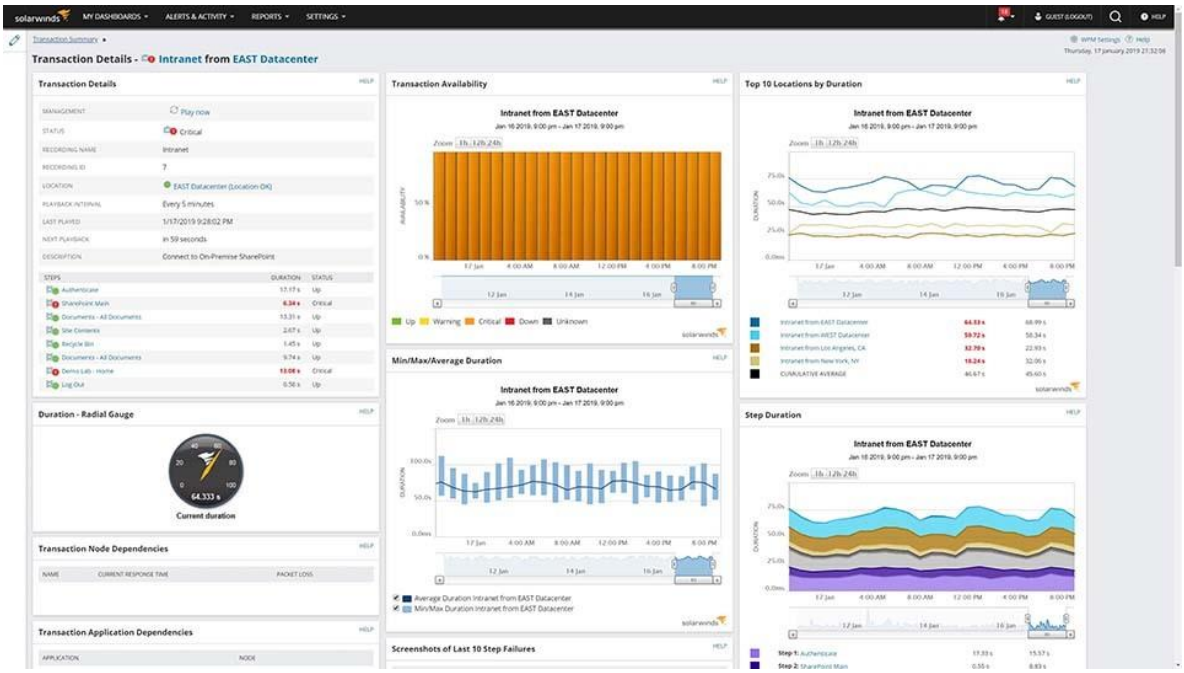
Ilustración 8 - IBM Security Qradar Suite



Tomado de ibm.com

- SolarWinds: Ofrece implementaciones en la nube y en instalaciones de sistemas operativos Windows y Linux; sus principales funciones son la detección oportuna de situaciones sospechosas, además permite un análisis forense en el cual se puede conocer la hora del evento, también permite la generación de informes.

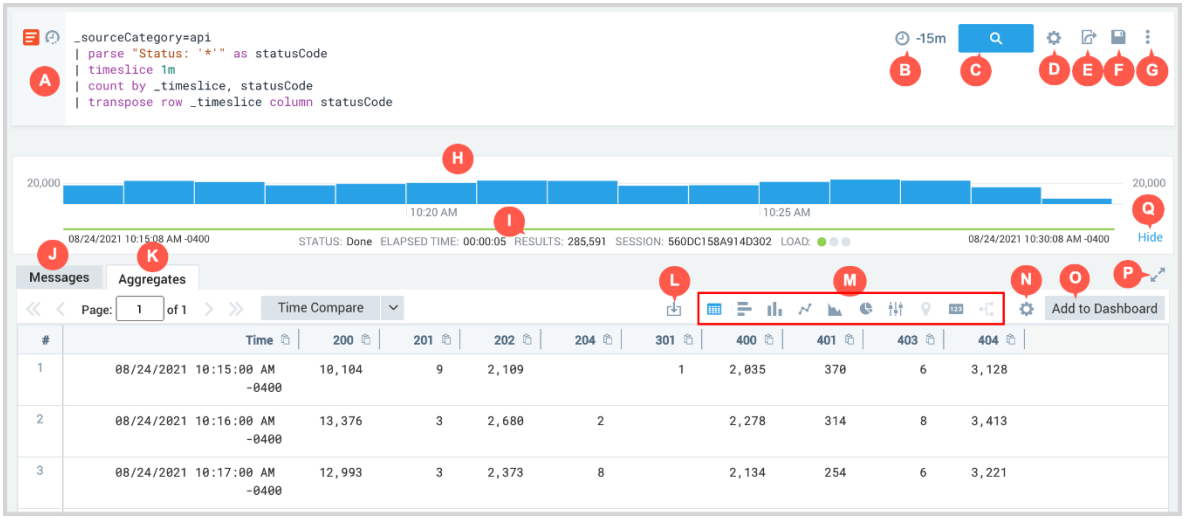
Ilustración 9 - Monitoreo de Solar Winds



Tomado de solarwinds.com

- Sumo Logic: Plataforma basada en la nube para el monitoreo, detección e investigación de actividades sospechosas, permite aislar activos y usuarios que puedan presentar riesgo.

Ilustración 10 - Suite de consulta Sumo Logic



Tomado de help.sumologic.com

- AlientVault: Consiste en una herramienta que combina múltiples factores de monitoreo como lo es la localización de amenazas, contestación a eventos o incidentes y permite la supervisión de inventarios, detección de intrusos, correlaciona eventos, entre otros.[62]

Ilustración 11 - Dashboard monitoreo AlienVault

Tomado de cybersecurity.att.com

Cabe aclarar que existen muchas herramientas en el mercado que también cumplen la función de además de identificar, monitorear, permite resolver automáticamente las vulnerabilidades encontradas, con ello se aceleran los procesos que se tienen actualmente en una compañía.

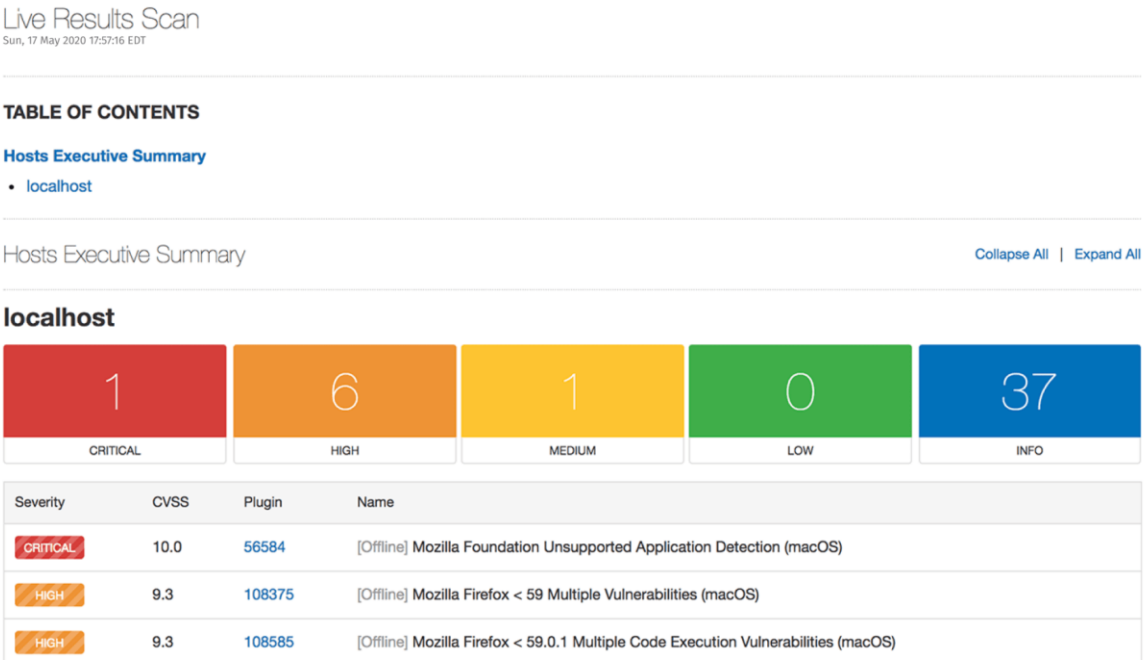
[62] KINGATÚA, Amos, geekflare, Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y empresas [En Línea] 18 febrero 2022, Disponible en https://geekflare.com/es/security-incident-response-tools/

Sin embargo, de acuerdo con investigaciones se visualiza que la herramienta Nessus cumple funciones destacadas y que sobresalen ante las demás, algunas de sus características y roles principales son:

- Cuenta con la mayor base de datos para identificar amenazas y tomar acciones frente a estas mismas.
- Contiene paneles de atribución que permite a los clientes robustecer las redes contra amenazas que se encuentran halladas.
- Es rentable dado a que se disminuyen tiempos y costos en el escaneo debido a que se pueden programar automáticamente para el cumplimiento de seguridad.
- Posee un cumplimiento del requisito PCI DSS 11.2.1. donde se pueden realizar explotaciones en la red interna del cliente.
- Nessus inicialmente lanza escaneos de puertos mediante nmap o con scanner de puertos propio con el fin de identificar cuales se encuentran abiertos y empezar a generar exploit para atacarlos.
- Cuando se corre un escaneo sobre la red o un equipo en específico se pueden generar estadísticas, pues en los resultados arrojados se pueden exportar en formatos HTML, XML, texto plano; así mismo, muestra las vulnerabilidades según la clasificación encontrada, permitiendo conocer con más detalle dicha vulnerabilidad.[63]

[63] SEAQ Servicios SAS, Nessus® es el escáner de vulnerabilidad web más utilizado de la industria. [En Línea] Disponible en https://www.seaq.co/nessus.html#:~:text=Beneficios,mayores%20amenazas%20y%20responder%20r%C3%A1pidamente.

Ilustración 12 - Evaluación de vulnerabilidades Nessus



Tomado de es-la.tenable.com

Más de 27.000 organizaciones en todo el mundo confían en este escáner para detectar, evaluar y gestionar posibles vulnerabilidades en sus sistemas. Es la tecnología de referencia en el mundo comercial. Una de sus ventajas más notables es la precisión, con la tasa de falsos positivos más baja de la industria; aproximadamente 0,32 defectos por millón de escaneos. También tiene la cobertura de vulnerabilidades más amplia y profunda del mercado.[64]

Teniendo en cuento lo anterior, con el fin de analizar los riesgos y vulnerabilidades en las capas OSI del 1 al 4 correspondientes a la infraestructura TI de una compañía se considera pertinente utilizar el software *Nessus* para obtener mayores beneficios comparados con sus competencias.

Con respecto a soluciones de *hardware* existe la empresa *Darktrace,* que ofrece soluciones de ciberseguridad basadas en inteligencia artificial y aprendizaje automático. El principal dispositivo es *Darktrace* Enterprise Immune System, el

[64] Gb-advisors, Nessus vs Trustware: ¿Cuál es el mejor escáner de vulnerabilidades?, [En línea] Disponible en https://www.gb-advisors.com/es/nessus-vs-trustwave-mejor-escaner-de-vulnerabilidades/#:~:text=Entre%20sus%20ventajas%20m%C3%A1s%20destacadas,amplia%20y%20profunda%20del%20mercado.

cual es una plataforma de ciberseguridad que utiliza tecnologías avanzadas para detectar y responder a amenazas cibernéticas en tiempo real.

A continuación, se presentan algunas de las características principales del dispositivo *Darktrace*:

Inteligencia Artificial (IA): *Darktrace* utiliza algoritmos de aprendizaje automático para analizar el comportamiento de la red y los usuarios, identificando patrones anómalos que podrían indicar actividades maliciosas.

Autodetección de Amenazas: La plataforma tiene la capacidad de aprender continuamente sobre la red y adaptarse a cambios en el entorno, permitiendo la detección temprana de amenazas.

Respuesta Automática: *Darktrace* puede tomar medidas automáticas para mitigar las amenazas detectadas, reduciendo el tiempo de respuesta y minimizando el impacto de los ataques.

Interfaz Gráfica de Usuario (GUI): Proporciona a los usuarios una interfaz visual para supervisar las amenazas, realizar investigaciones y tomar decisiones informadas.

Integración con Sistemas de Seguridad Existentes: *Darktrace* puede integrarse con otros sistemas de seguridad y herramientas existentes para proporcionar una defensa integral contra amenazas cibernéticas.

5.3 PROPONER PROCEDIMIENTOS QUE CONTRIBUYAN A LA DETECCIÓN DE AMENAZAS Y VULNERABILIDADES EN LAS INFRAESTRUCTURAS TI A PARTIR DE LAS DIFERENTES METODOLOGÍAS DE INTRUSIÓN Y COMPARATIVA DE LOS PROCESOS PARA MINIMIZAR Y GESTIONAR RIESGOS EN LAS ORGANIZACIONES.

Identificación de Riesgos. La seguridad informática es perpendicular a todas las tecnologías que se establecen en las empresas, la gestión de esta información es realmente indispensable para que una organización conserve niveles tolerables de prestación de servicios al instante de valorar los riesgos en los que se exhibe la información en la transmisión y administración para los procesos e instrucciones. [65]

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

Es por ello por lo que se requiere de *software* y *hardware* con una alta disponibilidad para evitar pérdidas de información de acuerdo con los 3 tipos de amenazas dentro de las cuales se encuentran las humanas con ataques activos y pasivos; la amenaza lógica y física, así mismo se debe de tener en cuenta los tipos de amenazas informáticas donde se usa el *phishing*, *Malware*, SPAM, *Spyware* o troyano, virus informáticos y el *Pharming*.[66]

Por otra parte, se sugiere que los riesgos, vulnerabilidades conocidas y encontradas en la infraestructura TI de una compañía, sean clasificadas de la siguiente manera:

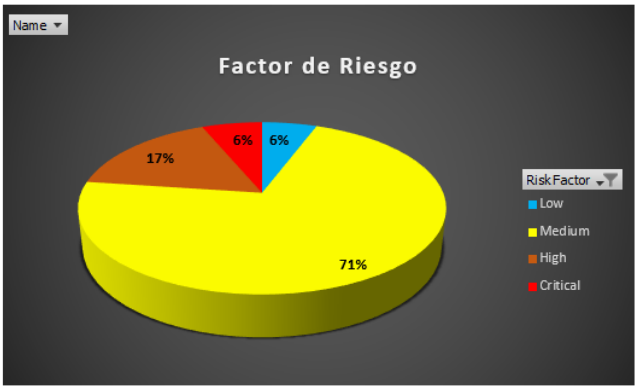
- *Low* (Baja)
- *Medium* (Media)
- *High* (Alta)
- *Critical* (critica)

[65] APD Suite, Tipos de seguridad informática: ¿Cuáles son y qué importancia tienen? [En Línea] 20 abril 2019, Disponible en https://www.apd.es/tipos-de-seguridad-informatica/

[66] IBERO, [En Línea] Tijuana México, 15 junio 2020 Disponible en https://blog.posgrados.ibero.mx/seguridad-informatica/

Ilustración 13 - Factor de Riesgo

Name	(Todas)
Factor de Riesgo	**Cantidad**
Low	170
Medium	2119
High	491
Critical	187
Total general	**2967**

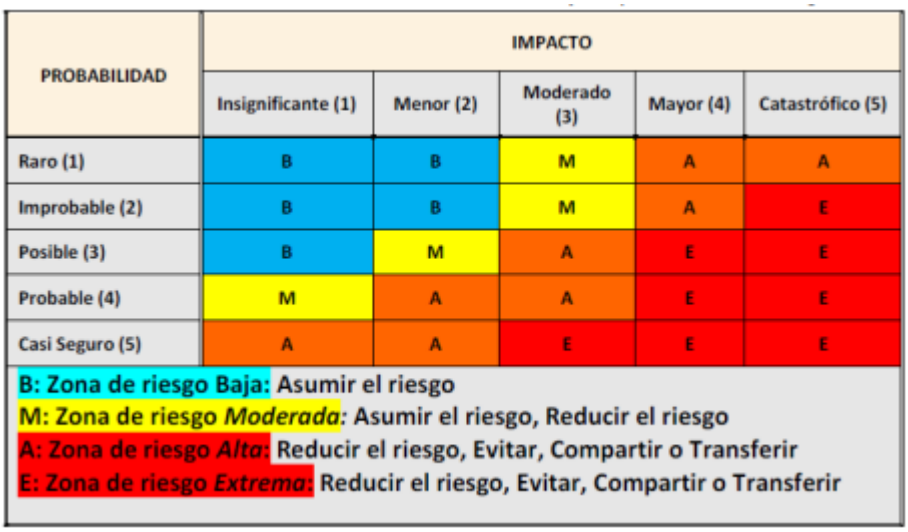


Elaboración propia

EVALUACIÓN DEL RIESGO:

Se recomienda realizar un análisis de forma cualitativa con una comparación donde se muestra el análisis de la posibilidad en que ocurra algún riesgo vs el impacto del mismo, logrando la matriz llamada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, para lo cual la guía ostenta la manera de considerar los riesgos de acuerdo con los niveles de impacto y posibilidad determinados, igualmente, se puede apreciar algunas maneras de procedimiento en un riesgo en específico, como se puede apreciar en la siguiente imagen:

Ilustración 14 - Mapa de riesgos[67]



PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Elaboración Propia

A continuación, se muestra la matriz de riesgos basada en el supuesto escaneo de vulnerabilidades realizado por parte de distintas organizaciones.

Cuadro 1. Matriz de riesgo vulnerabilidades encontradas

	IMPACTO			
PROBABILIDAD	**LOW**	**MEDIUM**	**HIGH**	**CRITICAL**
RARO	B	B	M	M
IMPROBABLE	B	B	M	A
POSIBLE	M	A	A	E
PROBABLE	M	A	A	E

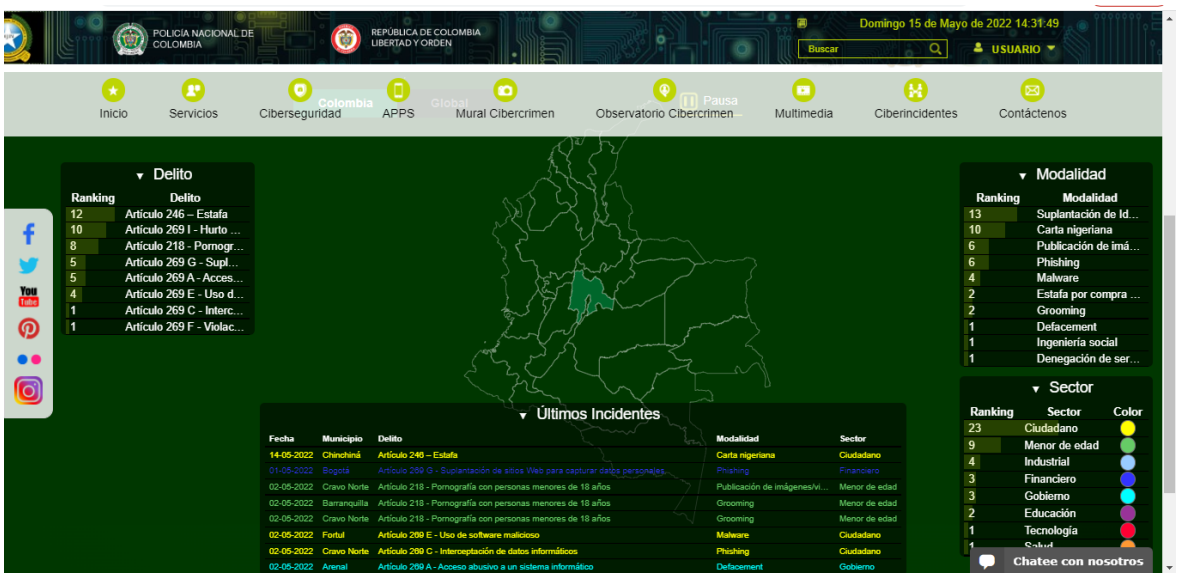
67 DAFP. Guía para la administración del riesgo. *Departamento Administrativo de La Función Pública de Colombia*, pag *4*, 49. [En Línea] 2011, Disponible en http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

B	Baja	
M	Moderada	
A	Alta	
C	Critica	

Elaboración propia

Actualmente existen páginas de monitoreo para visualización en Tiempo real sobre alertas, amenazas y vulnerabilidades tanto detectadas como reportadas, ofreciendo una alta gama de servicios para su monitoreo como lo es CAI virtual de la Policía Nacional de Colombia, Checkpoint, entre otras, no obstante se encuentran otros programas para la detección de alertas de intrusión o posibles ataques en la infraestructura, uno de ellos es conocido como Arbor donde se puede generar el monitoreo en tiempo real.

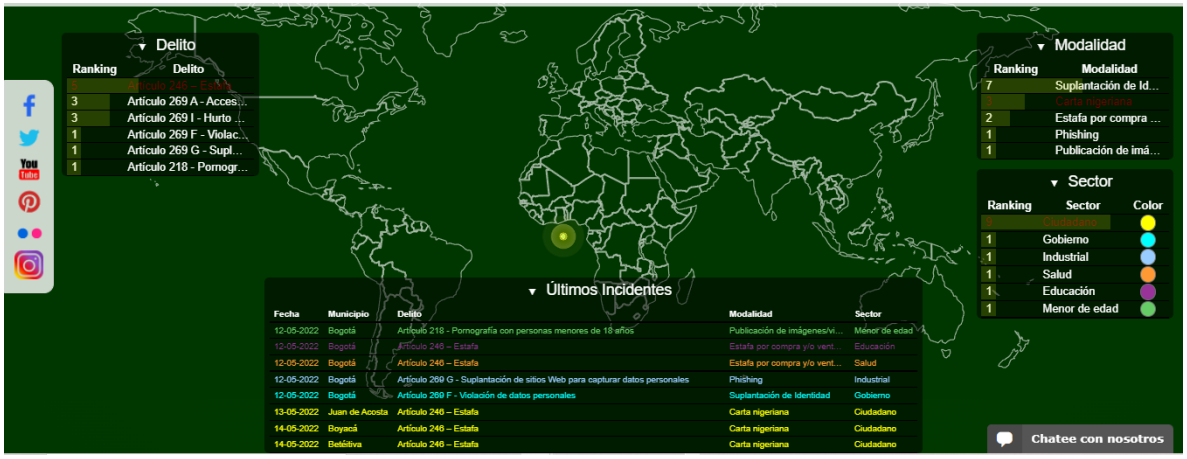
Ilustración 15 - Amenazas actuales registradas en Colombia mayo 2022[68]



Tomado de caivirtual.policia.gov.co

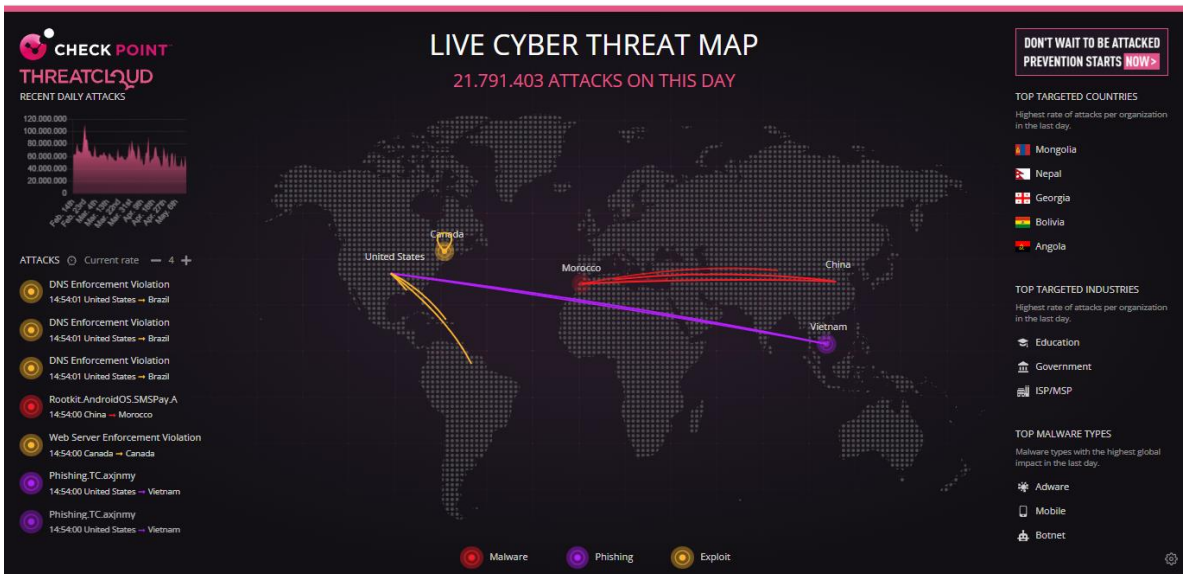
[68] POLICIA NACIONAL de Colombia, Amenazas actuales registradas en Colombia y el Mundo desde 1 a 15 mayo 2022, [En Línea] Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

Ilustración 16 - Amenazas actuales registradas en a nivel Mundial mayo 2022



Tomado de caivirtual.policia.gov.co

Ilustración 17 - Monitoreo de amenazas en tiempo Real 2022



Tomado de Threatcloud Checkpoint

Ilustración 18 - Ataques hallados de los últimos 30 días en Colombia[69]

Tomado de Threatcloud Checkpoint

5.3.2 Metodologías de intrusión y *testing* para análisis de vulnerabilidades. La metodología de intrusión y pruebas (también conocida como *Penetration Testing* o *Ethical Hacking*) es un enfoque sistemático utilizado para evaluar la seguridad de sistemas informáticos, redes y aplicaciones mediante la simulación de ataques cibernéticos controlados.

Teniendo en cuenta que existen múltiples metodologías y procesos desarrollados con el fin de realizar análisis de riesgos y vulnerabilidades, a continuación, se describirá la metodología *Magerit* (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología utilizada en España para la gestión de riesgos en sistemas de información. Fue desarrollada por el Centro Criptológico Nacional (CCN) y se utiliza ampliamente en organizaciones gubernamentales y empresas en España. El objetivo principal de MAGERIT es ayudar a las organizaciones a identificar, analizar y gestionar los riesgos de seguridad de sus sistemas de información.

Algunos de los puntos más importantes de Magerit son: Análisis de Riesgos: MAGERIT se centra en la identificación y análisis de los riesgos de seguridad de los sistemas de información. Esto implica evaluar amenazas, vulnerabilidades, impacto y probabilidad de ocurrencia.

Clasificación de Activos: La metodología MAGERIT comienza por clasificar los activos de información, lo que ayuda a priorizar la gestión de riesgos. Los activos pueden incluir datos, sistemas, hardware, software y procesos.

Fases del Proceso: MAGERIT sigue un proceso dividido en tres fases principales: Inventario de Activos y Valoración de la Información, Análisis de Riesgos y Gestión

[69] CHECKPOINT, Monitoreo de Ataques hallados de los últimos 30 Días en Colombia [En Línea] 15 mayo 2022, Disponible en https://threatmap.checkpoint.com/

de Riesgos. Cada fase implica actividades específicas para llevar a cabo el análisis de riesgos de manera sistemática.

Categorización de Riesgos: La metodología MAGERIT ayuda a categorizar los riesgos en diferentes niveles, desde los más críticos hasta los menos críticos. Esto facilita la priorización de las acciones de mitigación.

Documentación: La metodología MAGERIT promueve la documentación completa de los procesos de análisis y gestión de riesgos, lo que permite una comunicación clara y una toma de decisiones informada.

Enfoque de Toma de Decisiones: MAGERIT ayuda a las organizaciones a tomar decisiones informadas sobre cómo gestionar los riesgos identificados. Esto puede implicar la implementación de controles de seguridad, la aceptación de ciertos riesgos o la transferencia de riesgos a través de seguros.

Adaptabilidad: MAGERIT se ha desarrollado para ser una metodología flexible y adaptable, lo que significa que puede ser ajustada para adaptarse a las necesidades específicas de una organización.[70]

Para llevar a cabo esta metodología se divide en 3 fases las cuales se describen a continuación:

Fase 1: Inventario de activos y valoración de la información

Identificación de Activos: Enumerar y clasificar todos los activos de información, incluyendo datos, sistemas, hardware, software, personal y procesos relacionados con la seguridad de la información.

Valoración de Activos: Determinar el valor de los activos en términos de confidencialidad, integridad y disponibilidad. Esto se hace asignando niveles de importancia y categorizándolos.

Fase 2: Análisis de Riesgos

Identificación de Amenazas: Enumerar las amenazas potenciales que podrían afectar a los activos. Estas amenazas pueden incluir ciberataques, desastres naturales, errores humanos, etc.

[70] MAGERIT V.3, Metodología de Análisis y gestión de riesgos de los sistemas de información [En línea] Disponible en https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html

Identificación de Vulnerabilidades: Identificar las debilidades o vulnerabilidades que podrían ser explotadas por las amenazas identificadas.

Evaluación de Riesgos: Evaluar la probabilidad de ocurrencia y el impacto potencial de cada riesgo. Esto implica la determinación de la severidad de cada riesgo.

Fase 3: Gestión de riesgos

Priorización de Riesgos: Clasificar los riesgos en función de su gravedad, lo que ayuda a priorizar la gestión de riesgos. Los riesgos se pueden categorizar como críticos, importantes o menos importantes.
Selección de Medidas de Seguridad: Identificar y seleccionar las medidas de seguridad que se deben aplicar para mitigar los riesgos. Esto puede incluir la implementación de controles técnicos, políticas de seguridad y procedimientos.

Plan de Tratamiento de Riesgos: Desarrollar un plan que describa cómo se abordarán los riesgos identificados. Esto incluye la asignación de recursos, plazos y responsabilidades.

Seguimiento y Revisión: Continuar monitoreando la eficacia de las medidas de seguridad implementadas y revisar el plan de tratamiento de riesgos regularmente para adaptarse a cambios en el entorno de seguridad.

Documentación: Registrar todas las actividades realizadas y los resultados obtenidos en cada fase. Esto incluye la documentación de los riesgos identificados, las medidas de seguridad implementadas y los informes de revisión.

Comunicación: Comunicar los resultados y hallazgos a las partes interesadas clave, incluyendo la alta dirección, para asegurar una comprensión y apoyo adecuados.

Puntualmente MAGERIT Se basa en el análisis del impacto de una brecha de seguridad en la empresa, intenta identificar las amenazas que pueden afectar a la empresa y las vulnerabilidades que estas amenazas pueden explotar, permitiendo tomar medidas preventivas claras. Acción correctiva.

Lo interesante de este enfoque es que proporciona una guía completa paso a paso sobre cómo realizar un análisis de riesgos. Este método se divide en tres libros. El primero es un método que describe la estructura que debe tener un modelo de gestión de riesgos. Este libro cumple con las recomendaciones ISO para la gestión de riesgos.

El segundo libro es un Catálogo de Elementos, esta es una lista que las compañías pueden utilizar para centrar su análisis de riesgos. Como tal, contiene una

disposición sobre los activos de información que se considerarán, las características que se considerarán al valorar los activos identificados y una lista de peligros y controles que se considerarán.

Finalmente, el tercer libro es una Guía de Técnicas, lo cual lo convierte en un factor diferenciador con respecto a otras metodologías. En esta tercera parte se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.[71]

Este enfoque es útil para las empresas que comienzan a gestionar la seguridad de la información porque les permite centrarse en los riesgos que probablemente sean más críticos para el negocio, es decir, los relacionados con los sistemas de información. Curiosamente, al adaptarse a las normas ISO, su implementación se convierte en un trampolín para la certificación o mejora de los sistemas de gestión. Implementación de Medidas de Seguridad: Poner en práctica las medidas de seguridad según lo establecido en el plan de tratamiento de riesgos.

[71] GUTIERREZ, Camilo, MAGERIT: Metodología practica para gestionar riesgos, 2013, [En línea] Disponible en https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

6 CONCLUSIONES

En conclusión, a pesar de la existencia de numerosos estudios sobre ciberseguridad y la continua evolución de los modelos de protección de datos, las organizaciones siguen enfrentando una amplia gama de amenazas y vulnerabilidades que comprometen sus infraestructuras de TI. Estos desafíos pueden causar daños significativos, lo que subraya la necesidad de implementar medidas de seguridad más robustas.

Este trabajo ha identificado que muchas vulnerabilidades y riesgos en las organizaciones son atribuibles al factor humano. La falta de conocimiento sobre el valor de la información y los tipos de ataques actuales convierte al personal en una de las principales fuentes de riesgo. Por lo tanto, es fundamental desarrollar programas de capacitación continua que conciencien a los empleados sobre las mejores prácticas de seguridad y los riesgos asociados con su comportamiento diario.

Además, la insuficiencia en la implementación y cumplimiento de políticas de seguridad es un factor crítico que agrava la situación. Las organizaciones deben establecer y reforzar políticas claras, asegurándose de que todos los empleados estén informados y obligados a seguirlas. Esto incluye la realización de auditorías regulares para evaluar la adherencia a estas políticas.

La utilización de herramientas de monitoreo en tiempo real es esencial. Estas tecnologías permiten a las organizaciones identificar vulnerabilidades de manera proactiva y responder a incidentes de seguridad de forma rápida. Por ejemplo, la implementación de sistemas de detección de intrusiones (IDS) y software de análisis de vulnerabilidades puede ayudar a las empresas a anticiparse a posibles ataques, fortaleciendo su postura de seguridad.

Finalmente, es crucial realizar un análisis exhaustivo de los riesgos y vulnerabilidades utilizando software especializado para escaneo de redes. Este análisis no solo debe ser un ejercicio puntual, sino parte de una estrategia continua que informe el desarrollo de un plan de acción integral. Este plan debe contemplar medidas específicas para mitigar amenazas, como la segmentación de la red, la implementación de controles de acceso y la planificación de respuestas ante incidentes.

Al aplicar estos hallazgos en contextos reales, las organizaciones pueden mejorar significativamente su seguridad cibernética y proteger su infraestructura frente a posibles ataques, garantizando así la continuidad de sus operaciones y la integridad de su información.

7 RECOMENDACIONES

Como recomendación este documento tiene como compromiso apoyar cualquier individuo o compañía sobre las vulnerabilidades en una red, así como el amparo de la información, tener conocimientos suficientes y necesarios donde se puede llegar a perturbar un sistema de información, así como las metodologías o estrategias que se pueden llegar a manejar para advertir, descubrir y responder ante variados ataques que concurren en las redes.

Es esencial que futuras investigaciones se centren en desarrollar y evaluar programas de capacitación continua para empleados. Estos programas deben proporcionar conocimientos suficientes y necesarios para identificar y responder ante posibles perturbaciones en los sistemas de información. Incluir metodologías y estrategias para advertir, descubrir y responder ante diversos tipos de ataques cibernéticos fortalecerá la seguridad general de la organización.

Teniendo en cuenta los estándares, regularizan el procedimiento que se debe efectuar en la seguridad de las redes, admitiendo una mejor vigilancia y mayor funcionamiento. Se propone que el personal delegado de los sistemas de información se empape de conocimiento para ayudar a la conservación concorde a los entornos de red.

Sabiendo que la tecnología tiene un gran avance en la actualidad y se encuentra en constante actualización, se recomienda que las compañías se mantengan al tanto de esta información, ya que los ciberdelincuentes continúan creando nuevos ataques y buscando nuevas maneras de vulnerar las compañías, por lo que se hace necesario mantener la infraestructura protegida y actualizada en todo momento.

Se recomienda el uso de herramientas como Nessus para la detección de vulnerabilidades. A pesar de la existencia de diversas herramientas en el mercado, Nessus permite realizar un análisis completo de las capas del modelo OSI en una infraestructura de TI, proporcionando una visión detallada de las posibles vulnerabilidades.

Se recomienda utilizar una metodología de intrusión o *pentesting*, con el fin de poder auditar procesos internos y la infraestructura tecnológica de las organizaciones, por medio de estas metodologías es posible identificar todas las vulnerabilidades presentes y así poder mitigar estos riesgos de manera oportuna evitando ataques y daños mayores.

Las investigaciones deben explorar la creación y mejora constante de políticas de seguridad de la información. Estas políticas deben regularizar los procedimientos necesarios para la seguridad de las redes, permitiendo una mejor vigilancia y mayor eficiencia operativa. Se recomienda que el personal encargado de los sistemas de información esté bien informado y capacitado para mantener la integridad de los entornos de red.

8 BIBLIOGRAFÍA

1LIBRARY. Vulnerabilidades del modelo OSI [En Línea] Disponible en https://1library.co/article/vulnerabilidades-modelo-osi-seguridad-modelo-osi.z1l2ee3q

ALEMÁN NOVOA, R. B. C. Vista de Metodologías para el análisis de riesgos en los sgsi Publicaciones e Investigación. [En Línea] Bogotá. 2010. Disponible en https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

AMBIT TEAM, ambit-bst Tipos de Vulnerabilidades y Amenazas informáticas [En Línea] 10 noviembre 2020, Disponible en https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

APD Suite, Tipos de seguridad informática: ¿Cuáles son y qué importancia tienen? [En Línea] 20 abril 2019, Disponible en https://www.apd.es/tipos-de-seguridad-informatica/

ARIAS BUENAÑO, Gabriela, MERIZALDE ALMEIDA, Nelson, y NORIEGA GARCIA, Natasha UNIVERSIDAD POLITECNICA SALESIANA, Análisis y solución de las Vulnerabilidades de la seguridad informática. Guayaquil, octubre 2013 [En Línea] Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5386/1/UPS-GT000497.pdf

BECERRA POZAS, José Luis, CIO México, Guía para entender, y recordar, el modelo de red de 7 capas, Profesional Review [En Línea] 21, diciembre, 2017 Disponible en https://cio.com.mx/guia-entender-recordar-modelo-red-7-capas/

BERMUDEZ Kelly, BAILON Edber. Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/Iec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros. [En línea]. Bogotá: mayo de 2015. Disponible en https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Capítulo 1. Definiciones e historia de la seguridad informática. p.9-11 [En Línea] Disponible en http://www.ptolomeo.unam.mx:8080/jspui/bitstream/132.248.52.100/217/4/A4.pdf

CASTILLO José Antonio, Modelo OSI: que es y para que se utiliza, [En Línea] 22, noviembre, 2018 Disponible en https://www.profesionalreview.com/2018/11/22/modelo-osi/

CHECKPOINT, Monitoreo de Ataques hallados de los últimos 30 Días en Colombia [En Línea] 15 mayo 2022, Disponible en https://threatmap.checkpoint.com/

CLOUDFLARE. Modelo OSI cloudflare. Disponible en https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

COMMUNITY, F. (2019). ¿Cuál es la diferencia entre modelo OSI y modelo TCP/IP? | FS comunidad. [En Línea] 2019. Disponible en https://community.fs.com/es/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

COMUNICACIONES Decreto 1008 de 2018 (14, junio, 2018) p. 1 [En Línea] Disponible en http://es.presidencia.gov.co/normativa/normativa/DECRETO%201008%20DEL%2014%20DE%20JUNIO%20DE%202018.pdf

CONGRESO DE LA REPÚBLICA. Diario Oficial No. 48.587 de 18 de octubre de 2012.Ley estatutaria 1581 de 2012. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html/

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN (7, marzo, 2017) Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf

CREADPAG [En Línea] (22, mayo, 2018) Disponible en https://www.creadpag.com/2018/05/clonar-un-sitio-web-en-kali-linux.html

CRESPO MARTÍNEZ, E. Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Ecu@Risk In Enfoque UTE [En Línea] 2017 Vol. 8, Issue 1. Disponible en https://doi.org/10.29019/enfoqueute.v8n1.140

DAFP. Guía para la administración del riesgo. Departamento Administrativo de La Función Pública de Colombia, pág. 4, 49. [En Línea] 2011, Disponible en http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

DELPHI MAGIC. Tipos de ataques en cada nivel del modelo OSI Delphi Magic. Disponible en https://delphimagic.blogspot.com/2019/08/tipos-de-ataques-en-cada-nivel-del.html#:~:text=Navegando%20por%20la%20red%20me,%2C%20sesi%C3%B3n%2C%20presentaci%C3%B3n%20y%20aplicaci%C3%B3n.

DEPARTAMENTO ADMINISTRATIVO DEL SERVICIO CIVIL DISTRITAL NTC / ISO 27001:2013 [En Línea] Bogotá (22, junio,2006) Disponible en https://serviciocivil.gov.co/transparencia/marco-legal/normatividad/ntc-270012013

DIGITAL GUIDE IONOS. [En Línea] 25 de marzo de 2020. Disponible en https://www.ionos.es/digitalguide/servidores/know-how/el-modelo-osi-un-referente-para-normas-y-protocolos/

DOCUSIGN. [En línea] 24 de agosto de 2021. Disponible en https://www.docusign.mx/blog/seguridad-de-la-informacion

DRAGONJAR. DragonJAR. [En Línea] Disponible en https://www.dragonjar.org/la-arquitectura-de-seguridad-osi.xhtml

EDBER, B. M. K. G. B. Análisis En Seguridad Informática Y Seguridad De La Información Basado En La Norma Iso/Iec 27001- Sistemas De Gestión De Seguridad De La Información Dirigido a Una Empresa De Servicios Financieros. 2015

GIUSTO BILIĆ, Denise, We Live Security, Seguridad de la Información Universidad Veracruzana. 02 junio 2015 [En Línea] Disponible en https://www.uv.mx/infosegura/general/noti_red-4/

GRANIER, F. Electroindustria. [En línea] mayo de 2011. Disponible en http://www.emb.cl/electroindustria/articulo.mvc?xid=1593&ni=la-seguridad-informatica-se-construye-desde-la-base#:~:text=Seguridad%20seg%C3%BAn%20la%20capa%20del%20modelo%20OSI&text=A%20nivel%20l%C3%B3gico%20(capa%202,en%20base%20a%20direcciones%20MAC.

GRIMALDO, Leidy, LA IMPORTANCIA DE LAS AUDITORIAS INTERNAS Y EXTERNAS DENTRO DE LAS ORGANIZACIONES, Documento elaborado como parte de la opción de grado para obtener el título de Contadora Pública, UNIVERSIDAD MILITAR NUEVA GRANADA, FACULTAD DE ESTUDIOS A DISTANCIA (FAEDIS) [En Línea] Bogotá 2014, Disponible en https://repository.unimilitar.edu.co/bitstream/handle/10654/13537/Importancia%20de%20las%20Auditorias.pdf;jses

HOLGUIN Fresia, L. L. Model for measuring the maturity of the risk analysis of information assets in the context of shipping companies. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacion, [En línea] 2019 1-17pag. Disponible en https://doi.org/10.17013/risti.31.1-17

HOYOS TURBAY, Diana Carolina FUNCION PUBLICA Decreto 1078 de 2015 [en Línea] Bogotá. 15 mayo 2015. Disponible en https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

IBERO, [En Línea] Tijuana México, 15 junio 2020 Disponible en https://blog.posgrados.ibero.mx/seguridad-informatica/

Ibid., Universidad itroque, Curso CISCO Modulo 3.2.2.1, [En Línea], Disponible en http://itroque.edu.mx/cisco/cisco1/course/module3/3.2.2.1/3.2.2.1.html

INFRAESTRUCTURA, R., & LANAMMEUCR. En 2016 Vol.1

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION ICONTEC [En Línea] Bogotá. (22, febrero.2011) Disponible en http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf

KASPERSKY. Kaspersky. [En Línea] Disponible en https://latam.kaspersky.com/resource-center/threats/ransomware

KINGATÚA, Amos, geekflare, Las 9 mejores herramientas de respuesta a incidentes de seguridad para pequeñas y empresas [En Línea] 18 febrero 2022, Disponible en https://geekflare.com/es/security-incident-response-tools/

LOPEZ, María Teresa, Universidad de Murcia, Departamento de Sociología, [En Línea] 2013, Disponible en https://www.tdx.cat/bitstream/handle/10803/117203/TESIS.pdf?sequence=

LOZANO Michael, CORREA Miguel, ANÁLISIS DE LAS VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA MEDIANTE TESTING DE CAJA BLANCA, BAJO LA NORMA ISO 27005 EN LA COMPAÑÍA CARACOL RADIO, NODO PRINCIPAL BOGOTÁ. [En Línea] Bogotá, 2020 Disponible en https://repository.ucc.edu.co/bitstream/20.500.12494/16502/1/2020_Analisis_Vulnerabilidades_Infraestructura.pdf

LOZANO, J. R. Itadmins [En Línea] 10 de octubre de 2019. Disponible en https://itadmins.es/networking-i-el-modelo-osi/

MATHEUS Yuri, Alura Latam 4 junio 2021 [En Línea] Disponible en https://www.aluracursos.com/blog/el-modelo-osi-y-sus-capas

MICROSOFT. [En Línea] Disponible en https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=El%20phishing%20es%20un%20ataque,que%20fingen%20ser%20sitios%20leg%C3%ADtimos.

MONSALVE, J. CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). [En Línea] Bogotá. 2020. Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

NIVEL4 SEGURIDAD [En Línea] (14, diciembre,2020) Disponible en https://blog.nivel4.com/noticias/la-ciberseguridad-su-origen-y-la-trayectoria-que-ha-tenido-hasta-nuestros-dias/

NOVOA, A. Vista de Metodologías para el análisis de riesgos en los sgsi Publicaciones e Investigación. Bogotá. 2010 [En línea] Disponible en https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

POLICIA NACIONAL de Colombia, Amenazas actuales registradas en Colombia y el Mundo desde 1 a 15 mayo 2022, [En Línea] Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

POLICIA NACIONAL. Ciberincidentes | Centro Cibernético Policial. 2021. [En Línea] Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

RENTERIA ECHEVERRY, Fernando Antonio, Inicio y evolución de la Seguridad Informática en el Mundo, Universidad Piloto de Colombia [En Línea] Disponible en http://polux.unipiloto.edu.co:8080/00001532.pdf

ROJAS, C. E. UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA. [En Línea] 2015 Disponible en https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/7402/Carlos_Exam.Suf.Prof_titulo_2014.pdf?sequence=1&isAllowed=y

SÁNCHEZ-Henarejos, et al. Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Atencion Primaria, [En Línea] Bogotá, 2014. p. 214–222 Disponible en https://doi.org/10.1016/j.aprim.2013.10.008

SEAQ Servicios SAS, Nessus® es el escáner de vulnerabilidad web más utilizado de la industria. [En Línea] Disponible en https://www.seaq.co/nessus.html#:~:text=Beneficios,mayores%20amenazas%20y%20responder%20r%C3%A1pidamente.

SGSI, ISO 27001: Los activos de información, [En Línea] 30 marzo 2015, Disponible en https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

SOFISTIC CYBERSECURITY [En Línea] 30 Nov 2019 Disponible en https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

Universidad itroque, Curso CISCO Modulo 3.2.2.1, [En Línea], Disponible en http://itroque.edu.mx/cisco/cisco1/course/module3/3.2.2.1/3.2.2.1.html

Universidad Itroque, Curso CISCO, modulo 2.2.1.2 [En Línea] Disponible en http://itroque.edu.mx/cisco/cisco1/course/module3/3.3.1.2/3.3.1.2.html#:~:text=Encapsulaci%C3%B3n%20de%20datos&text=Esto%20com%C3%BAnmente%20se%20conoce%20como,el%20protocolo%20que%20se%20utiliza.

WELIVESECURITY [En Línea] 1 Jun 2015 Disponible en https://www.welivesecurity.com/la-es/2015/06/01/como-fortalecer-capas-redes-informaticas/

BENITO Maria, Ciberdelincuencia: ¿Qué es y cómo combatirla?, 2023 [En línea] Disponible en https://blogs.uoc.edu/edcp/ciberdelincuencia-que-es-y-como-combatirla/

FORTRA, Qué es el escaneo de vulnerabilidades y cómo funciona, 2022 [En línea] Disponible en https://www.fortra.com/es/blog/escaneo-vulnerabilidades

Web Performance Monitor, SolarWinds [En línea] Disponible en https://www.solarwinds.com/es/web-performance-monitor

ManageEngine OPManager, Software de monitoreo de red [En línea] Disponible en https://www.manageengine.com/latam/network-monitoring/

IBM, IBM Security QRadar Suite [En línea] Disponible en https://www.ibm.com/mx-es/qradar

AT&T Cybersecurity, Dashboard AlienVault [En línea] Disponible en https://cybersecurity.att.com/open-threat-exchange/security-tools

Tenable, Analisis de vulnerabilidades [En línea] Disponible en https://es-la.tenable.com/products/nessus

MAGERIT V.3, Metodología de Análisis y gestión de riesgos de los sistemas de información [En línea] Disponible en https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html