IDENTIFICACIÓN DE VULNERABILIDADES Y RIESGOS EN LOS ACTIVOS DE TI DE ENERGITEL.

ING. HILBERT LEONARDO SANCHEZ GAMBOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
IBAGUÉ
2018

IDENTIFICACIÓN DE VULNERABILIDADES Y RIESGOS EN LOS ACTIVOS DE TI DE ENERGITEL.

ING. HILBERT LEONARDO SANCHEZ GAMBOA

Monografía como requisito para optar el título de: Especialista en Seguridad Informática

PhD(c). Gabriel Mauricio Ramírez
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA –UNAD
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
IBAGUÉ
2018

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Ibagué, 16, Septiembre, 2018

DEDICATORIA

La presente monografía proyecto de grado que se desarrolló con mis mayores esfuerzos la dedico a mis padres, esposa e hija quienes me han apoyado dándome ánimos y estimulándome para que logre mis objetivos, y metas propuestas como profesional.

AGRADECIMIENTOS

Quiero agradecer a mi dios, quien con su bendición me dio la fortaleza y la sabiduría de continuar formándome como profesional, a mis padres por estar en la lucha continua para enfrentar este reto tan importante en mi vida, y los orientadores de la Unad quienes me han guiado por el buen camino brindándome las herramientas necesarias para consolidar este proyecto de gran calidad.

RESUMEN

La presente monografía consiste en la descripción, gestión, análisis e identificación de las principales vulnerabilidades y riesgos a los que están expuestos los activos de TI de la organización Enegitel, resaltando la importancia de la protección de la información para mantener la disponibilidad, confidencialidad e integridad, en el periodo transcurrido del año 2015 a 2018.

Se pudo establecer las características de las condiciones actuales, que han generado inestabilidad dentro de la organización debido a los ataques informáticos que han afectado el sistema informático deteriorando la estabilidad y continuidad de la organización, dicha debilidad del sistema informático radica en el fácil acceso a ciertos dispositivos que tienen contraseñas vulnerables que son fáciles de identificar, por esta razón se ha visto la necesidad de implementar una metodología para contrarrestar estas vulnerabilidades y así evitar los riesgos que han sido originados por la falta de controles de acceso a sus dispositivos.

Problemas que ocasionaron perjuicios a nivel interno y externo materializándose en pérdidas o fugas inevitables de información confidencial, dicho análisis ayudara a la empresa a diseñar estrategias de mejora para así mitigar el impacto generado por los ataques informáticos evidenciados.

Se propone la utilización de la metodología como la Magerit que es una alternativa que se puede implementar para evaluar la seguridad del sistema informático existente, de esta forma determinar la vulnerabilidad y así tomar medidas preventivas contra ataques futuros en la organización.

El problema de investigación a parte de analizar e identificar las falencias o debilidades del sistema informático, busca salvaguardar la información poniendo en conocimiento los controles que se deben implementar para mitigar el efecto de los riesgos como producto de la materialización de las amenazas.

Palabras Clave

Monografía, seguridad, amenazas, vulnerabilidades, riesgos, controles, activos de TI, ataques informáticos, Hackers, Magerit, metodologías, fugas de información, salvaguardar, materialización, confianza, autenticación e integridad.

ABSTRACT

This monograph consists of the description, management, analysis and identification of the main vulnerabilities and risks to which the IT assets of the Enegitel organization are exposed, highlighting the importance of information protection to maintain availability, confidentiality and integrity. , in the period elapsed from the year 2015 to 2018.

It was possible to establish the characteristics of the current conditions, which have generated instability within the organization due to computer attacks that have affected the computer system deteriorating the stability and continuity of the organization, said weakness of the computer system lies in the easy access to certain devices that have vulnerable passwords that are easy to identify, for this reason we have seen the need to implement a methodology to counteract these vulnerabilities and thus avoid the risks that have been caused by the lack of access controls to their devices.

Problems that caused damages internally and externally materializing in losses or inevitable leaks of confidential information, this analysis will help the company to design improvement strategies to mitigate the impact generated by the computerized attacks evidenced.

It is proposed the use of the methodology as the Magerit that is an alternative that can be implemented to evaluate the security of the existing computer system, in this way to determine the vulnerability and thus take preventive measures against future attacks in the organization.

The research problem apart from analyzing and identifying the flaws or weaknesses of the computer system, seeks to safeguard the information by making known the controls that must be implemented to mitigate the effect of the risks as a result of the materialization of the threats.

Keywords

Monograph, security, threats, vulnerabilities, risks, controls, IT assets, computer attacks, hackers, Magerit, methodologies, information leaks, safeguard, materialization, trust, authentication and integrity.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Monografía: Estudio detallado de un proceso o tema en particular, que brinda un aporte y la cual está ceñida a una secuencia ordenada de pasos para obtener buenos resultados.

Seguridad informática: Seguridad informática: es cualquier medición que impide la realización de operaciones no legales sobre un sistema o red informática, cuyos resultados pueden ocasionar daños sobre la información, involucrando su confidencialidad, autenticidad o integridad, reduciendo el rendimiento de los equipos, bloquear el acceso de usuarios autorizados al sistema.

Vulnerabilidad: son posibilidades que existen de que una amenaza se materialice contra un activo[1]. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, la información es vulnerable a los movimientos de los hackers, mientras que una parcial eléctrica es vulnerable a un cortocircuito. Al realizar el análisis de riesgo hay que tener en cuenta la vulnerabilidad de cada activo.

Riesgo: a la probabilidad que se materialice o no una amenaza beneficiándose de una vulnerabilidad[2]. No crea riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no es real la amenaza para la misma.

Tecnología de la información: relacionado con el uso implementos de telecomunicaciones y computadoras (dispositivos) para la transmisión, el procesamiento y el almacenamiento de datos. La noción integra cuestiones propias de la informática, la electrónica y las telecomunicaciones.

Activos informáticos: son los que permiten el desarrollo de las actividades diarias dentro de una organización, es el recurso más importante debido a que sin ellos las actividades serian difíciles de realizar, pero son muy vulnerables a los diferentes ataques informáticos que se presentan a nivel de procesos dentro de una compañía por la gran cantidad de información contenida en ellos.

Políticas de Seguridad: son una serie de reglas o directrices plasmadas y documentadas que indican cómo se llevan a cabo determinados procedimientos y actividades al interior de una organización.

Gestión de activos: Está basada en la protección de los activos de información por medio de un inventario de identificación, que permite determinar su grado de valor y su clasificación en el interior de la organización.

---

1 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 13

2 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 14

Control de accesos: Metodología para tener el control de acceso al sistema de información, privilegios o beneficios de algunos usuarios ayudados por tres directrices como lo es la identificación, autenticación y autorización.

Seguridad Informática: Son métodos que permiten elaborar una serie de normas, mecanismos y procedimientos primordiales para obtener un sistema de información confiable y seguro.

Confiabilidad: Accesibilidad a personal autorizado, dimensiones de seguridad que cumple una función específica durante un lapso de tiempo en otras palabras que cumpla durante un tiempo determinado las condiciones establecidas optimizando las expectativas de la empresa.

Integridad: Certeza e integridad de la información y procesos. “propiedad de salvaguardar la exactitud e integridad de los activos"[3]

Disponibilidad: Acceso a la información y procesos por parte del personal autorizado, cuando sea necesario. “La propiedad de un activo de estar disponible y utilizable cuando lo requiera una persona, entidad o proceso autorizados. Ibid[3]”

No repudio: Es una forma de negar él envió de un mensaje o información que fue trasmitido, es una manera de demostrar que una información fue enviada por emisor o receptor.

Trazabilidad: es la delimitación de los componentes generales y distintivos de los productos sometidos a proceso, los primeros permiten mostrar una relación entre ellos y los segundos reconocen el proceso[4]. La seguridad de la información a nivel de ENERGITEL, depende del grado de protección y seguridad de sus activos de información, por lo tanto, es básicamente la implementación de medidas, controles de seguridad apropiados, y el permanente control, revisión y avance de los mismos de manera efectiva y dinámica.

Ethical Hacking: Test de intrusión o pruebas de penetración que se realiza en un sistema informático para validar su nivel de seguridad y así localizar vulnerabilidades que podría aprovechar un a hacker dependiendo de su perfil sea bueno o malo dependiendo de sus propósitos.

Magerit: Es una metodología para facilitar el análisis, gestión y aplicación del sistema general de riesgos, facilitando los principios esenciales y requisitos mínimos

3 Cabezas, Ivan Correa Martha. Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional SIUN. 2014. [En linea] [10 de junio de 2018] disponible en: https://studylib.es/doc/7044575/definici%C3%B3n-de-pol%C3%ADticas-de-seguridad-inform%C3%A1tica-de-los-s...

4 Asintec. ¿Qué es Trazabilidad? [En linea]. [Citado 17 junio 2018] disponible en: http://www.asintec.es/que-es-trazabilidad/article/130-2

para la protección oportuna de la información también le permita a la empresa saber cuánto valor está en juego, ayudándola a protegerse dando la opción a los directivos tomar decisiones.

NTC- ISO 27001:2013: es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan, su objetivo es la implementación de un SGSI, evaluar los riesgos y aplicar los controles[5].

NTC- ISO 27002:2013: Es un módulo de buenas prácticas que explica los objetivos de control y exámenes requeridos en cuanto a seguridad de la información, contiene 39 objetivos de control y 133 controles, integrados en 11 dominios. Actualmente, la última edición de 2013 ha sido renovada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles divulgándose inicialmente en inglés y en francés tras su alianza de publicación el 25 de Septiembre de 2013[6].

Metasploit: es un software de código fuente abierto para realizar pruebas de pentesting en sistemas, que se utiliza para la gestión de vulnerabilidades informáticas y poder detectar posibles intrusos y provee información sobre vulnerabilidades de seguridad[7].

5 ISOTOOLS. ¿Qué es la NTC ISO 27001? [En linea]. [Citado 17 junio 2018] disponible en: https://www.isotools.com.co/normas/ntc-iso-27001/

6 UTP. Universidad Tecnológica de Pereira. [En linea]. [Citado 18 junio 2018] disponible en: https://www.utp.edu.co/gestioncalidad/sin-categoria/279/ntc-iso-iec-27002/pdf

7 REDESZONE. DE LUZ. Sergio. Ya puedes ejecutar Metasploit Framework directamente en un contenedor Docker. [En linea]. [Citado 17 junio 2018] disponible en: https://www.redeszone.net/2016/05/15/ya-puedes-ejecutar-metasploit-framework-directamente-contenedor-docker/

INTRODUCCIÓN

La seguridad informática es un método de control, que permite identificar los usuarios que usan los recursos informáticos, tecnología e información de la organización, con el propósito de evidenciar las vulnerabilidades, amenazas y riesgos que enfrenta, respecto a los pilares básicos de confidencialidad, integridad y disponibilidad de la seguridad de la información. Considerando que la información que maneja la organización es amplia por los medios electrónicos, que son fáciles de vulnerar e interceptar, por ello la empresa debe implementar métodos y procedimientos de control para mitigar el impacto que generan esos riesgos.

Esta monografía pretende generar un diagnóstico del estado actual de la seguridad de la información de la empresa Energitel, su baja inversión presupuestal en seguridad, la poca importancia en la implementación de políticas de seguridad y la falta de conocimiento respecto a cultura en seguridad informática.

Para ello requiere de la implementación de estándares como ISO 27001, metodologías Magerit, y Ethical Hacking debido a que la seguridad de la información requiere de la revisión, monitoreo, seguimiento y mejoras en los procesos que involucran los activos informáticos de la organización Energitel en cuestión de ataques cibernéticos los cuales le han ocasionado grandes pérdidas económicas.

Identificadas las vulnerabilidades no deseadas, se pretende establecer medidas respecto a la seguridad de los sistemas informáticos garantizando la continuidad del modelo de negocio que podría estar en riesgo. La presente monografía permite visualizar las vulnerabilidades y riesgos de seguridad informática que tiene la compañía Energitel, debido a que no tienen los conocimientos y herramientas mínimas para detectarlos y contrarrestarlos teniendo en cuenta que no son conscientes de la magnitud del riesgo y tampoco han tomado medidas respecto a temas de seguridad de la información.

Esta monografía documenta de forma clara la identificación, detección y tratamiento que se debe dar a las diferentes vulnerabilidades y riesgos existentes en la organización Energitel, respecto a la perdida de información como por ejemplo la propuesta del Conjunto las Juanas y el conjunto Verde Menta, con el propósito de garantizar la protección de la información entendido como el activo más importante.

Por otra parte realizar la evaluación de seguridad del sistema informático con la utilización de metodologías como la Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), Ethical Hacking o la misma ISO 27001 para establecer controles pertinentes y así reducir el nivel de exposición de los activos informáticos evitando que se exploten las vulnerabilidades existentes del sistema pero a su vez permitiendo el fortalecimiento de la organización en temas de seguridad.

1. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

El desarrollo y avance de las nuevas tecnologías, en la última década, ha dado un impulso considerable a nuevos medios de comunicación e interacción, donde la seguridad en redes es un tema primordial para las organizaciones debido al gran número de ataques cibernéticos que enfrentan las empresas respecto al manejo de su información. Los empleados y usuarios de la empresa Energitel manifiestan que tienen problemas en la seguridad de su sistema informático debido a la perdida de información por los ataques que ha enfrentado.

Robo de información, en el año 2016 del equipo portátil del supervisor de zona repercutiendo en la pérdida de un contrato[8] de redes de distribución de MT (Media Tensión) del Condominio las Juanas el cual fue ejecutado por el proveedor de servicio Electrotodo de la competencia.

Perdida de información, se detectó que 3 de los 15 empleados para un total del 20% tienen privilegios de acceso al sistema informático los cuales han suministrado información confidencial a clientes y socios. Información perdida, por abuso de privilegios y falta de control en la accesibilidad al sistema informático, información del proyecto[9] Verde Menta para diseño eléctrico, por valores invertidos por verificaciones en terreno, cálculos de cargas, visitas técnicas, viáticos y ejecución de informes y socios que se han desvinculado de Energitel, (Hacienda el Pilar, Pailaquinta y Purifil) ocasionando pérdidas monetarias mes a mes[10].

La empresa Energitel tiene identificado los siguientes ataques (3) que han afectado la operativa, robo de contrato de redes Condominio las Juanas. (Ver anexo D), perdía de información proyecto de diseño eléctrico conjunto Verde Menta Año 2016. (Ver anexo E), y suministro de información base datos de clientes (Ver anexo F).

Los ataques cibernéticos[11] hoy en día son más profesionales y específicos los cuales generan vulnerabilidad para el acceso de la información prioritaria, que pondría en riesgo la razón de ser de la compañía, y afectando la calidad del servicio ofertado por la empresa. Para Energitel la información contenida en su sistema informático y bases de datos es fundamental para su normal funcionamiento teniendo en cuenta que los procedimientos que realiza a nivel de servicios tienen

8 ANEXO D. PROPUESTA DE PROYECTO DE ELECTRIFICACIÓN CONJUNTO LAS JUANAS (ROBO DE CONTRATO).

9 ANEXO E. PROYECTO DE DISEÑO VERDE MENTA (PERDIDA DE INFORMACIÓN).

10 ANEXO F. PÉRDIDA DE INFORMACIÓN DE CLIENTES.

11 ANEXO G. ACTA DE REUNION Y EVALUACION MENSUAL

que brindar solidez en cuestión de seguridad de la información que posee para sus clientes y proveedores (ver anexos de figuras 19 y 20).

La baja confidencialidad de las contraseñas hace fácil el acceso de información a través de los equipos de cómputo, generando robo de contratos, clientes, pólizas de cumplimiento, estados de cuentas y abuso de privilegios, para acceder a las bases de datos de la compañía, deterioran la estabilidad del negocio.

Este proyecto pretende dar a conocer las debilidades que presentan el sistema informático de Energitel y las amenazas existentes a las que está expuesta y los impactos generados por los riesgos evidenciados. De acuerdo con Areitio[12] riesgo, asociado a un activo señalado dentro de la organización, mirado como la probabilidad de que una amenaza se materialice sobre un activo y ocasione un determinado impacto.

Las vulnerabilidades advierten la existencia de la debilidad de un activo, esta puede llegar a concretarse o no dependiendo de la situación de cada organización, para ello es necesario tomar medidas efectivas de control o salvaguardas, como lo indica Javier Jarauta Sánchez[13], salvaguarda: Medición de control para disminuir el riesgo asociado a una conocida amenaza.

Vulnerabilidades identificadas, antivirus desactualizados, no se tienen copias de seguridad y procedimiento de backup, fluctuaciones de energía en el sistema de distribución y protección, daños en hardware (daño del disco duro del equipo Samsung Core i3 Windows 7), caída de red de energía y servidor fuera de servicio (perdida de información en equipos de trabajadores del área de ATC, atención al cliente) y pérdida de credibilidad (pérdida de confianza de los socios y usuarios).

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué medidas y procedimientos se pueden implementar para minimizar el impacto generado en el sistema informático debido a las vulnerabilidades y riesgos que afectan la seguridad de los activos de Energitel?

12 Areitio. Javier. Seguridad Informática. Capítulo 2: Análisis de riesgo de seguridad. Pág. 57. [En linea]. España: Paraninfo, 2008. [Citado 15 marzo 2018] disponible en: https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q=Riesgo&f=false

13 Javier Jarauta Sánchez. Seguridad Informática Capítulo 1: Introducción y conceptos básicos Definiciones: Análisis y Gestión de Riesgos. [En linea]. [Citado 15 marzo 2018] disponible en: https://www.iit.comillas.edu/palacios/seguridad/cap01.pdf

2. JUSTIFICACIÓN

La seguridad informática es el proceso por medio del cual se protegen los activos informáticos, debido a que lo más importante dentro de una organización es la información contenida en sus bases de datos[14], se puede decir que la información es la base principal más trascendental a la hora de tomar decisiones para cada una de ellas por eso es tan importante la protección y prevención de los sistemas de información.

Héctor Jara[15], afirma que una de las formas más distinguidas de expresar la idea de seguridad informática es la siguiente: un grupo de medidas de prevención, localización, y modificación, destinadas a proteger la confiabilidad, integridad y disponibilidad de los activos de información.

Las organizaciones vienen siendo objeto de incontables ataques a sus sistemas por delincuentes informáticos cuyas personas tienen gran conocimiento en los medios informáticos y en el manejo de sus herramientas que las usan para delinquir y perjudicar, por eso es de vital importancia idear estrategias de seguridad que permitan establecer algún tipo de barreras que minimicen de manera efectiva los ataques tanto internos.

Uno de los métodos para lograr minimizar los impactos provocados por un ataque informático, es tener conocimiento claro de la manera cómo operan estos atacantes y determinar los puntos débiles de nuestro sistema informático de esta forma se creará una barrera que minimice la efectividad de estos ataques. Se puede garantizar que los activos, recursos informáticos de una entidad u organización estarán disponibles si se tiene un claro conocimiento e identificación de las potenciales técnicas hacking a las que estas se enfrentan.

Se conserva la necesidad primordial de proteger la integridad de la información de la organización Energitel, esta propuesta a parte de beneficiar pretende establecer un análisis para prevenir las debilidades del sistema informático y de esta manera traspasar los obstáculos de seguridad permitiendo establecer, mejorar o actualizar las políticas de seguridad respecto a sus activos informáticos debido a que son responsabilidad de la misma organización, además de garantizar a sus clientes y proveedores mayor seguridad y confianza.

---

14 ANEXO G. ACTA DE REUNION Y EVALUACION MENSUAL

15 JARA. Héctor. Ethical Hacking 2.0. Implementación de un Sistema para la Gestión de la Seguridad. [En linea]. [Citado 05 julio 2018] disponible en: https://books.google.es/books?hl=es&lr=&id=PkDCIzakkB4C&oi=fnd&pg=PA4&dq=ethical+hacking+espa%C3%B1ol&ots=B4v-9UA65w&sig=k0V5i4e7qr4xpqBDh9VAX0IAafc#v=onepage&q=ethical%20hacking%20espa%C3%B1ol&f=false

La iniciativa es proveer a Energitel la oportunidad de identificar vulnerabilidades y corregir los errores de seguridad en su red antes de que sean aprovechados, para que así la empresa pueda mejorar la seguridad de su sistema informático, implementando controles de acceso a sus datos, para establecer, documentar y revisar la política de control de acceso con base a los requisitos del negocio y seguridad de la información.

Al adoptar un control de acceso apropiado se garantizará que sólo se permita el acceso a personal autorizado, de modo que se reduzcan las fallas operativas, realizando controles en la red, verificando copias de seguridad, cumplimiento de normas, análisis de resultados y control de actividades sospechosas permitiendo al sistema informático de Energitel ser confiable en el manejo y gestión de la información.

Las vulnerabilidades[16] latentes en el sistema informático de Energitel han ocasionados cambios negativos y perdidas monetarias, a su vez han generado una mala atmosfera respecto a sus colaboradores y deterioro de la imagen corporativa frente a sus clientes y proveedores, para ello se disponen metodologías como lo es Ethical Hacking o la misma Magerit que a futuro se puedan implementar para mitigar el impacto producido por la materialización de las amenazas provenientes de las debilidades del sistema informático y posteriormente convertidos en riesgos.

El Ethical Hacking[17], es de las técnicas de seguridad informática más deseadas por las grandes organizaciones a nivel mundial, todos los días aumenta la necesidad de tener personas con los suficientes conocimientos en este campo, para neutralizar los ataques de la creciente comunidad de hackers, la cual tiene mayor representación en Asia y el Medio Oriente, pero que esta regada por todo el mundo.

Es muy angosta la línea entre un hacker de sombrero blanco y un hacker de sombrero negro, a nivel de competencia ambos tienen el mismo talento de reconocer vulnerabilidades y/o fallos en sistemas, para sacar ganancia de la situación, el hacker ético tiene como labor aprovechar estas vulnerabilidades y reportar las mismas, el fin nunca es el sacar utilidad económica de la situación, por lo contrario, el objetivo es hacer advertencias y/o crear controles para la mejora del sistema[18].

16 BARRIOS CANTILLO. Jaime (2017). Pasos para el análisis de riesgos basados en MAGERIT. [En línea]. [11 de febrero de 2017] [revisado 25 marzo de 2018] disponible en: https://es.slideshare.net/jaimeral73/pasos-para-el-anlisis-de-riesgos-basados-en-magerit.

17 ISAZA VILLAR, Miguel Arturo. La Seguridad Informática Hoy. [En línea], 20 de septiembre de 2013 [revisado 25 marzo de 2018]. Disponible en: https://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html

18 VALENCIA BLANCO. Leidi Stefani. Universidad Mayor de San Andrés Metodologías Ethical Hacking. [En línea], [revisado 25 marzo de 2018]. Disponible en: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a12.pdf

De acuerdo con Areitio[19] la inclinación, cada vez más dominante, hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones, e incluso, de las compañías, ha ubicado a la seguridad de los sistemas de información como una pieza central en todo el avance de la sociedad.

La seguridad ha pasado de emplearse para conservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener un uso de dimensiones inimaginables y crecientes que incluye negociaciones financieras, intercambios contractuales, información personal, documentos médicos, comercio y lucros por internet, domótica, inteligencia ambiental y computación ubicua.

Según adminso[20], lo primero que se debe tener en cuenta es la protección física de los diferentes dispositivos del sistema informático. Cualquier elemento en general y, con particular atención, los servidores y hardware de red, deben situarse en sitios protegidos para que solo el personal tenga acceso a ellos. Los mecanismos adaptables varían desde una habitación con una cerradura y llave, a los más complejos métodos de acceso por huella digital, cámaras de seguridad y guardias que reaccionen ante violaciones de la política de acceso.

Según Manjarres[21], el constante desarrollo de las tecnologías de la información ha ocasionado a la sociedad en general, la propagación de los denominados delitos informáticos, los cuales están caracterizados en el delito instrumentado por el uso de los computadores a través de redes de comunicación e interconexión de la computadora, ocasionados por la limitada cultura informática lo cual es un agente crítico en el impacto de los ataques informáticos en la sociedad.

Con la implementación de la metodología Magerit se puede dar solución a todas aquellas vulnerabilidades presentes en el sistema informático de Energitel evitando que los delincuentes informáticos tengan acceso a la información, permitiendo ofrecer recomendaciones y definir controles para detectar problemas y reducir los riesgos evidenciados.

19 Areitio. Javier. Seguridad Informática. 1a ed. España: Paraninfo, 2008. p.2

20 Adminso. Administración de sistemas operativos. Prevención. [En línea] [Consultado 11 de febrero de 2017] disponible en: http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos

21 Iván. Manjarrés. Bolaño, Caracterización de los delitos informáticos en Colombia, Octubre 2012. [En línea] [Consultado 11 de febrero de 2017] disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar la seguridad del sistema informático para identificar los mecanismos que permitan mitigar las vulnerabilidades y riesgos a los que están expuestos los activos de TI de Energitel.

3.2 OBJETIVOS ESPECÍFICOS

1. Verificar que activos en lo concerniente a sistemas de información TI de Energitel son vulnerables y pasan a fase de riesgos.

2. Determinar las causas de los riesgos potenciales a los que está expuesta la organización en cuanto a la tecnología que posee.

3. Establecer procedimientos para identificar y mitigar las vulnerabilidades y riesgos evidenciados.

4. Definir estrategias de seguridad para la protección de la información y así disminuir el riesgo de ataques en cuanto al manejo de la información de Energitel.

4. MARCO REFERENCIAL

En este marco se presenta la identificación de las vulnerabilidades y riesgos que afectan la operativa de Energitel, pretendiendo buscar soluciones positivas a su operativa y orientada a la perspectiva concreta de los profesionales en seguridad de la información para salvaguardar los activos informáticos.

De acuerdo con Ferro[22] las TI son un grupo de técnicas y productos originados de las nuevas herramientas (hardware y software), soportes de la información y vías de comunicación, enlazadas con el almacenamiento, procesamiento y transmisión digitalizados de la información de forma activa y en grandes proporciones.

Las organizaciones[23] requieren de un gran trabajo para avalar la seguridad, frente a las insistentes amenazas que hoy en día violan la seguridad de la información que cada vez son más especializadas, complejas y avanzadas. La normatividad vigente regula, demanda mayor protección, privacidad de los datos sensibles, personales, comerciales, financieros de los clientes y de las organizaciones.

Stallings[24] con la incorporación del computador, se hizo obvio la necesidad de establecer herramientas automatizadas para la protección de archivos y otros tipos de información guardada en el computador. Esto pasa fundamentalmente en el caso de los sistemas compartidos como, por ejemplo, un sistema de tiempo compartido; y la necesidad se recalca en los sistemas a los que se puede acceder por medio de una red telefónica publica, una red de datos o internet.

De acuerdo con José Fernández G[25], la Seguridad Informática, radica en asegurar que los bienes del sistema de información (material informático o software) de una organización sean usados de la forma que se planteó y que el ingreso a la información allí contenida así como su alteración solo sea posible por las personas que se encuentren autorizadas y dentro de los límites de sus permisos.

---

22 Ferro Soto, Carlos. Martínez Senra Ana Isabel. Otero Neira, Ma Carmen. Ventajas del Uso de las Tics en el proceso de Enseñanza Aprendizaje desde la Óptica de los Docentes Universitarios Españoles. Edutec. Revista Electrónica de Tecnología Educativa. Número 29/julio 2009, pág. 3

23 DUCUARA CRUZ. ángel Yesid. MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE. [En línea], 11 de febrero de 2017 [revisado 14 julio de 2018]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/997/Proyecto%20de%20Grado%20Manual%20de%20Buenas%20Practicas%20DANE.PDF?sequence=1&isAllowed=y.

24 Stallings, Williams. Fundamentos de seguridad en redes aplicaciones y estándares. Segunda edición. Madrid. Pearson Educacion.2004. Pág. 2

25 José Fernández G. Seguridad en Informática Aspectos Duros y Blandos. Octubre 2013. [En línea]. [revisado 14 julio de 2018]. Disponible en: http://www.aprocal.org.mx/files/2200/03SeguridadenInformaticaV1.0.pdf

El mundo de la informática es vulnerable de soportar algún tipo de ataque por terceras personas, con el deseo de difundir algún tipo de malware o robar información primordial de la víctima. Debido a esto, es importante tomar las medidas que sean precisas para mantener en buen estado la información. Dentro de todo esto, las bases de datos son uno de los sistemas que más padecen de este tipo de ataques. Para acceder a ella, los hackers investigan cualquier tipo de vulnerabilidad que no haya sido examinada para acceder al sistema[26].

Para ello es indispensable promover una metodología funcional, concreta, clara y drástica para la valoración y tratamiento de los riesgos de seguridad, con el propósito de saber el estado actual de la seguridad de los activos de información que son los que mueven el negocio, permitiendo identificar las amenazas que puedan complicar la seguridad de la información.

Proporcionar un servicio eficiente y de calidad, pueden hacerse dinámicamente y bajo demanda de los propios usuarios, si su sistema operativo gestiona los recursos del sistema, optimiza su uso, resuelve conflictos y permite realizar las tareas de forma sincrónica, coordinando todo el funcionamiento del hardware y el software.

Las fallas del sistema operativo son muy comunes y actualmente son blanco de los ataques que causan alto impacto en el sistema, pero esto puede mitigarse con la introducción de mecanismos y medidas de seguridad para reducir las pérdidas de confiabilidad, integridad y disponibilidad de la información.

La realización, notificación y documentación del manual de políticas de seguridad de la información que contiene los requisitos, normas, responsabilidades y lineamientos que regirán la seguridad de la información de la organización permiten disminuir al máximo los riesgos asociados con la seguridad de la información, y que son de gran compromiso para la Alta Dirección que a su vez compromete aspectos administrativos, físicos y tecnológicos dirigidos a orientar y proteger los activos de información.

Según Walter Vega Velasco[27], Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos, es decir, acomodarse y mejorarse constantemente según las modificaciones que se presentan en los ambientes donde se originaron.

26 ACENS. Bases de datos y sus vulnerabilidades más comunes. [En línea]. https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

27 Walter Vega Velasco. Septiembre de 2008. . [En línea]. http://www.scielo.org.bo/scielo.php?pid=S2071-081X2008000100008&script=sci_arttext&tlng=es

Según Walter Vega Velasco[28], Recursos de información, se consideran así a las bases de datos, manuales de usuario, procedimiento operativos o de soporte, planes de continuidad, información archivada, disposiciones de emergencia para la recuperación de información.

ISO 2700[29], las amenazas son las situaciones que desencadenan en un incidente en la empresa, ocasionando un perjuicio material o pérdidas inmateriales de sus activos de información. El Sistema de Gestión de Seguridad de la Información justificado en la ISO 27001 favorece al controlar las amenazas que pueden desencadenar los incidentes. La definición de amenaza es la multiplicidad de consecuencias, lo que hay que tener en cuenta es examinar el impacto.

Aguilera López[30] Amenaza se entiende como la asistencia de uno o más componentes de diversa naturaleza (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema provocándole daños aprovechando su nivel de vulnerabilidad.

4.1 MARCO TEÓRICO

La sociedad actual, muestra cambios constantemente gracias a los avances tecnológicos en los sistemas informáticos, por tal razón las empresas deben optar por el cambio y acondicionar sus servicios, estrategias y objetivos hacia la seguridad de su información supliendo las necesidades del cliente.

Gómez Vieites[31] Seguridad informática es “cualquier medida que impide la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden llevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos, bloquear el acceso de usuarios autorizados al sistema”.

El sistema informático se debe almacenar, administrar y gestionar de forma que se garantice la confidencialidad, integridad y disponibilidad, como síndrome de identificación del peligro, para clasificarlo y protegerlo de los ataques y daños con el propósito de conocer las debilidades y así adoptar medidas para la restauración

28 Walter Vega Velasco. Septiembre de 2008. [En línea]. [Consultado 20 de julio de 2018] disponible en: http://www.scielo.org.bo/scielo.php?pid=S2071-081X2008000100008&script=sci_arttext&tlng=es

29 SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: Amenazas y vulnerabilidades. [En línea]. [Consultado 20 de julio de 2018] disponible en: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

30 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 13-14

31 Gómez Vieites, Álvaro. Seguridad informática Básico. [En línea]. [Consultado 20 de julio de 2018] disponible en: http://www.ecoeediciones.com/wp-content/uploads/2016/08/seguridad-informatica-basico.pdf

de la información contenida en las bases de datos minimizando riesgos y ataques con la implementación de la ISO27001[32] la cual especifica que es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan.

Los pilares de la seguridad Informática buscan proteger la información para que esta pueda ser resguardada, para ello la protección de la información debe ser concreta y tener una accesibilidad controlada con unas políticas que aparte de ser documentadas deben ser llevadas a cabo para salvaguarda.

Las normas que rigen la funcionalidad de los sistemas informáticos deben estar avaladas por la normatividad legal vigente en pro de las buenas prácticas para la seguridad de la información. Las vulnerabilidades identificadas en los equipos logran sacar a la luz las falencias y fallas en la seguridad del sistema de información.

Los métodos de seguridad, y políticas de acceso definidas es el fin primordial del proyecto de grado del cual se derivan innumerables soluciones y de las cuales se tomarán como referencia proyectos desarrollados e implementados en Colombia con resultados efectivos en cuanto a la aplicabilidad y continuidad del negocio. En Colombia, la Universidad de los Andes diseñó un "Esquema de Seguridad en Redes de Datos" en donde se determina el análisis de vulnerabilidades aplicado a la empresa las cuales fueron objeto de estudio y evaluación.

Riesgo[33] es la posibilidad de que se origine un impacto en un activo o en el dominio. Para Magerit la deducción del riesgo presenta un indicador que accede a tomar decisiones por confrontación explícita con un Umbral de Riesgo definido; ósea una cualidad de relación Vulnerabilidad /Impacto y por tanto un vínculo entre Activos y Amenazas.

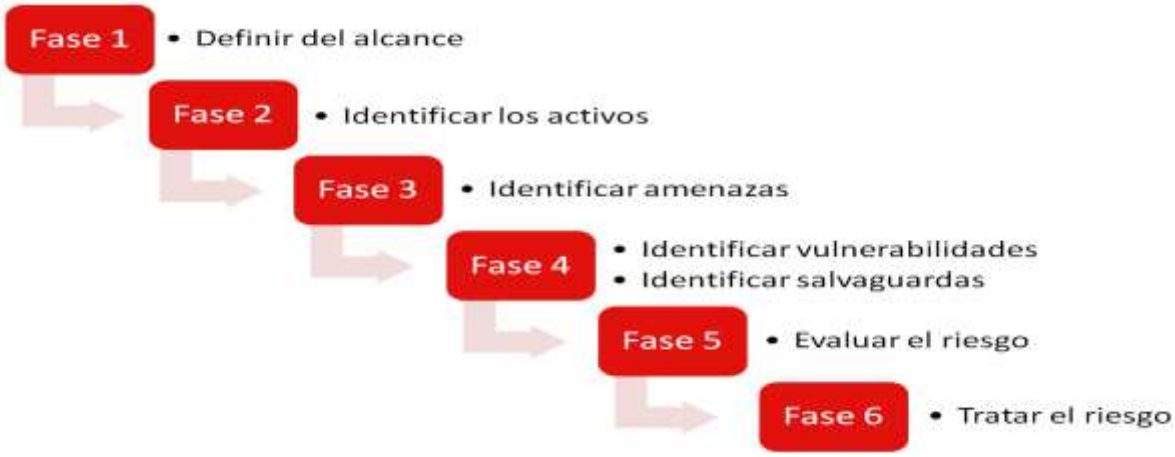
Magerit[34] implementa el Proceso de Gestión de Riesgos dentro de un ámbito de operación para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos provenientes del uso de tecnologías de la información. Las facetas esenciales más comunes de la metodología que constituyen el análisis de riesgos según Magerit se pueden percibir en la siguiente figura.

32 ISOTOOLS. ¿Qué es la NTC ISO 27001? [En línea]. [Consultado 10 marzo 2018] disponible en: https://www.isotools.com.co/normas/ntc-iso-27001/

33 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT Versión 1.0. Riesgo. [En línea]. [Consultado 31 agosto 2018] disponible en: recuperado de: http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

34 MAÑAS, José A. MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p 7

Figura 1 Fases del análisis de riesgo según Magerit



Fuente: Instituto Nacional de Ciberseguridad (incibe), 2017

¿Porque es importante la implementación del análisis y gestión de los riesgos? Primero hay que saber que Magerit es un instrumento que facilita la protección de la información, el cual permite investigar los riesgos y con la ayuda de las fases de análisis de riesgo poder tomar medidas apropiadas para controlarlos de forma efectiva y así reducir al mínimo el impacto que estos generan en los sistemas de información. Por otra parte, brindara a sus clientes y proveedores la garantía y confianza respecto al tratamiento de su información personal, aumentando la seguridad de los servicios tecnológicos que ofrece.

4.1.1 Vulnerabilidad en sistemas informáticos. Las vulnerabilidades en seguridad informática se refieren a la debilidad que poseen los sistemas informáticos los cuales pueden ser utilizados por un agente externo como un hacker o cracker para causar daño, ocasionando malestar en las bases de datos y en la información de carácter privado de la organización, la preocupación principal de las empresas es la posibilidad de que la vulnerabilidad se materialice dejando grandes pérdidas financieras.

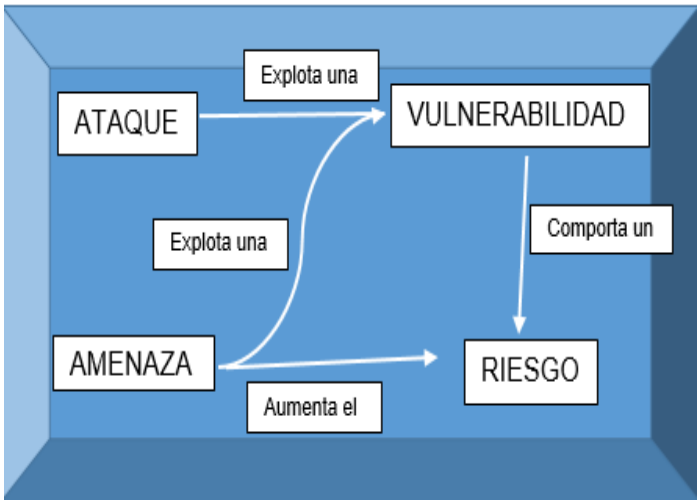
Aguilera López[35] Vulnerabilidades son hipótesis que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Al realizar el análisis de riesgo hay que tener en cuenta la vulnerabilidad de cada activo.

35 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 13

4.1.2 Amenazas informáticas. Iglesias Mouteria[36] define amenaza como cualquier factor que pueda causar potencialmente una afectación a una empresa por medio de la exposición, transformación o daño de información, o mediante la negación de servicios críticos. Las amenazas pueden, también, comprometer la reputación de una organización. Es toda actividad que explota una vulnerabilidad para atacar la seguridad de un sistema de información, ocasionando un efecto negativo sobre los activos informáticos de cualquier organización.

4.1.3 Riesgos en sistemas informáticos. Aguilera[37] denomina riesgo a la expectativa que se materialice o no una amenaza aprovechando una vulnerabilidad. No establece riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. La gran cantidad de información almacenada en los sistemas informáticos, crea una dependencia de la misma y el manejo inadecuado que se le dé incide en nuevos riesgos que al materializarse darán vía libre a las pérdidas de los activos informáticos, dichos riesgos van evolucionando con el trascurrir del tiempo y se refleja en el ritmo acelerado de los cambios tecnológicos.

Figura 2. Relación entre Ataque, riesgo amenaza.



Fuente: Autor

36 Iglesias Mouteria, Rubén. Instalación De Redes Informáticas e Ordenadores. España Editorial Ideas Propias .2006 Pág. 136

37 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 14

4.1.4 Tecnologías de información. Pérez[38] define tecnología de la información el uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. La idea objeta cuestiones propias de la informática, la electrónica y las telecomunicaciones

Se define TI aquellas herramientas y equipos tecnológicos diseñados y aplicados para la consecución de las actividades de forma rápida y precisa permitiendo que las labores sean más fáciles de hacer ayudando al tratamiento y proceso evolutivo de la información.

4.1.5 Activos informáticos. Los activos informáticos son los que permiten el incremento de las actividades diarias dentro de una organización, es el recurso más importante debido a que sin ellos las actividades serian difíciles de realizar, pero son muy vulnerables a los diferentes ataques informáticos que se presentan a nivel de procesos dentro de una compañía por la gran cantidad de información contenida en ellos.

Como Menciona Aguilera[39] Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La aparición de los activos facilita el movimiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en cada uno de ellos un daño ocurrido a otro.

4.2 MARCO CONCEPTUAL

Según Mario G. Piattini Velthuis[40], la calidad de los sistemas informáticos se ha catalogado hoy en día uno de los principales objetivos estratégicos de las organizaciones debido a que, cada vez más, su vida depende de los sistemas informáticos para su buen funcionamiento. En la evolución experimentada por la calidad en esta área se ha pasado de un método centrado básicamente en la fiscalización y descubrimiento de errores en los programas, a una semejanza más

38 Pérez, Julián Gardey, Ana. Definición de tecnología de información. [En línea]. [10 julio 2018] disponible en: (https://definicion.de/tecnologia-de-la-informacion/)

39 Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 12-14

40 Mario G. Piattini Velthuis. Calidad de sistemas informático. [En línea]. [10 junio 2018] disponible en: https://books.google.com.co/books?id=yoi4GAAACAAJ&dq=importancia+de+los+sistemas+informaticos&hl=es&sa=X&ved=0ahUKEwjAzKP82O_aAhVJrFMKHaaLBQwQ6AEIMDAC

sistemática, dada la magnitud que ha obtenido la calidad en la ingeniería de sistemas y en la ingeniería del software.

Políticas de Seguridad: Borghello[41] "es un grupo de obligaciones definidas por los responsables de un sistema, que señala en términos generales que está y que no está autorizado en el área de seguridad durante la ejecución general del sistema." Para la realización del proyecto se tendrán en cuenta definiciones relacionadas con vulnerabilidades, amenazas y riesgos, variables que deben ser considerados en los esquemas de seguridad. Teniendo en cuenta que si no se mitigan estos eventos que atentan directamente con los pilares de un sistema de seguridad como son: Disponibilidad, integridad y Confidencialidad[42].

La gestión de activos, está basada en la protección de los activos de información por medio de un inventario de identificación, que permite determinar su grado de valor y su clasificación en el interior de la organización, y el control de acceso como metodología de seguridad para tener el control al sistema de información, donde los privilegios o beneficios de algunos usuarios se fundamentan por tres directrices como lo es la identificación, autenticación y autorización.

La seguridad informática, como método que permite elaborar una serie de normas, mecanismos y procedimientos primordiales para obtener un sistema de información confiable y seguro para la obtención de los niveles de seguridad y confort en el tratamiento y protección de la información.

Como explica Aguilera en el libro de seguridad informática de la editorial Editex S.A por más medidas de seguridad que se apliquen siempre tenemos un margen de riesgo, es por esto que es necesario conocer muy bien el sistema, sus componentes, y posibles peligros para determinar las medidas que se pueden implementar para contrarrestarlos[43].

Disponibilidad, tiene que ver con el acceso a la información y procesos por parte del personal autorizado, cuando sea necesario. La característica y cualidad de un activo de estar disponible cuando lo requiera una persona, o proceso autorizado y la confiabilidad, tiene que ver con la accesibilidad del personal autorizado, la

41 BORGHELLO, Cristian. Políticas de Seguridad de la Información. [En linea]. 2009. [10 marzo 2018] disponible en: https://www.segu-info.com.ar/politicas/polseginf.htm

42 CARDONA A. Omar Darío EVALUACIÓN DE LA AMENAZA, LA VULNERABILIDAD Y EL RIESGO. "Elementos para el Ordenamiento y la Planeación del Desarrollo". [En linea]. 2009. [10 marzo 2018] disponible en: http://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

43 AGUILERA LOPEZ. Seguridad informática: Madrid: Editex, S.A, 2010. 240 p

integridad, de la información y procesos. Cabezas[44] determina disponibilidad como la facultad de salvaguardar la precisión e integridad de los activos.

El tema no repudio, es una forma de negar él envió de un mensaje o información que fue trasmitido, es una manera de demostrar que una información fue enviada por emisor o receptor este tipo de servicio criptográfico permite la realización de pruebas de integridad, autenticación y originalidad de los datos.

4.3 MARCO LEGAL

Cada día es más habitual escuchar sobre ataques informáticos en Colombia lo que perjudica la seguridad de la información en las organizaciones debido a esto es necesario saber, comprender y cumplir con la legislación relacionada con la seguridad informática.

Actualmente existen muchas leyes que rigen la seguridad de la información para las organizaciones de las cuales están condicionadas a cumplirlas según un marco legal aplicable a sus negocios, y de sus actividades en este caso para Energitel debe cumplir normas para garantizar la calidad de los servicios prestados. Si infringe la confidencialidad, integridad y disponibilidad de los datos de sus clientes pueden tener sanciones según la Ley 1581 del 2012 que reglamenta y regula el tratamiento y la protección de datos personales, para ello Energitel debe estar legalmente constituida.

Ley 23 de 1982[45]. Esta ley es básicamente sobre los derechos de autor, presenta toda la regulación correspondiente a los derechos de autor en Colombia. Ley 44 de 1993. Esta modifica la Ley 23 de 1982 y la ley 29 de 1944, se adicionan nuevas disposiciones como el soporte lógico (Software).

Ley 527 de 1999[46]. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Esta permite el uso de información o datos para el comercio electrónico, firmas digitales, mensajes de datos por medio

44 Cabezas, Ivan-Correa Martha. Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional – SIUN.2014. Página 1. [En linea]. 2009. [10 marzo 2018] disponible en:http://investigacion.unal.edu.co/fileadmin/recursos/docs/politicas/seguridad/siun_web_politicas_seguridad.pdf

1 Ibíd. Pág. 1

45 Legislación Informática de Colombia. [En linea] [01 de septiembre de 2018] disponible en: http://www.informatica-juridica.com/legislacion/colombia/

46 Legislación Informática de Colombia. [En linea] [01 de septiembre de 2018] disponible en: http://www.informatica-juridica.com/legislacion/colombia/

escrito y digital, también permite la certificación de las personas naturales y jurídicas para realizar transacciones electrónicas.

Ley 1266 de 2008. En la cual se dictan mandatos del hábeas data y se organiza la información el manejo de la misma que está incorporada en las bases de datos personales, en especial la financiera, crediticia, comercial de servicios y la proveniente de terceros países.

Ley 1581 de 2012[47]. Esta ley dicta disposición sobre la protección de datos personales. Esta ley tiene por objetivo fomentar el derecho constitucional que tienen todas las personas a saber, renovar y ajustar las aclaraciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

4.4 MARCO CONTEXTUAL.

ENERGITEL empresa especialista en el manejo integral de sus proyectos de ingeniería eléctrica, electrónica, telecomunicaciones y eficiencia energética. Tenemos óptima experiencia con el fin de atender requerimientos y necesidades en todo el territorio nacional, contamos con el conocimiento necesario para desarrollar soluciones acordes a sus proyectos.

Fue creada en el año 2015 en la ciudad de Ibagué, con un campo de acción inicialmente en los departamentos como el Tolima, Risaralda, Huila y Cundinamarca, al igual que en los diferentes municipios dentro de la periferia urbana y rural, dichos proyectos se han llevado a cabo con empresas de telecomunicaciones como Nesitelco, ETB, Claro, Movistar, Huawei, Telmacom, la parte eléctrica con Electrotodo, Enertolima, Obras y Diseños y Eléctricos Ibagué, aires acondicionados y transferencias con Seiclimatizar.

Organización poseedora del manejo integral eléctrico a nivel urbano y rural al igual que en las telecomunicaciones, se ha implementado nueva tecnología, materiales que cumplen con los estándares de calidad adaptando avances según requerimientos de los proveedores, basándonos en normas vigentes como (RETIE, Retilap, NTC 2050, 1409), para ofrecer soluciones a las necesidades de los clientes, difundiendo una política de buenas prácticas ambientales, trabajos seguros en procedimientos, vida saludable y salud ocupacional.

47 Legislación Informática de Colombia. [En linea] [01 de septiembre de 2018] disponible en: http://www.informatica-juridica.com/legislacion/colombia/

4.5 ESTADO ACTUAL.

Para desarrollar este proyecto tipo monografía se realiza un análisis de las vulnerabilidades existentes en el sistema informático de Energitel, por causa de los diferentes ataques que ha enfrentado la organización, los cuales han generado alarmas tempranas que con la ayuda de la metodología Magerit se pueden mitigar reduciendo el impacto ocasionado en la infraestructura de la red informática actual.

VELASCO[48], Lo que no cambia con el transcurrir de los años son las amenazas informáticas, estas son cada vez más complejas, difíciles de detectar y a pesar de los avances tecnológicos y mecanismos para contrarrestarlas, por eso es difícil hacerles frente debido a que hay nuevos métodos criptográficos utilizados para infiltrar malware ocultos en páginas web ejecutando procesos maliciosos en el sistema informático y bases de datos.

La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT[49], es un sistema para explorar los riesgos que conforman los sistemas de información, y para indicar las medidas correctas que deberían aprobarse para controlar estos riesgos.

PAE[50], Magerit de origen en el Consejo Superior de la Administración Electrónica, como un dictamen de la dependencia de las tecnologías de información actual, metodología de interés para sistemas de información como lo son los activos que tienen un valor muy alto dentro de las organizaciones, también para determinar y conocer el nivel de exposición en el que se encuentra y protegerlo.

Este documento investigativo propone metodologías de seguridad para proteger la información que se utiliza en un sistema informático, impulsando la realización de un análisis de riesgos con base en los recursos humanos, tecnológicos y administrativos con el propósito de conservar y garantizar la integridad, confidencialidad y disponibilidad de la información.

48 REDES ZONE. VELASCO. Rubén Qué nos deparará 2018 en cuanto a seguridad informática. [En linea]. 1 de enero de 2018. [10 abril 2018] disponible en: https://www.redeszone.net/2018/01/01/seguridad-informatica-2018/

49 Universidad de Murcia. Capítulo 5. IAGP 2005/06. Gestión de riesgos en ingeniería del software. 5.8 Magerit. [En linea]. [17 de junio de 2006] disponible en: http://www.um.es/docencia/barzana/IAGP/Iagp5.html

50 PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea], octubre de 2012 [06 abril de 2018] disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WszQP4jwbIU

5. METODOLÓGIA

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación formalizado para este proyecto es de fundamentación cuantitativa para medir los riesgos, amenazas y debilidades que pueden afectar el normal funcionamiento del sistema informático y bases de datos, por otra parte también estará orientada en la investigación descriptiva, porque se basa en la especificación de técnicas, procedimientos para la identificación de características que ayudan a procesar y analizar los datos de manera dinámica y eficaz orientada a observar y describir las vulnerabilidades del sistema informático existente en Energitel.

5.2 METODOLOGIA DE DESARROLLO

La monografía se basa en el análisis de la seguridad de la información, la cual se fundamenta en el manejo de la metodología Magerit como mecanismo para evaluar la seguridad del sistema informático existente brindando un diagnóstico de referencia respecto a las vulnerabilidades y riesgos evidenciados, para el cumplimiento de los objetivos del proyecto que justifique la generación de conclusiones y recomendaciones a partir del estudio de fuentes reales. La siguiente grafica describe y garantiza la efectividad de Magerit:

Figura 3 Magerit Fases

Fuente: Autor

Al concluir esta temática se procederá con la entrevista con el fin de verificar el grado de conocimientos del personal en las diferentes áreas para así minimizar las vulnerabilidades existentes y con la metodología Magerit mejorar la seguridad del sistema informático de Energitel teniendo en cuenta que con esta metodológica se actualizo el inventario de activos y también se logró detectar el nivel de riesgo y el tratamiento adecuado para contrarrestarlo. El anexo A correspondiente a la tabla 5 la cual refleja el inventario actual de los activos de Energitel[51].

La metodología Magerit puede ser la alternativa apropiada para constatar la seguridad del sistema informático existente, de esta forma determinar la vulnerabilidad para poder tomar medidas preventivas contra ataques futuros de la organización, también podemos verificar y evaluar la seguridad física y lógica de los sistemas de información para garantizar la seguridad informática y poder controlar el grado de acceso a todas las actividades maliciosas**.**

También se pueden apoyar en todo lo referente a seguridad de la información según la Norma NTC ISO27001:2013 que consiste en la conservación de su confidencialidad, integridad y disponibilidad dentro de cualquier organización. (Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. Compendio seguridad de la información, segunda edición 2015[52].

5.3 FUENTES Y TÉCNICAS DE RECOLECCION DE INFORMACIÓN

La fuente de información será por medio de visitas y contacto directo con las instalaciones de la empresa Energitel y con el personal del área de sistemas, también con ayuda de entrevistas y listas de chequeo se hará la recolección de la información para conocer el estado actual del sistema informático de la empresa. También se utilizará información obtenida de la búsqueda bibliográfica, artículos científicos, monografías, tesis, libros especializados, relacionados con el objeto de estudio y por medios de las metodologías Magerit y la misma ISO27001.

5.4 POBLACION Y MUESTRA

La población está conformada por todo el personal administrativo y operativo de Energitel y la muestra será tomada en cuenta de diferentes áreas y procesos que

51 ANEXO A. INVENTARIO DE ACTIVOS ENERGITEL

52 MINTIC. Controles de seguridad de la información. [En línea]. [10 mayo 2017], disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

manejan gran cantidad de información contenida en las bases de datos y que es de carácter confidencial.

6. VULNERABILIDADES Y RIESGOS DE ENERGITEL

Una forma óptima de realizar la evaluación es seguir una metodología, que defina unos pasos ordenados de forma concreta para la consecución de los dos objetivos específicos propuestos en esta monografía, evitando que durante el proceso no se obvien aspectos importantes de seguridad. Un paso significativo para implementar la seguridad de la información en la organización es elaborar la localización de las vulnerabilidades y riesgos a los cuales se enfrentan los activos de la organización, para tener la convicción y la probabilidad de que estas amenazas no se materialicen[53].

Metasploit permite realizar escaneo de forma fácil de las vulnerabilidades del sistema informático atacando puertos que pueden tener acceso a información confidencial, El anexo B evidencia las pruebas realizadas en algunos dispositivos de Energitel[54]. Al no tener dominadas estas amenazas se pueden convertir en realidad a través de fallas de seguridad, estas deben ser eliminadas al máximo y en línea. Con una buena gestión de riesgos se logrará identificar, dominar, reducir y eliminar las amenazas que afectan el normal funcionamiento de la organización.

Según Tarazona[55] la debilidad que permite que los usuarios sean atacados y víctimas de la gran cantidad de amenazas que los vigilan, radica en que hay muchos casos no se está tramitando la tecnología dentro de un marco completo de protección de la información, y en la falta de concientización a las personas en los riesgos relacionados con el uso de tecnología y de herramientas como internet, por lo que los esfuerzos se pierden o se orientan a cumplir objetivos imprecisos.

Las inversiones en tecnología de seguridad, como solución a los problemas planteados, deben ser realizadas dentro de un marco sincronizado con otra serie de medidas para formar lo que se conoce como un “Sistema de Gestión de Seguridad de la Información”

6.1 PRUEBAS Y EVIDENCIAS

Teniendo completo conocimiento de las vulnerabilidades y amenazas del sistema informático de Energitel se determinó realizar la tabla 1 para definir e identificar las

53 Sosa. Johana. Análisis de Riesgos. [En línea]. [27 enero 2012], disponible en:http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

54 ANEXO B. PRUEBAS DE VULNERABILIDAD DE PUERTOS

55 TARAZONA T. César H. AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. file:///D:/Users/Usuario/Downloads/965-3375-2-PB%20(1).pdf. Pág. 141.

falencias que aquejan la organización y de esta forma realizar un consolidado a modo de evidencias para poder dar un tratamiento adecuado.

Tabla 1 Vulnerabilidades y Amenazas

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
HARDWARE	Sensibilidad: Humedad, polvo.	Polvo, corrosión
	Sensibilidad: Radiación electromagnética	Radiación electromagnética
	Variación de voltaje	Perdida suministro de energía
	Variaciones de temperaturas	Fenómenos meteorológicos
	copias no controladas	Hurtos, medios y documentos
SOFTWARE	Ausencio o insuficiencia de pruebas de software	Abuso de derechos
	Utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error de uso
	Fechas incorrectas	Error de uso
	Ausencia de mecanismos de autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas sin proteger	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos

Tabla 1. (Continuación)

TIPO DE ACTIVO	VULNERABILIDADES	AMENAZAS
	Descarga y uso no controlado de software	Manipulación de software
	Líneas de comunicación sin proteger	Escucha encubierta
PERSONAL	Entrenamiento insuficiente en seguridad	Error de uso
	Falta de conciencia acerca de la seguridad	Error de uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo no supervisado del personal externo	Hurtos, medios y documentos
	Ausencia de políticas para el uso correcto de los medios	Uso no autorizado del equipo
ORGANIZACIÓN	Ausencia de procedimiento para el registro y retiro de usuarios	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Falta de mantenimiento del SI
	Ausencia de planes de contingencia	Falla del equipo
	Ausencia de registros de bitácoras	Error de uso

Fuente. Guía de gestión de riesgos. Guía 7. MINTIC[56]

56 Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía de gestión de riesgos. Guía 7. [En línea]. [10 agosto 2017], disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Magerit juega papel fundamental en el tratamiento que se debe dar a las amenazas, en la siguiente tabla se logró identificar que la metodología de análisis y gestión de riesgos a utilizar es un mecanismo que permite evaluar la seguridad del sistema informático existente brindando un diagnóstico de referencia claro respecto a las vulnerabilidades y riesgos evidenciados, permitido establecer soluciones en el área de almacenamiento de información.

Las amenazas plasmadas en la tabla 2 reflejan las debilidades del sistema informático de Energitel, de igual manera también podemos determinar la falta de controles en la accesibilidad y la poca eficiencia de las políticas existentes frente a los diferentes ataques informáticos.

Tabla 2 Amenazas Energitel

ITEM	AMENAZAS	DESCRIPCION
1	No tiene contraseñas seguras	En el último mantenimiento realizado el mes de agosto se detectó que de 10 equipos solo hay 2 que tienen contraseñas confiables comprobándose que un 80% de los trabajadores no emplean contraseñas seguras lo cual puede ocasionar robo o pérdida de información (crimen informático) como el ocurrido el año 2016 cuando uno de los empleados saco información del equipo portátil del supervisor de zona repercutiendo en la pérdida de un contrato de redes de MT del conjunto las Juanas el cual fue ejecutado por el proveedor de servicio Electrotodo de la competencia.
2	Antivirus desactualizados	En los 10 equipos de cómputo tipo escritorio de los empleados se evidencio que 3 de ellos presentaron fallas protección contra virus informáticos, los cuales tuvieron pérdida y daño de información del 30% referente a datos confidenciales de socios de la compañía.
3	No se tienen copias de seguridad y procedimiento de backup	Daño de disco duro del equipo Samsung core i3 Windows 7, del ingeniero residente de obra ocasionando pérdida total del 100% de la información respecto a informes de mes de avance de obras, contratos, propuestas de mantenimiento, rutinas y procedimientos de actividades.
4	Fluctuaciones de energía en el sistema de distribución y protección	Esta vulnerabilidad física produjo perdida de información en un 15% de los equipos referente a licitaciones de contratos tercerizados afectando la seguridad de la información y principalmente la confidencialidad de la misma.

Tabla 2. (Continuación)

ITEM	AMENAZAS	DESCRIPCION
5	Abuso de privilegios	Se detectó que 3 de los 15 empleados para un total del 20% tienen privilegios de acceso al sistema informático los cuales han suministrar información confidencial a clientes y socios.
6	Pérdida y fuga de información confidencial	Pérdida de un contrato de redes de MT conjunto las Juanas e información de proyecto Verde Menta para diseño eléctrico, daño de información referente a datos confidenciales de socios de la compañía).
7	Pérdidas económicas	No ejecución de contratos.
8	Daños en hardware	Daño del disco duro del equipo Samsung Core i3 Windows 7.
9	Caída de red de energía y servidor fuera de servicio	Perdida de información en equipos de trabajadores del área de ATC, atención al cliente.
10	Pérdida de credibilidad	Pérdida de confianza de los socios y usuarios.

Fuente: El Autor

6.1.1 Cumplimiento de Objetivos específicos.

1. Verificar que activos en lo concerniente a sistemas de información TI de Energitel son vulnerables y pasan a fase de riesgos.

Dando paso al objetivo número uno se realiza la verificación y análisis de los activos vulnerables que pasan a la fase riesgo catalogados en la siguiente tabla 3 la cual permite conocer las vulnerabilidades, amenazas y riesgos que enfrenta Energitel determinando que para la seguridad de la información la protección de los activos frente a un nivel alto de amenazas brinda el poder de garantizar la continuidad del negocio, minimizando el riesgo y maximizando el retorno de las inversiones.

Magerit, metodología sistemática que analiza los riesgos derivados del uso de las TI permitiendo saber el valor real que está en juego de cada activo y cómo la empresa puede protegerlos, ayudando a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Tabla 3 Consolidado de las vulnerabilidades, amenazas y riesgos

Activos de Información	Vulnerabilidades	Amenazas	Impacto	Riesgos
Documentación y Archivos	Deterioro	Polvo, corrosión	Archivos y documentación ilegible	Perdida de documentación con información valiosa (contratos, HV, Procedimientos, Facturas y demás).
	No existencia de copias de seguridad	Pérdida o destrucción de información.	Destrucción de información física	Pérdida total de la información
Activos de Software y Hardware	Vulnerabilidades	Amenazas	Impacto	Riesgos
Programas y discos duros	Versiones obsoletas, licencias vencidas, Descarga y uso no controlado de software y falta de mantenimiento	Programas vencidos, posibles ataques, manipulación de software y Polvo, corrosión	Fallas en Software y equipos, alteración de información o pérdida y daños en sistemas.	Retrasó de actividades, pérdida de tiempo y de información

Tabla 3. (Continuación)

Activos de Información	Vulnerabilidades	Amenazas	Impacto	Riesgos
Activos Físicos	Vulnerabilidades	Amenazas	Impacto	Riesgos
PCs	Limitado mantenimiento preventivo y disminución de ciclo de vida	Deterioro de los componentes de hardware	Fallas en hardware	Perdida de PC e información.
Activo Establecimiento	Vulnerabilidades	Amenazas	Impacto	Riesgos
Oficina	Deterioro y falta de control de acceso a personal no autorizado	Humedad, deterioros e ingreso de personal no autorizado	Destrucción de la infraestructura física y Robos o daños	Retraso en actividades y pérdida de información.
Activos de Servicios	Vulnerabilidades	Amenazas	Impacto	Riesgos
Paginas y plataforma	Programación desactualizada y fallas de configuración de servicios	Hacking y Ataques	Alteración de la información y parada en servicios	Destrucción de datos e información y retrasos en actividades
Activos Servicio de Electricidad	Vulnerabilidades	Amenazas	Impacto	Riesgos
Instalación y protecciones eléctricas	Fluctuaciones y fallas en fluido eléctrico	Variaciones de voltajes, cortos de energía e inestabilidad en el servicio y continuidad	Fallas o pérdidas de equipos	Perdidas monetarias e información
Activos de Personal	Vulnerabilidades	Amenazas	Impacto	Riesgos
Personal	Permisos no controlados por Accesibilidad, falta de capacitación en manejos de TI	Ataques por personal interno Ingeniería social, accesos no controlados en BD y Privilegios no autorizados	Acceso y robo de información no autorizada	Alteraciones informáticas, robo de información y reprocesos

Fuente: El Autor

Las siguientes imágenes evidencian y representan los diferentes activos informáticos que están en la fase de riesgo clasificados y valorarlos según las cinco dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Figura 4 Puesto de trabajo oficina del Coordinador de Proyecto

Fuente. El Autor

Puesto de trabajo del director de proyectos el cual tiene un equipo computador tipo portátil con sistema operativo Windows 10, punto de conexión eléctrica regulada, cableado estructurado, con la plataforma de seguimiento de actividades SISE de control operativo, se observa conexión por BT y cableado de red de datos o comunicaciones a la vista, el cual es vulnerable a posibles ataques teniendo en cuenta que la información que maneja es confidencial y bastante importante para Energitel debido a que su clave de acceso no es confiable.

Figura 5. Puestos de trabajo Departamento Técnico

Fuente. El Autor

Puestos de trabajo de las ingenieras los cuales poseen equipos computador todo en uno con sistema operativo Windows 10, punto de conexión eléctrica regulada, cableado estructurado, telefonía IP, con la novedad de que todo el personal pasa por el lado de estos puestos los cuales son vulnerables a posibles ataques y teniendo en cuenta que la información que manejan es confidencial y bastante importante para Energitel.

Figura 6. Archivo documental central

Fuente. El Autor

En esta oficina se encuentra organizada, detallada y ordenada toda la documentación referente al personal, contratación, propuestas, proyectos, procedimientos y demás documentos necesarios para la operativa de la organización Energitel, en esta oficina no se ejerce un control de ingreso al igual que el acceso a la información.

De acuerdo con Javier Fombona[57] la oportuna gestión de recursos informáticos se encadena con una organización eficiente de las instituciones y una mejor satisfacción de las personas. Estas tecnologías restringen el rendimiento en las tareas y su normal desajuste o mal funcionamiento deteriora los resultados y las relaciones internas y externas de la entidad y sus miembros.

57 FOMBONA. Javier. Revista Iberoamericana CTS. Centro de Estudios sobre Ciencia, Desarrollo y Educación Superior (Centro REDES) Mansilla 2698, 2º piso - Ciudad Autónoma de Buenos Aires, Argentina. [En línea]. [10 agosto 2017], disponible en: http://www.revistacts.net/volumen-11-numero-32/316-articulos/726-los-problemas-de-los-recursos-informaticos-en-el-contexto-universitario

2. Determinar las causas de los riesgos potenciales a los que está expuesta la organización en cuanto a la tecnología que posee.

Para dar respuesta al objetivo número dos se implementa la metodología Magerit para la determinación de los riesgos potenciales de la organización según los recursos afectados y analizados por causa que origina cada uno de los riesgos encontrados. La presente tabla 4 brinda la posibilidad de diagnosticar la metodología para identificar, clasificar los tipos de activos de información, valorando y realizando el tratamiento de riesgos potenciales evidenciados.

Tabla 4. Riesgos Potenciales Por Causa

TIPO DE ACTIVO	RIESGO	CAUSAS QUE ORIGINAN LOS RIESGOS ENCONTRADOS	ACTIVO AFECTADO
1. [D]DATOS / INFORMACION	Fuga de información	Incumplimiento en políticas de acceso a la información. Falla en los controles de seguridad para el manejo de información.	[BACKUP] COPIAS DE RESPALDO. [KEYS] CLAVES CRIPTOGRAFICAS. [CRE_ACC] CREDENCIALES DE ACCESO. [DAT_CON_ACC] DATOS DE CONTROL DE ACCESO. [LOG] REGISTRO DE ACTIVIDAD. [SER_BD] SERVIDOR DE BASE DE DATOS.
	Robo Información	Falta de capacitación del personal. Falta de toma de conciencia y de ética profesional de los trabajadores respecto al manejo de la información.	
2. [S]SERVICIOS	Caída o falla en el servicio de internet	Caída de red de energía y servidor fuera de servicio. Fallas por parte del proveedor de servicio red local, hardware o servidor.	[BACKUP] COPIAS DE RESPALDO. [SER_BD] SERVIDOR DE BASE DE DATOS. [SER_WWW] SERVIDOR PORTAL WEB [SER_INTRANET] SERVIDOR INTRANET [SER_EMAIL] SERVIDOR CORREO ELECTRONICO [SER_ARCHIVOS] SERVIDOR DE ARCHIVOS

Tabla 4. (Continuación)

TIPO DE ACTIVO	RIESGO	CAUSAS QUE ORIGINAN LOS RIESGOS ENCONTRADOS	ACTIVO AFECTADO
3. [SW] SOFTWARE - APLICACIONES INFORMÁTICAS	Abuso de privilegios de acceso	Acceso a los sistemas de información por personas no autorizadas.	[SER_WWW] SERVIDOR PORTAL WEB [SER_INTRANET] SERVIDOR INTRANET [SER_EMAIL] SERVIDOR CORREO ELECTRONICO [SER_ARCHIVOS] SERVIDOR DE ARCHIVOS [SER_BD] SERVIDOR DE BASE DE DATOS [OFF]OFIMÁTICA [AV]ANTIVIRUS [SO]SISTEMA OPERATIVO [BACKUP] COPIAS DE RESPALDO [MAN] RED METROPOLITANA
	Corte de la red de Eléctrica Regulada	Perdidas de Información y fallas en hardware	
	Virus	Pérdida de información confidencial por problemas de antivirus (inestabilidad del sistema).	
4. [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)	Deterioro de hardware	Incumplimiento al cronograma de mantenimiento de los equipos de cómputo. Errores de mantenimiento/actualización de equipos Debió al polvo, suciedad y demás.	[SER] SERVIDORES [PC] EQUIPOS DE COMPUTO [SWI] SWITCH [AP] PUNTOS DE ACCESO [FIREWALL] FIREWALL [IMP] IMPRESORA [ESC] ESCANER [GEN_ELE] GENERADORES ELÉCTRICOS INSTALACIONES
	Virus	Trasmisión y propagación de virus informático	
5. [COM] REDES DE COMUNICACIONES	Perdida de información	Por acceso no autorizado y contraseñas seguras. Archivo documental central: no se ejerce un control de ingreso al igual que el acceso a la información en las BD.	[MAN] RED METROPOLITANA [INTERNET] INTERNET [BACKUP] COPIAS DE RESPALDO [SER_BD] SERVIDOR DE BASE DE DATOS

Tabla 4. (Continuación)

TIPO DE ACTIVO	RIESGO	CAUSAS QUE ORIGINAN LOS RIESGOS ENCONTRADOS	ACTIVO AFECTADO
6. [L] INSTALACIONES	Falla en el servicio de energía	Corte del suministro eléctrico, no cuentan con un sistema de protección contra rayos, fluctuaciones de energía en el sistema de distribución y protección.	[SER] SERVIDORES [FIREWALL] FIREWALL [GEN_ELE] GENERADORES ELÉCTRICOS INSTALACIONES [EDIFICIO] EDIFICIO
	Desastres Naturales	Daños causados por acción de la naturaleza en las instalaciones físicas de la entidad (Bodega Energitel)	
7. [P] PERSONAL	Fuga de información	Perdida de confidencialidad del personal de custodia de la información.	[BACKUP] COPIAS DE RESPALDO [SW_FOREST] SISTEMA DE AUTOMATIZACION DE PROCESOS Y DOCUMENTOS [SER_BD] SERVIDOR DE BASE DE DATOS
	Falta de Personal Capacitado	Falta de personal con competencias.	

Fuente: El Autor

3. Establecer procedimientos para identificar y mitigar las vulnerabilidades y riesgos evidenciados.

Para dar respuesta a este objetivo número 3 Magerit propone dos pasos fundamentales los cuales son el análisis de riesgo, el cual es una técnica para determinar los riesgos y la gestión de riesgos que decide qué hacer con los riesgos e impactos generados y definidos.

Procedimientos para el análisis de riesgo:

- Especificar a qué amenazas se enfrentan los activos.
- Definir con cuáles salvaguardas se cuenta y si son efectivas ante el riesgo.
- Valorar el impacto, sabiendo el daño sobre el activo originado por la materialización de la amenaza.
- Valorar el riesgo, sabiendo el impacto real con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Procedimientos para la gestión de riesgo:

- Definición de los valores de impacto y riesgo residual.
- Elección de salvaguardas.
- Estudio de pérdidas y ganancias.
- Apoyo por parte de la dirección de la empresa.
- Verificación de los activos de la empresa.

4. Descubrir estrategias de seguridad para la protección de la información y así disminuir el riesgo de ataques en cuanto al manejo de la información de Energitel.

Para dar cumplimiento al objetivo número cuatro se debe implementar métodos o técnicas que permitan evidenciar y contrarrestar las vulnerabilidades y riesgos que afectan los activos de la organización como:

- Seguridad física que permita la protección del entorno informático brindando obstáculos frente a un ataque y procedimientos de control eficaces.
- Seguridad lógica de la información respecto al software y actualizaciones.
- Autenticación de usuarios.
- Administración de usuarios y contraseñas.
- Implementación de contraseñas robustas.

- Administración de puertos y servicios activos que hacen vulnerable el sistema informático.
- Formulación de políticas de seguridad y análisis de vulnerabilidades.

La empresa H.S Energitel sufrió ataque a su sistema informático en el departamento de TI, por falta de controles e incumplimiento a sus políticas de seguridad de la información, debido a la vulnerabilidad o debilidad en la implementación de sus contraseñas de acceso en sus dispositivos.

- Utilizar y cambiar periódicamente las contraseñas.
- Maximizar el control de acceso a sus datos.
- Revisar la política de control de acceso para los empleados.
- Controlar de manera adecuada los cambios en plataformas y sistemas de información.
- Reducir los errores operativos.
- Realizar controles en la red.
- Verificar copias de seguridad.
- Imponer cumplimiento de normas.
- Realizar análisis de resultados y control de actividades sospechosas.
- Capacitar al personal respecto al buen uso de la información de la organización.

David A. Franco[58] afirma que los activos que se encontraron como críticos son los que definitivamente se entregaran a evaluación en esta última fase, en la que se procede a la utilización de un escáner de vulnerabilidades. Este tiene como objetivo identificar los potenciales riesgos al que están expuestos los equipos escogidos, debido a que estos juegan el rol más crítico para la red objetivo. Berzosa[59] Las contraseñas desarrollan una seguridad contra los usuarios no autorizados, el sistema de seguridad solo puede ratificar que la contraseña es apta, y si no el usuario está autorizado a utilizar esa contraseña.

Fileadmin[60] define que para contraseñas de cuentas de usuario de bases de datos: deben ser distintas para cada una y regirse a las políticas de confiabilidad y cambio

58 David A. Franco, Jorge L (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. [En línea]. [10 agosto 2017], disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

59 Ecured (2017). Luis Rodríguez Berzosa. Control de acceso. [En línea]. [10 agosto 2017], disponible en: https://www.ecured.cu/Control_de_acceso

60 Fileadmin. Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional – SIUN. Recuperado el día 03 de julio de 2017 de http://investigacion.unal.edu.co/fileadmin/recursos/docs/politicas/seguridad/siun_web_politicas_seguridad.pdf

de contraseñas. Estas deben ser robustas para evitar que sean identificadas y así maximizar la seguridad en cuestiones de acceso.

8. RESULTADOS E IMPACTOS

Para las pruebas realizadas al sistema informático de Energitel se aplicó la metodología Magerit que ofrece un método para analizar los riesgos descubriendo y planificando las medidas necesarias para mantener los riesgos bajo control en un contexto de efectividad que se transmite en ganancias para la organización:

8.1 IMPORTANCIA DE IMPLEMENTAR LA METODOLOGÍA MAGERIT EN LA ORGANIZACION

Para la implementación de Magerit siempre se debe cumplir ciertos pasos fundamentales, lo que posibilitaría saber cuánto valor está en juego, como preservarlo determinando el riesgo al que están sometidos los elementos de trabajo para así poder gestionarlos. Jaime Barrios Cantillo[61], brinda un paso a paso respecto al análisis de riesgos como una actividad que sirve para limitar el riesgo a través de unos pasos secuenciales:

1. identificar los activos relevantes para la compañía, su interrelación y su valor, en el sentido en que afectaría su degeneración.
2. determinar a qué amenazas están expuestos aquellos activos
3. Constituir qué medidas preventivas hay habilitadas y que tan efectivas son respecto al riesgo.
4. medir el impacto, definido como la afectación causada sobre el activo generado por la materialización de la amenaza
5. medir el riesgo, reconocido como el impacto ponderado con la probabilidad de materialización de la amenaza.

De acuerdo al autor Jaime Barrios, el cual brinda información respecto al análisis de riesgos los cuales podrán determinar en la tabla de inventario de activos de Energitel según Magerit donde los resultados obtenidos permiten identificar el proceso y el responsable de cada activo, para ello es muy importante que la organización implemente un sistema que proteja la información, controlando que los intrusos no causen y afecten los recursos de la empresa teniendo en cuenta que los obstáculos principales son la falta de cultura en seguridad informática y la poca inversión en ella.

61 BARRIOS CANTILLO. Jaime (2017). Pasos para el análisis de riesgos basados en MAGERIT. [En línea], 11 de febrero de 2017 [revisado 13 mayo de 2018] disponible en: https://es.slideshare.net/jaimeral73/pasos-para-el-anlisis-de-riesgos-basados-en-magerit

8.2 ESTIMACIÓN DEL IMPACTO

El primer dato notificado es el “Nivel del activo” valorado cuantitativa y/o cualitativamente. El segundo dato pertinente para la valoración del impacto es la “Degradación”, el cual nos indica que tan perjudicado resulta el [valor del] activo de información (1%, 50%, 100%), como producto de la materialización de las amenazas[62]

90% a 100%: Degradación muy considerable del activo
25% a 89%: Degradación medianamente considerable del activo
1% a 24%: Degradación poco considerable del activo

La tabla 5 de valoración del activo, nos indica los impactos generados por los riesgos que se pueden calcular por cada activo, por cada amenaza y por cada dimensión de valoración, en función del valor acumulado y de la degradación causada[63]

Tabla 5 Valoración del Activo

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal
ETI HW03	Servidor Web Físico 1	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Jefe de sistemas

62 SOLARTE SOLARTE. Francisco Nicolás. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BAJO LA NORMA ISO 27001 Y 27002. 5.3.3 ESTIMACIÓN DEL IMPACTO. Recuperado el día 6 de JULIO de 2016. disponible en: http://sgsipractico.blogspot.com/2016/07/estimacion-del-impacto.html

63 SOSA. Johana. Análisis de Riesgos. Estándares para la administración de riesgos. Recuperado el día 27 de enero de 2012. disponible en: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf.Pag.41.

Tabla 5. (Continuación)

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal
ETI HW04	Servidor Web Físico 2	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Analista de sistemas 1
ETI HW06	Servidores Web Lógico 1	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Aux. de sistemas
ETI HW07	Servidores Web Lógico 2	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Analista de sistemas 2
ETI HW17	Computadores escritorio 7	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Jefe de Comunicaciones
ETI HW18	Computadores escritorio 8	1	HW	Confidencial	Sensible	Alta	Muy Alto	5	Aux. de Comunicaciones

Tabla 5. (Continuación)

ID	ACTIVO	CANT	TIPO ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal
ETIS1	Información al cliente	1	S	Confidencial	Normal	Media Baja	Medio	3	Jefe Comercial
ETIS2	Conexión a la base de datos	1	S	Confidencial	Sensible	Alta	Alto	5	Supervisor de sistemas
ESI01	Portafolio de servicios	1	SI	Uso Público	Baja	Baja	Muy Bajo	1	Subgerente Comercial
ETIS3	Correo Electrónico	1	S	Uso Interno	Sensible	Alta	Muy Alto	5	Analista de sistemas 1

Fuente. El Autor

En la tabla 6 se determina la probabilidad de que una vulnerabilidad potencial pueda suceder por una fuente de amenaza puede ser definida como alto, medio o bajo[64].

Tabla 6. Valor del Impacto

IMPACTO		Degradación		
		1%	50%	100%
Valor del activo	Muy Alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente. El Autor

Desastroso (8): Impacta fuertemente en la operatividad de los procesos. Mayor (5): Impacta en la operatividad de los procesos.

Moderado (3): Impacta en la operatividad del macro proceso. Menor (2): Impacta en la operatividad del proceso.

Insignificante (1): Impacta levemente en la operatividad del proceso

8.3 ESTIMACIÓN DEL R IESGO

Este valor se obtiene como resultado de la siguiente fórmula:

Riesgo (R)= Probabilidad (F) x Impacto

64 SOSA. Johana. Análisis de Riesgos. Estándares para la administración de riesgos. Recuperado el día 27 de enero de 2012. disponible en: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf.Pag.14.

La siguiente tabla 7 evidencia los resultados del análisis de riesgos realizado, esta posibilita a la organización tomar decisiones reales sobre las amenazas que se consideren primero dependiendo de la gravedad de las mismas, la probabilidad de que se presente, y que valor representa la perdida si se materializa.

Tabla 7. Riesgo (R)= Probabilidad (F) x Impacto

Activo TI		Servidores Web Físicos y Lógicos						
Administrador		Administrador de Sistemas						
Impacto		8	Desastroso					
Tipo activo		Equipos informáticos						
Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
						2.66	Tolerable	
				Frecuencia (F)		R	NR	
Desastres naturales	N1	Fuego	Se posee dos extintores uno de solkaflam y uno multipropósito, se tiene matriz de riesgos para equipos eléctricos en caso de incendios.	Muy baja	2	16	4	Extremo

Tabla 7. (Continuación)

Activo TI		Servidores Web Físicos y Lógicos						
De origen industrial	I*	Desastres industriales	No existe sistema de alarma de control de temperatura y humedad. No hay sistema de protección contra rayos.	Muy baja	2	16	4	Extremo
	I6	Corte del suministro eléctrico	No cuentan con un sistema de protección contra rayos. Fluctuaciones de energía en el sistema de distribución y protección. Caída de red de energía y servidor fuera de servicio.	Baja	3	24	4	Extremo
	I7	Condiciones inadecuadas de temperatura o humedad	No existe sistema de detección de alarmas de control de temperatura y humedad.	Baja	3	24	4	Extremo

Tabla 7. (Continuación)

Activo TI		Servidores Web Físicos y Lógicos						
E	E2	Errores del administrador	Falta de conocimiento del administrador.	Muy baja	2	16	4	Extremo
	E14	Escapes de información.	Pérdida de información confidencial por problemas de antivirus.	Baja	3	24	4	Extremo
	E19	Fugas de información.	Fuga de información confidencial por ciertos empleados.	Baja	3	24	4	Extremo
	E23	Errores de mantenimiento/ actualización de equipos	Antivirus desactualizados por malos procedimientos en mantenimientos.	Baja	3	24	4	Extremo
Ataques intencionados	A6	Abuso de privilegios de acceso	UPS y Tablero de Control: El acceso para el área técnica no tiene sistema de seguridad y control de acceso, solo una llave de la puerta principal que maneja el área técnica y de operaciones.	Baja	3	24	4	Extremo

Fuente. El Autor

Esta tabla 8 determina los efectos negativos del resultado al punto de potencializarse una amenaza.

Tabla 8. El valor NR (Nivel de Riesgo) obedece al Mapa de Riesgos

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	5	8
		1	2	3	5	8
				Impacto		

Fuente. El Autor

Tabla 9. Nivel de Riesgo

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente. El Autor

Apoyándonos en la función promedio se obtiene el Nivel de Riesgo total del activo de información, que para el Servidor es de 4, es decir, extremo y por lo tanto se requiere de atención inmediata y monitoreo permanente[65].

65 SOLARTE SOLARTE. Francisco Nicolás. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BAJO LA NORMA ISO 27001 Y 27002. 5.3.5 ESTIMACIÓN DEL RIESGO. Recuperado el día 6 de JULIO de 2016. disponible en: http://sgsipractico.blogspot.com/2016/07/estimacion-del-impacto.html

8.4 EVALUACIÓN DE RIESGOS

Para cada activo de información, el proceso concluye si el Nivel de Riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles necesarios.

Tabla 10. Tratamiento del Riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Finaliza el proceso.
Tolerable	Una de las tres opciones:
	a. Se transfiere el riesgo por ejemplo tomando un seguro.
Intolerable	b. Se evita el riesgo retirando el activo de información.
Extremo	c. Se reduce o mitiga el riesgo por medio de controles.

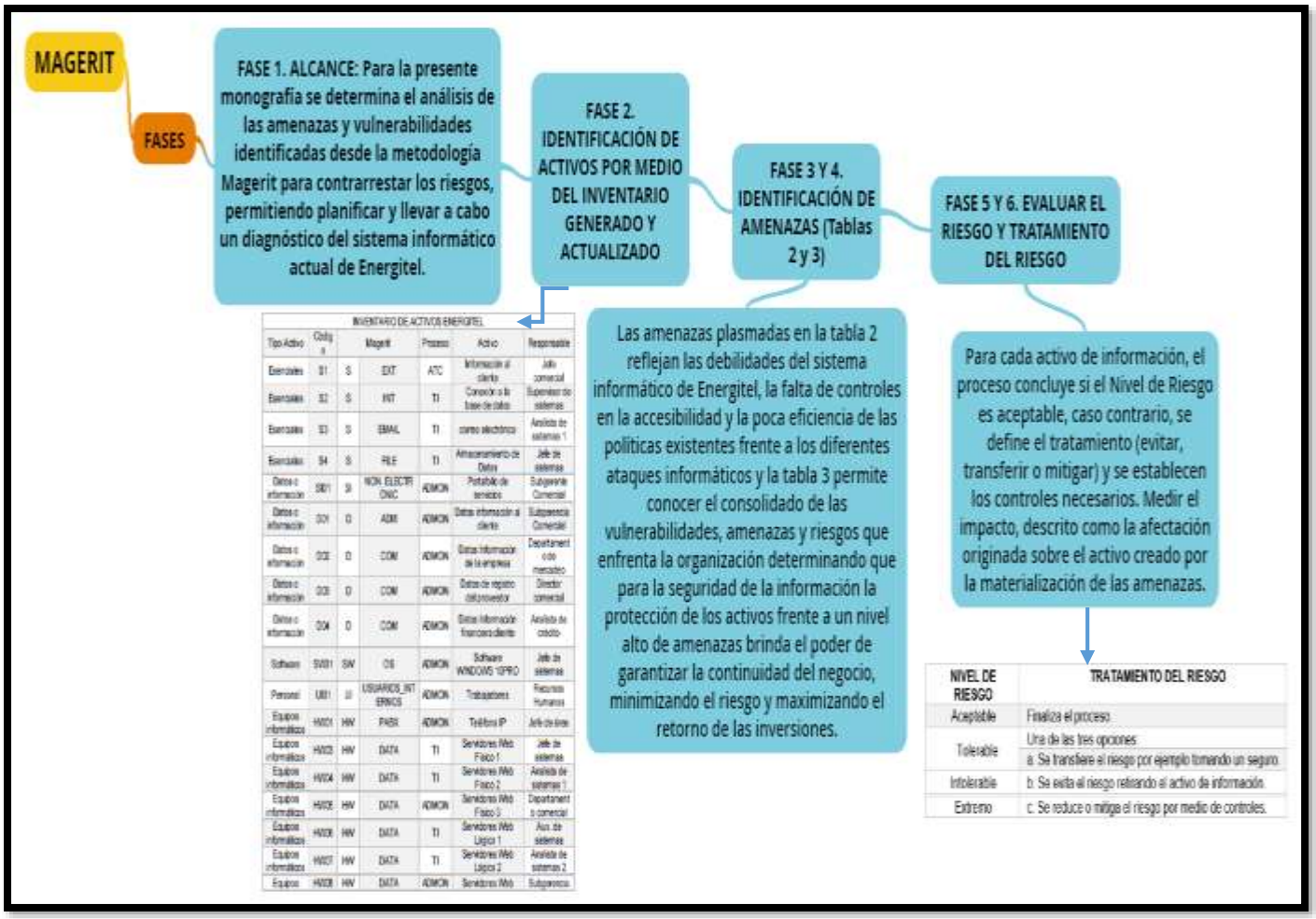
Fuente. El Autor

Para los servidores físicos y lógicos de Energitel el Nivel de Riesgo es extremo, se hace necesario definir el tratamiento a seguir, se descarta la opción de evitar el riesgo, porque este es un activo con un valor Muy Alto por lo cual no se puede eliminar debido a que presta muchos servicios esenciales para la organización[66].

La opción de transferir el riesgo no se recomienda por los altos costos de inversión, lo aconsejable es la implementación de nuevos controles de tipo preventivo o correctivo que minimicen el impacto de los riesgos y así pasar de un nivel extremo a tolerable o aceptable.

66 SOLARTE SOLARTE. Francisco Nicolás. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BAJO LA NORMA ISO 27001 Y 27002. EVALUACIÓN DE RIESGOS. Recuperado el día 6 de JULIO de 2016. disponible en: http://sgsipractico.blogspot.com/2016/07/estimacion-del-impacto.html

Figura 7 Proceso de Metodología Magerit Implementado



Fuente. El Autor

9. DIVULGACIÓN

Este proyecto se dará a conocer a todo el personal de Energitel y a la Universidad Nacional Abierta y a Distancia Unad, con el propósito de que sepan cuáles fueron los resultados obtenidos respecto al estado actual de su sistema informático y que con la metodología Magerit se evidencio los activos críticos y el impacto que genero su afectación.

El proyecto brinda oportunidades a las organizaciones para que de alguna manera logren identificar las vulnerabilidades y riesgos que enfrentan sus activos informáticos, bases de datos y sistemas de información. Hay que tener en cuenta que los ataques cibernéticos implementan técnicas letales para hacer daño y someter a sus víctimas, por esta razón es fundamental orientar de forma precisa y oportuna a las organizaciones para que estos ataques informáticos no se materialicen y ocasionen pérdidas monetarias considerables.

El actual proyecto es puesto en conocimiento y a disposición de la Universidad Nacional Abierta y a Distancia “Unad”, con el ánimo de contribuir en el fortalecimiento para la adquisición, trasferencia de conocimientos y consulta tanto pública y privada de toda la comunidad estudiantil, de las organizaciones, entidades, instituciones y empresas, para que tengan un claro conocimiento sobre la temática y metodología implementada a la hora de salvaguardar y proteger un sistema informático minimizando el impacto generado por los ataques cibernéticos haciendo que las políticas de seguridad sean más efectivas.

RECOMENDACIONES

Se sugiere a Energitel implementar controles o precisarlos para la consecución de sus objetivos minimizando en gran parte los impactos que generan los delitos informáticos, concientizándose de la existencia de riesgos y la necesidad de tramitarlos por medio de un método seguro para avalar que el sistema de información no sea vulnerable a las diferentes amenazas o ataques ocasionados por los delitos informáticos.

Promover la capacitación del personal de Energitel sobre el buen uso de la información, las TI y la normatividad legal vigente referente a estándares de seguridad, para reducir las debilidades en su sistema informático permitiendo la integridad y disponibilidad de la misma manteniendo un control sobre sus activos evitando su perdida y manipulación.

Se recomienda a la organización se validen los niveles de riesgo según la clasificación y el valor del activo determinado por la metodología de análisis y gestión de riesgos Magerit, para que de esta manera sea más fácil identificar las amenazas y vulnerabilidades permitiendo generar controles eficaces que garanticen confianza a la hora de proteger la información.

CONCLUSIONES

Una vez revisado el sistema informático de Energitel y culminado el análisis de los resultados respecto a las pruebas de seguridad, se pudo deducir que el objeto de estudio de la monografía ha sido cumplido, debido a que se encontraron las pruebas suficientes para evidenciar las amenazas, vulnerabilidades y riesgos que afectaron el sistema informático de la compañía por causa de los diferentes ataques que enfrento dando como resultado perdidas de información valiosa y a su vez perdidas monetarias.

Con el análisis del estado actual de la seguridad informática de Energitel se pretende suministrar un diagnostico general sobre la importancia y medidas necesarias para proteger el activo de la información, teniendo en cuenta los diferentes ataques informáticos los cuales son cada vez más efectivos y organizados, por lo cual se requiere estar actualizado según el avance tecnológico en temas de seguridad.

Energitel con la metodología Magerit, identifico la forma precisa de mitigar el riesgo mejorando sus políticas de acceso en los diferentes dispositivos y con la incorporación de nuevas contraseñas más sólidas evitar ser vulnerados, entendiendo que debe implementar controles que representan costos más elevados en su presupuesto pero con el beneficio de ser viables para la consecución de sus objetivos en temas de seguridad.

Se brinda la posibilidad de erradicación y análisis de los comportamientos de los atacantes informáticos que enfrentó Energitel dándoles la oportunidad de crear un entorno informático más seguro, emitiendo la posibilidad de implementar políticas de seguridad que garanticen el control y protección de la información, bases de datos y demás activos valiosos para la organización.

De los riesgos hallados ocho se encuentran en una franja de gestión de carácter urgente debido a su probabilidad de ocurrencia y su impacto en el sistema, el resultado obtenido según la metodología Magerit es la de generar controles y salvaguardas para un tratamiento adecuado de los riesgos de seguridad para el sistema, teniendo en cuenta que las vulnerabilidades identificadas según las pruebas realizadas no solamente tienen una alta probabilidad de ocurrencia sino que además pueden generar un impacto negativo.

El análisis profundo y crítico de vulnerabilidades en los canales de transmisión de información, permitirá decretar el valor del activo, versus el valor de inversión en profesionales de seguridad informática, software especializado, y herramientas para su soporte en las actividades para proteger los activos significativos para la empresa Energitel.

Magerit permitió identificar el inventario actual de los activos de Energitel, soportando la fase 2 de esta metodología, de igual manera se puede evidenciar en el anexo A, las fases 3 y 4 respecto a la identificación de vulnerabilidades y amenazas se reflejan en las tablas 2 y 3, y con la herramienta Metasploit se logró realizar escaneo de forma fácil de las vulnerabilidades del sistema informático atacando puertos que pueden tener acceso a información confidencial, con el anexo B se puede verificar las pruebas realizadas en algunos dispositivos de Energitel.

Metasploit permite ingresar de forma fácil al sistema informático y puertos abiertos mediante un escáner completo permitiendo observar que hay un equipo conectado a la red que está incorporada en la IP 192.168.0.8 llamativo por su gran cantidad de puertos y servicios abiertos, esta vulnerabilidad es soportada en las imágenes 10 y 11. El comando nmap -O identifica que la máquina de IP 192.168.0.6 requiere de pruebas de análisis por vulnerabilidades encontradas, ver imágenes 12 y 13.

El ataque Metasploit permitió tomar varios puertos dentro del cual está el puerto 21 con el servicio FTP que es bastante vulnerable el cual es el más sencillo para analizar y atacar, para verificar este procedimiento se puede observar y ver las imágenes 18 y 19.

Para las fases 5 y 6 de Magerit se determinó la estimación del impacto el cual permite valorar el activo y determinar su impacto (tabla 5 y 6), la estimación del riesgo que es soportado en la tabla 7 de análisis del riesgo, la tabla 8 que representa los efectos negativos por causa del nivel de riesgo (tabla 9), por último la evaluación del riesgo (tabla 10) que delimita el (NR) y el tratamiento a seguir por la organización en la consecución de evacuar sus debilidades en su sistema informático respecto a las vulnerabilidades y riesgos detectados.

REFERENCIAS BIBLIOGRÁFICAS

ACENS. Bases de datos y sus vulnerabilidades más comunes. [En línea]. https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

Adminso. Administración de sistemas operativos. Prevención. [En línea] [Consultado 11 de febrero de 2017] disponible en: http://www.adminso.es/index.php/4._Medidas_de_seguridad_en_los_sistemas_inform%C3%A1ticos

Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 12-14

Aguilera López, Purificación. Seguridad Informática. España Editorial Editex .2010 Pág. 13-14

Aguilera López. Seguridad informática: Madrid: Editex, S.A, 2010. 240 p

Areitio. Javier. Seguridad Informática. Capítulo 2: Análisis de riesgo de seguridad. Pág. 57. [En linea]. España: Paraninfo, 2008. [Citado 15 marzo 2018] disponible en: https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q=Riesgo&f=false

Areitio. Javier. Seguridad Informática. 1a ed. España: Paraninfo, 2008. p.2

Asintec. ¿Qué es Trazabilidad? [En linea]. [Citado 17 junio 2018] disponible en: http://www.asintec.es/que-es-trazabilidad/article/130-2

BARRIOS CANTILLO. Jaime (2017). Pasos para el análisis de riesgos basados en MAGERIT. [En línea]. [11 de febrero de 2017] [revisado 25 marzo de 2018] disponible en: https://es.slideshare.net/jaimeral73/pasos-para-el-anlisis-de-riesgos-basados-en-magerit.

BORGHELLO, Cristian. Políticas de Seguridad de la Información. [En linea]. 2009. [10 marzo 2018] disponible en: https://www.segu-info.com.ar/politicas/polseginf.htm

Cabezas, Ivan Correa Martha. Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional SIUN. 2014. [En linea] [10 de junio de 2018] disponible en: http://investigacion.unal.edu.co/fileadmin/recursos/docs/politicas/seguridad/siun_web_politicas_seguridad.pdf 1 Ibíd. Pag 1

COMPUTERHOY. Rubén Andrés. Qué es Kali Linux y qué puedes hacer con él. Recuperado el día 27 de enero de 2012 disponible en: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux

CARDONA A. Omar Darío EVALUACIÓN DE LA AMENAZA, LA VULNERABILIDAD Y EL RIESGO. "Elementos para el Ordenamiento y la Planeación del Desarrollo". [En linea]. 2009. [10 marzo 2018] disponible en: http://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

David A. Franco, Jorge L (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. [En línea]. [10 agosto 2017], disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

DUCUARA CRUZ. Ángel Yesid. MANUAL DE BUENAS PRACTICAS SOBRE LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE DE LA ENTIDAD DEL DANE. [En línea], 11 de febrero de 2017 [revisado 14 julio de 2018]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/997/Proyecto%20de%20Grado%20Manual%20de%20Buenas%20Practicas%20DANE.PDF?sequence=1&isAllowed=y.

Ecured (2017). Luis Rodríguez Berzosa. Control de acceso. [En línea]. [10 agosto 2017], disponible en: https://www.ecured.cu/Control_de_acceso

Ferro Soto, Carlos. Martínez Senra Ana Isabel. Otero Neira, Ma Carmen. Ventajas del Uso de las Tics en el proceso de Enseñanza Aprendizaje desde la Óptica de los Docentes Universitarios Españoles. Edutec. Revista Electrónica de Tecnología Educativa. Número 29/julio 2009, pág. 3

Fileadmin. Definición de políticas de seguridad informática de los servidores y sitios web del Sistema de Investigación de la Universidad Nacional – SIUN. Recuperado el día 03 de julio de 2017 de http://investigacion.unal.edu.co/fileadmin/recursos/docs/politicas/seguridad/siun_web_politicas_seguridad.pdf

FOMBONA. Javier. Revista Iberoamericana CTS. Centro de Estudios sobre Ciencia, Desarrollo y Educación Superior (Centro REDES) Mansilla 2698, 2º piso - Ciudad Autónoma de Buenos Aires, Argentina. [En línea]. [10 agosto 2017], disponible en: http://www.revistacts.net/volumen-11-numero-32/316-articulos/726-los-problemas-de-los-recursos-informaticos-en-el-contexto-universitario

Gómez Vieites, Álvaro. Seguridad informática Básico. [En línea]. [Consultado 20 de julio de 2018] disponible en: http://www.ecoeediciones.com/wp-content/uploads/2016/08/seguridad-informatica-basico.pdf

Iglesias Mouteria, Rubén. Instalación De Redes Informáticas e Ordenadores. España Editorial Ideas Propias .2006 Pág. 136

ISAZA VILLAR, Miguel Arturo. La Seguridad Informática Hoy. [En línea], 20 de septiembre de 2013 [revisado 25 marzo de 2018]. Disponible en: https://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html

ISOTOOLS. ¿Qué es la NTC ISO 27001? [En línea]. [Consultado 10 marzo 2018] disponible en: https://www.isotools.com.co/normas/ntc-iso-27001/

Iván. Manjarrés. Bolaño, Caracterización de los delitos informáticos en Colombia, Octubre 2012. [En línea] [Consultado 11 de febrero de 2017] disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149.

Javier Jarauta Sánchez. Seguridad Informática Capítulo 1: Introducción y conceptos básicos Definiciones: Análisis y Gestión de Riesgos. [En linea]. [Citado 15 marzo 2018] disponible en: https://www.iit.comillas.edu/palacios/seguridad/cap01.pdf

JARA. Héctor. Ethical Hacking 2.0. Implementación de un Sistema para la Gestión de la Seguridad. [En linea]. [Citado 05 julio 2018] disponible en: https://books.google.es/books?hl=es&lr=&id=PkDCIzakkB4C&oi=fnd&pg=PA4&dq=ethical+hacking+espa%C3%B1ol&ots=B4v-9UA65w&sig=k0V5i4e7qr4xpqBDh9VAX0IAafc#v=onepage&q=ethical%20hacking%20espa%C3%B1ol&f=false

José Fernández G. Seguridad en Informática Aspectos Duros y Blandos. Octubre 2013. [En línea]. [Revisado 14 julio de 2018]. Disponible en: http://www.aprocal.org.mx/files/2200/03SeguridadenInformaticaV1.0.pdf

Legislación Informática de Colombia. [En linea] [01 de septiembre de 2018] disponible en: http://www.informatica-juridica.com/legislacion/colombia/

MAÑAS, José A. MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012. p 7

Mario G. Piattini Velthuis. Calidad de sistemas informático. [En línea]. [10 junio 2018] disponible en: https://books.google.com.co/books?id=yoi4GAAACAAJ&dq=importancia+de+los+sistemas+informaticos&hl=es&sa=X&ved=0ahUKEwjAzKP82O_aAhVJrFMKHaaLBQwQ6AEIMDAC

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. MAGERIT Versión 1.0. Riesgo. [En línea]. [Consultado 31 agosto 2018] disponible en: recuperado de: http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Guía de gestión de riesgos. Guía 7. [En línea]. [10 agosto 2017], disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC. Controles de seguridad de la información. [En línea]. [10 mayo 2017], disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea], octubre de 2012 [06 abril de 2018] disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WszQP4jwbIU

Pérez, Julián Gardey, Ana. Definición de tecnología de información. [En línea]. [10 julio 2018] disponible en: (https://definicion.de/tecnologia-de-la-informacion/)

REDESZONE. DE LUZ. Sergio. Ya puedes ejecutar Metasploit Framework directamente en un contenedor Docker. [En linea]. [Citado 17 junio 2018] disponible en: https://www.redeszone.net/2016/05/15/ya-puedes-ejecutar-metasploit-framework-directamente-contenedor-docker/

REDES ZONE. VELASCO. Rubén Qué nos deparará 2018 en cuanto a seguridad informática. [En linea]. 1 de enero de 2018. [10 abril 2018] disponible en: https://www.redeszone.net/2018/01/01/seguridad-informatica-2018/

Stallings, Williams. Fundamentos de seguridad en redes aplicaciones y estándares. Segunda edición. Madrid. Pearson Educacion.2004. Pág. 2

SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: Amenazas y vulnerabilidades. [En línea]. [Consultado 20 de julio de 2018] disponible en: https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/

SOLARTE SOLARTE. Francisco Nicolás. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BAJO LA NORMA ISO 27001 Y 27002. EVALUACIÓN DE RIESGOS. Recuperado el día 6 de JULIO de 2016 disponible en: http://sgsipractico.blogspot.com/2016/07/estimacion-del-impacto.html

SOSA. Johana. Análisis de Riesgos. Estándares para la administración de riesgos. Recuperado el día 27 de enero de 2012 disponible en: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf.Pag.41.

SOSA. Johana. Análisis de Riesgos. Estándares para la administración de riesgos. Recuperado el día 27 de enero de 2012 disponible en: http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf.Pag.14.

TARAZONA T. César H. AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN. file:///D:/Users/Usuario/Downloads/965-3375-2-PB%20(1).pdf. Pág. 141.

Universidad de Murcia. Capítulo 5. IAGP 2005/06. Gestión de riesgos en ingeniería del software. 5.8 Magerit. [En linea]. [17 de junio de 2006] disponible en: http://www.um.es/docencia/barzana/IAGP/Iagp5.html

UTP. Universidad Tecnológica de Pereira. [En linea]. [Citado 18 junio 2018] disponible en: https://www.utp.edu.co/gestioncalidad/sin-categoria/279/ntc-iso-iec-27002/pdf

VALENCIA BLANCO. Leidi Stefani. Universidad Mayor de San Andrés Metodologías Ethical Hacking. [En línea], [revisado 25 marzo de 2018]. Disponible en: http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a12.pdf

Walter Vega Velasco. Septiembre de 2008. . [En línea]. http://www.scielo.org.bo/scielo.php?pid=S2071-081X2008000100008&script=sci_arttext&tlng=es

ANEXOS

ANEXO A. INVENTARIO DE ACTIVOS ENERGITEL

La tabla 11 de inventario de activos nos da la información actualizada de la existencia, estado, finalidad y persona responsable teniendo en cuenta las funciones y el grado de valor de cada activo dentro del proceso orientándonos de forma especifica si este fuese afectado y en dado caso si llegase a faltar por causa de una amenaza, vulnerabilidad o riesgo materializado.

Tabla 11. Inventario de Activos Energitel

INVENTARIO DE ACTIVOS ENERGITEL						
Tipo Activo	Código	Magerit		Proceso	Activo	Responsable
Esenciales	S1	S	EXT	ATC	Información al cliente	Jefe comercial
Esenciales	S2	S	INT	TI	Conexión a la base de datos	Supervisor de sistemas
Esenciales	S3	S	EMAIL	TI	correo electrónico	Analista de sistemas 1
Esenciales	S4	S	FILE	TI	Almacenamiento de Datos	Jefe de sistemas
Datos o información	SI01	SI	NON_ELECTRONIC	ADMON	Portafolio de servicios	Subgerente Comercial
Datos o información	D01	D	ADM	ADMON	Datos información al cliente	Subgerencia Comercial
Datos o información	D02	D	COM	ADMON	Datos Información de la empresa	Departamento de mercadeo
Datos o información	D03	D	COM	ADMON	Datos de registro del proveedor	Director comercial
Datos o información	D04	D	COM	ADMON	Datos Información financiera cliente	Analista de crédito

Tabla 11. (Continuación)

INVENTARIO DE ACTIVOS ENERGITEL						
Tipo Activo	Código	Magerit		Proceso	Activo	Responsable
Software	SW01	SW	OS	ADMON	Software WINDOWS 10PRO	Jefe de sistemas
Personal	UI01	UI	USUARIOS_INTERNOS	ADMON	Trabajadores	Recursos Humanos
Equipos informáticos	HW01	HW	PABX	ADMON	Teléfono IP	Jefe de área
Equipos informáticos	HW03	HW	DATA	TI	Servidores Web Físico 1	Jefe de sistemas
Equipos informáticos	HW04	HW	DATA	TI	Servidores Web Físico 2	Analista de sistemas 1
Equipos informáticos	HW05	HW	DATA	ADMON	Servidores Web Físico 3	Departamento comercial
Equipos informáticos	HW06	HW	DATA	TI	Servidores Web Lógico 1	Aux. de sistemas
Equipos informáticos	HW07	HW	DATA	TI	Servidores Web Lógico 2	Analista de sistemas 2
Equipos	HW08	HW	DATA	ADMON	Servidores Web	Subgerencia

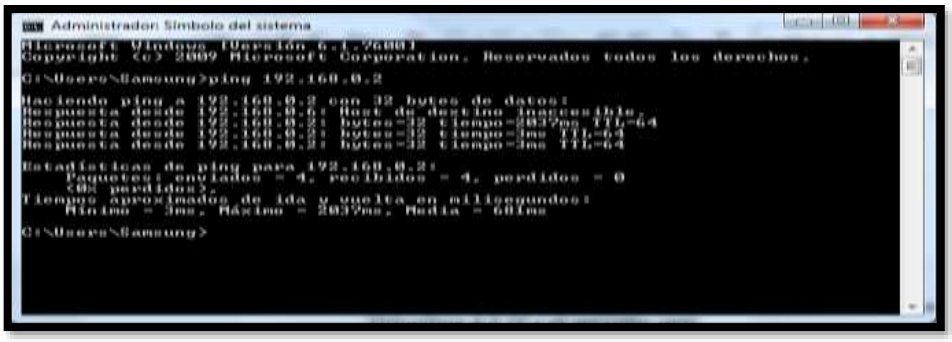
Fuente: El Autor

ANEXO B. PRUEBAS DE VULNERABILIDAD DE PUERTOS

Pruebas de seguridad en dispositivos e identificación de datos en la red de Energitel:

Servidor web: 192.168.0.2
Mascara: 255.255.255.0

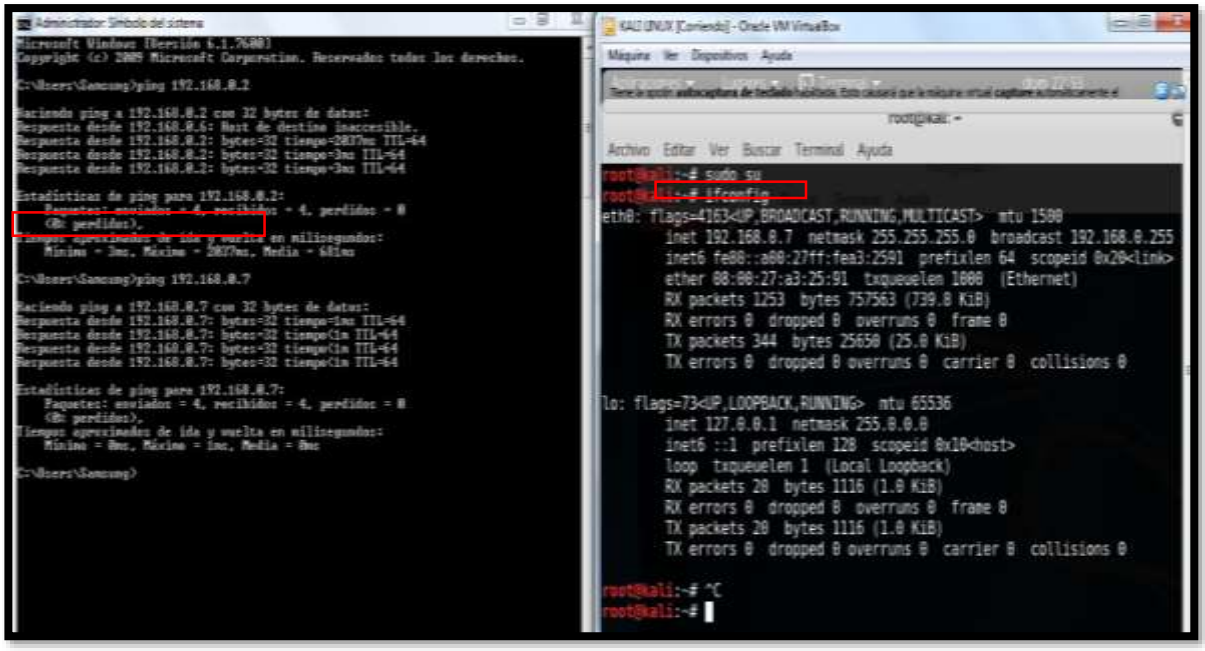
Figura 8. Símbolo del Sistema o Consola CMD



Fuente. El Autor

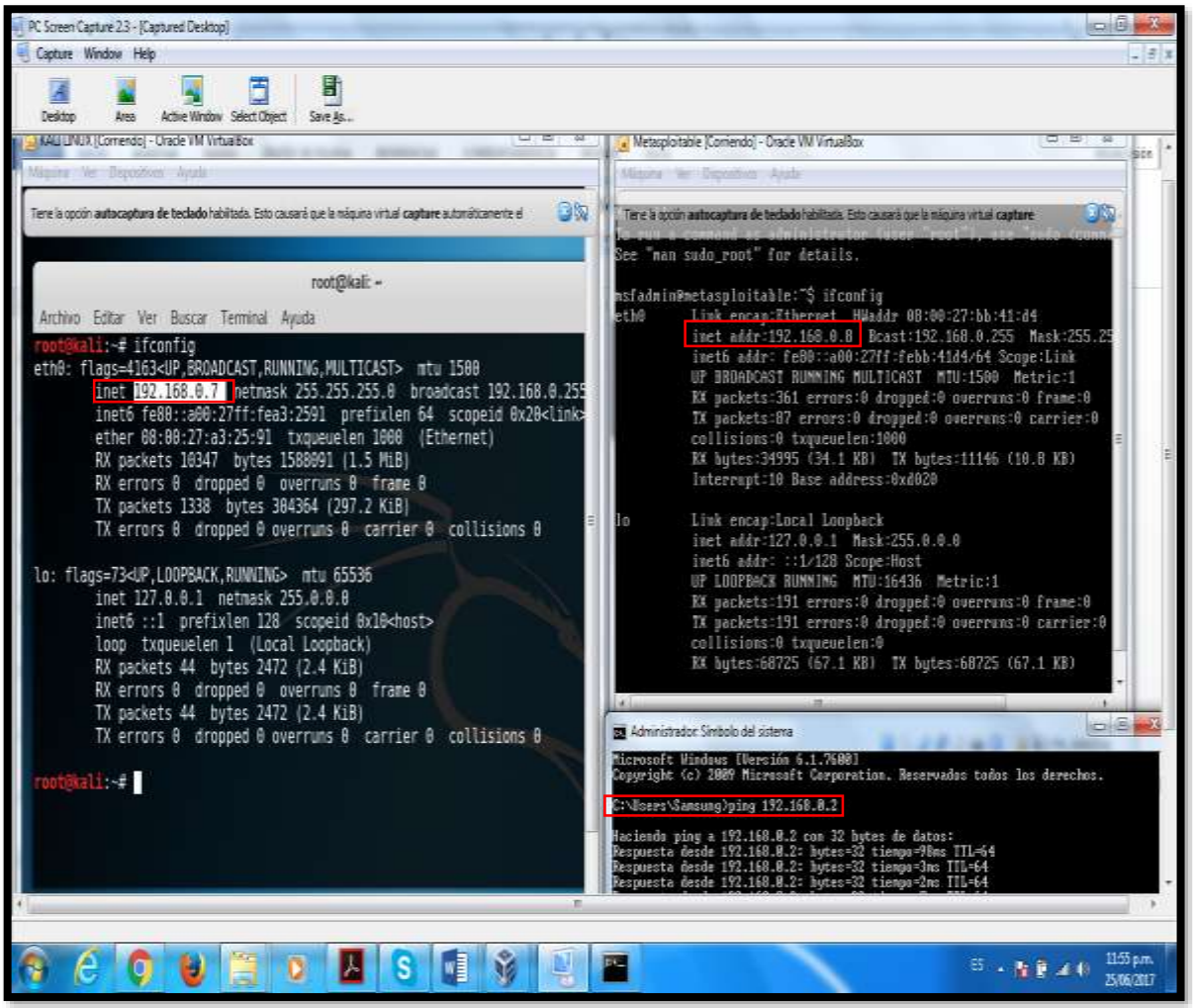
Kali Linux: 192.168.0.7
Mascara: 255.255.255.0

Figura 9. Prueba IP Kali Linux



Fuente. El Autor

Figura 10. Trazabilidad de IPs



Fuente. El Autor

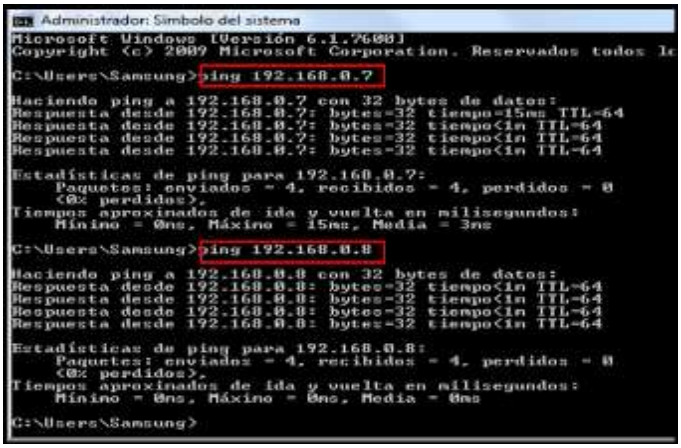
Metasploitable en virtual box 4.3.12

IP host: 192.168.0.2
IP Kali: 192.168.0.7
IP Metasplotable: 192.168.0.8

Desde el servidor de Windows se comprobó que la conexión de las dos máquinas virtuales es real: Ping para las dos máquinas IP Kali: 192.168.0.7 y IP Metasplotable: 192.168.0.8

MetaSploit[54] es un conjunto de programas en realidad. Está proyectada para aprovechar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo.

Figura 11. Comprobación de Conexión de Maquinas

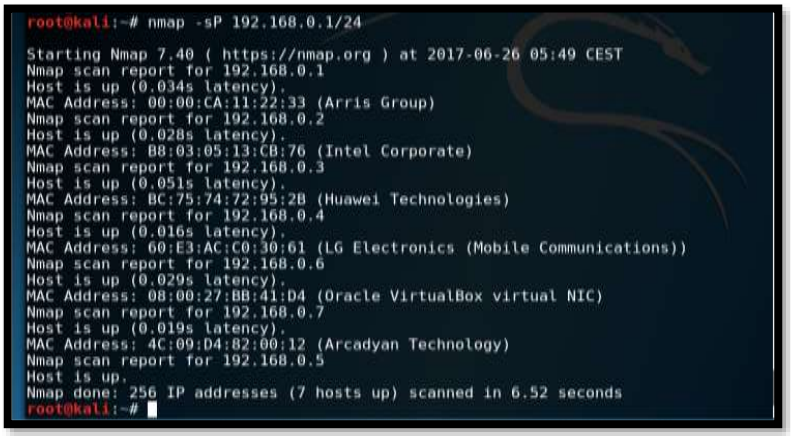


Fuente. El Autor

Se procede a buscar vulnerabilidades con la herramienta nmap teniendo en cuenta que no conocen la IP:

Namp -sp 192.168.0.7/24 (se encontró 7 dispositivos conectados a la red).

Figura 12. Verificación de Conexión de Dispositivos en Kali Linux

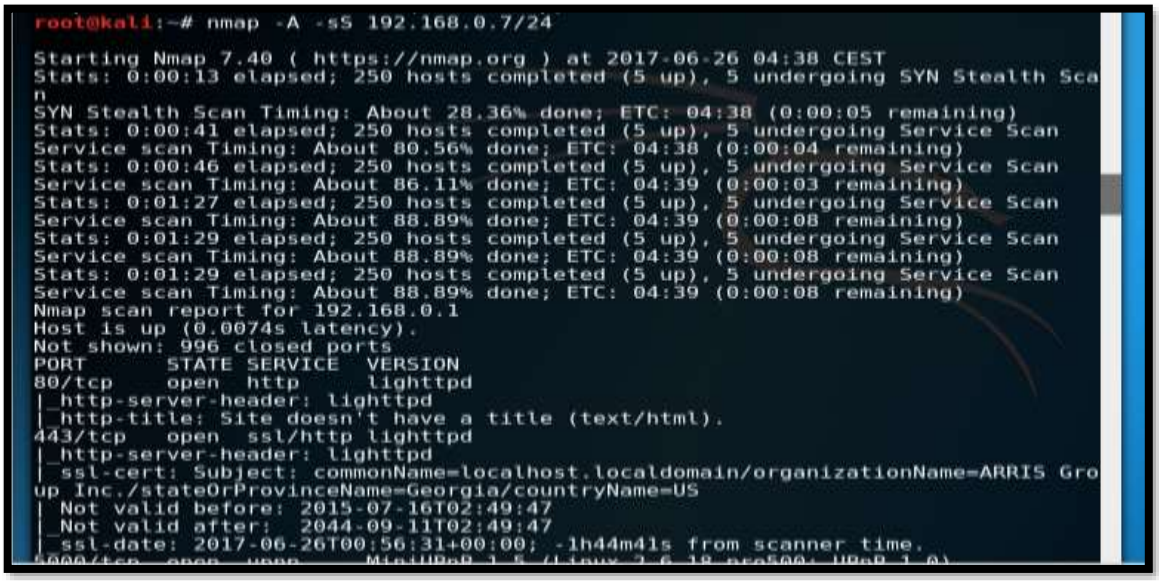


Fuente. El Autor

54 CURSO DE HACKERS. MetaSploit, tomar control de equipos remotos. Recuperado el día 27 de enero de 2012. disponible en: http://www.cursodehackers.com/metasploit.html

Se realiza un escáner más completo para evidenciar datos del sistema operativo y puertos abiertos:

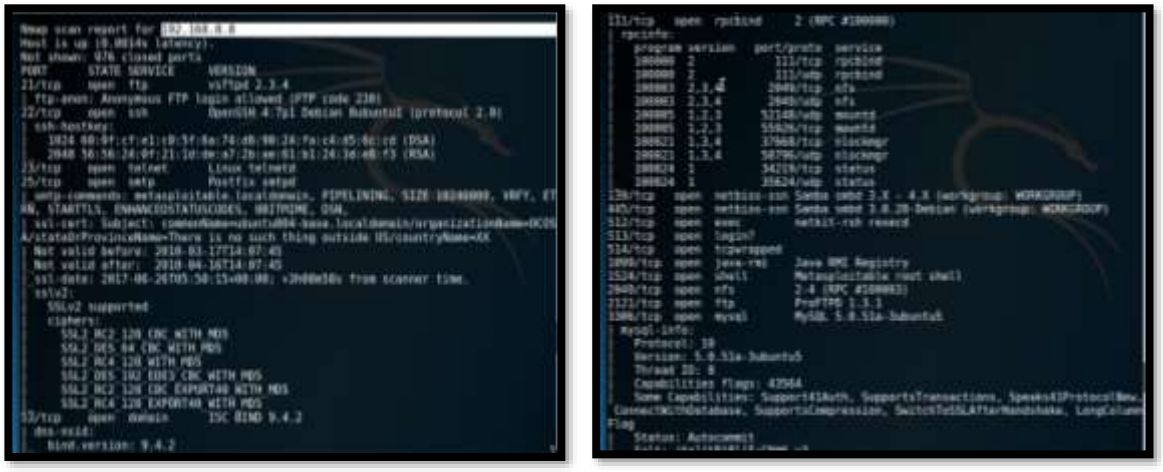
Figura 13. Nmap -A -sS 192.168.0.7/24 (Examina las IPS conectadas)



Fuente. El Autor

Finalizado el escáner hay un equipo conectado a la red que está incorporada en la IP 192.168.0.8 que es llamativo debido a su gran cantidad de puertos y servicios abiertos:

Figura 14. Puertos y Servicios Abiertos IP



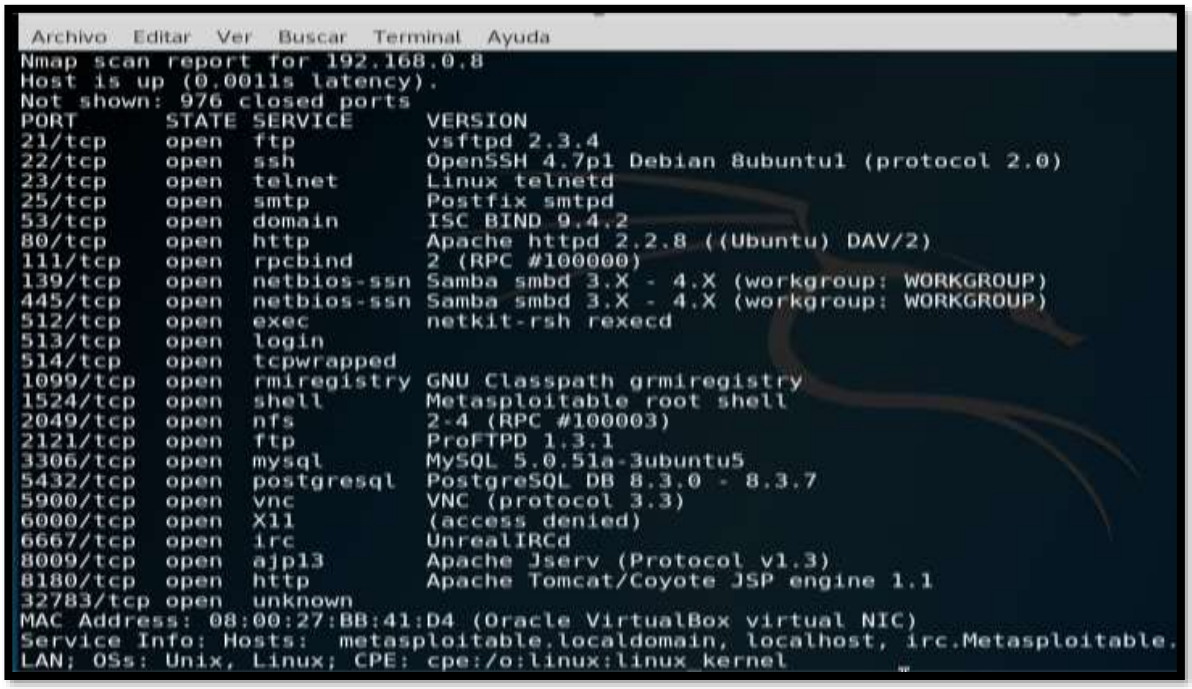
Fuente. El Autor

Según Fernando Muñoz[55], los puertos serían las ventanas y puertas nuestra casa, es decir, servicios que ofrece y que fácilmente utilizan para comunicarse, bien internamente (localhost) o bien externamente.

Reconocida la dirección IP de la máquina que puede tener las vulnerabilidades se procede a realizar nuevamente el escaneo con nmap para identificar los puertos de forma más específica:

Nmap -sV -T4 -Pn 192.168.0.8

Figura 15. Escaneo Nmap para Identificar los Puertos



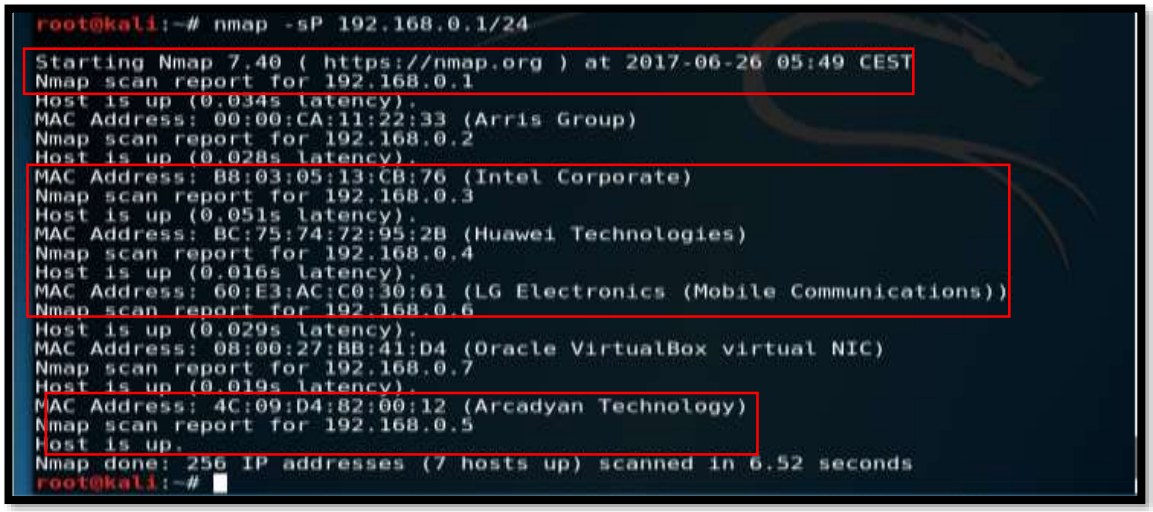
Fuente. El Autor

Realizado la revisión y análisis se procede a utilizar metasploit para saber cuáles de los servicios presentan vulnerabilidades.

Para ello podrán utilizar el comando nmap -O más las IPS que no reconozco para determinar cuál es la máquina que requieren para realizar el análisis. Las Ips que están en el recuadro son las que no se reconocen:

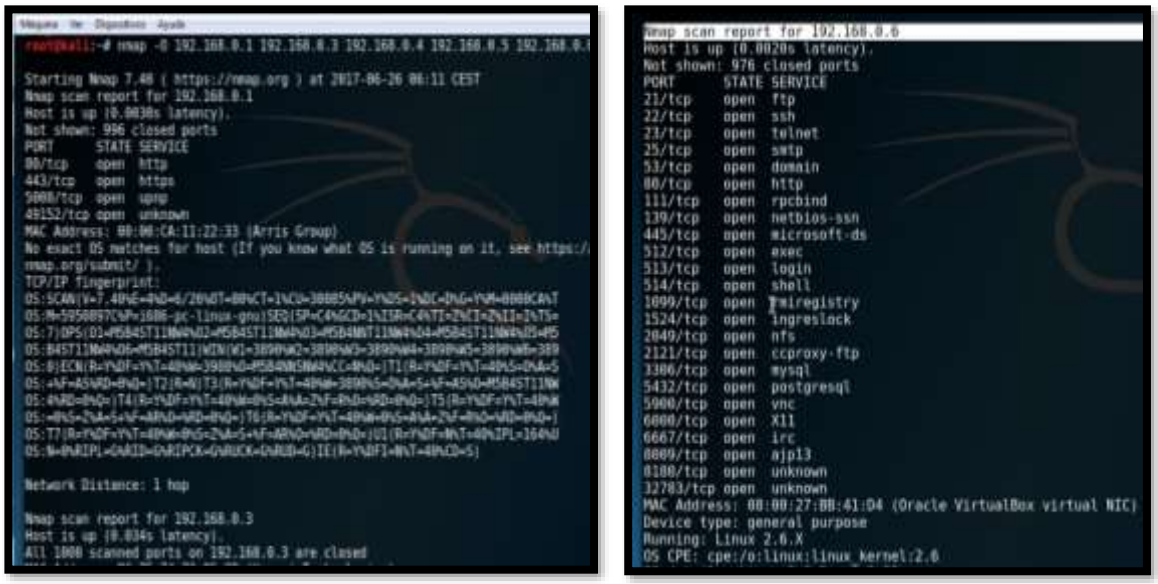
55 FERMU. MUÑOZ. Fernando. SEGURIDAD EN INTERNET: EL COMANDO NETSTAT, PUERTOS Y COMUNICACIONES. En linea. Recuperado el día 27 de enero de 2012. disponible en:http://www.fermu.com/articulos/windows/articulos-y-tutoriales/285-seguridad-en-internet-el-comando-netstat-puertos-y-comunicaciones

Figura 16. Uso Comando nmap -O



Fuente. El Autor

Figura 17. Identificación IP 192.168.0.6



Fuente. El Autor

Con este escaneo identificaran que la maquina tiene la IP 192.168.0.6

La sintaxis dentro del metasploit es la siguiente (realizaran el ataque o análisis a los puertos siguientes):

Utilizaran el comando *msfconsole* para iniciar los servicios de metasploit y podrán verificar la línea de comandos:

Figura 18. Activación de Servicios de Metasploit

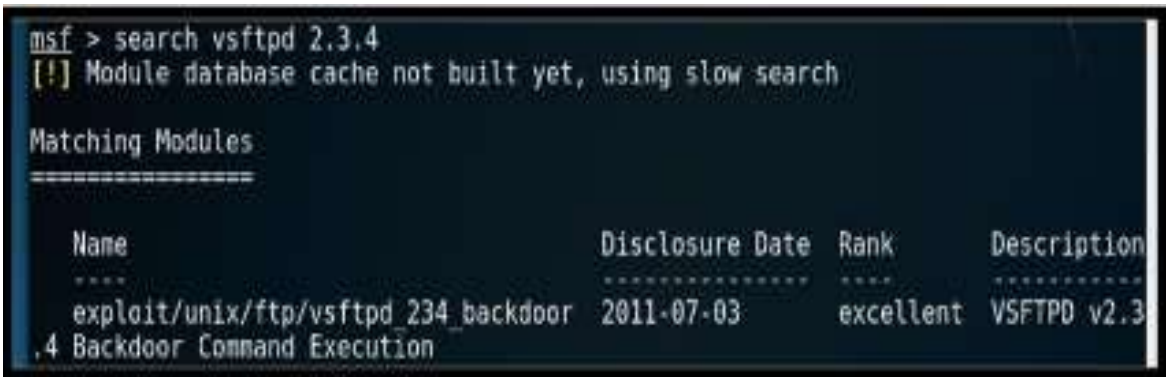
Fuente. El Autor

Utilizaran nmap para el análisis de los puertos
Nmap -sV 192.168.0.8
msf > search vsftpd 2.3.4 Puerto (analizado)

Figura 19. vsftpd 2.3.4 Puerto (analizado)

Fuente. El Autor

Figura 20. Resultado



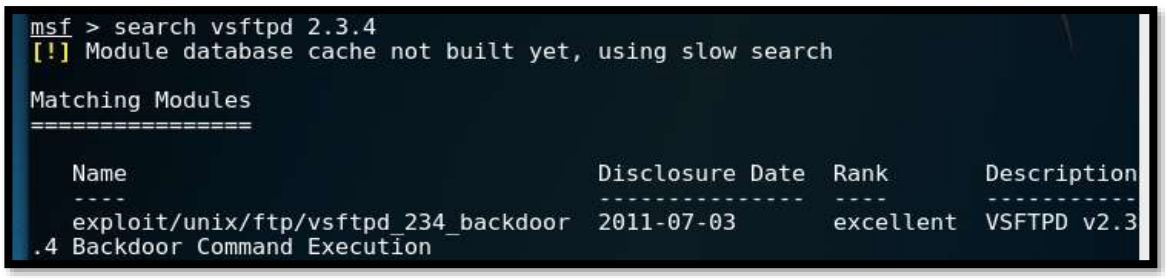
Fuente. El Autor

Evidencia de la vulnerabilidad dentro del servidor FTP, en una versión modificada del paquete oficial, la cual contenida un backdoor.

Análisis de vulnerabilidad:

Iniciaran el tipo de vulnerabilidad en metasploit para así revisar las opciones:

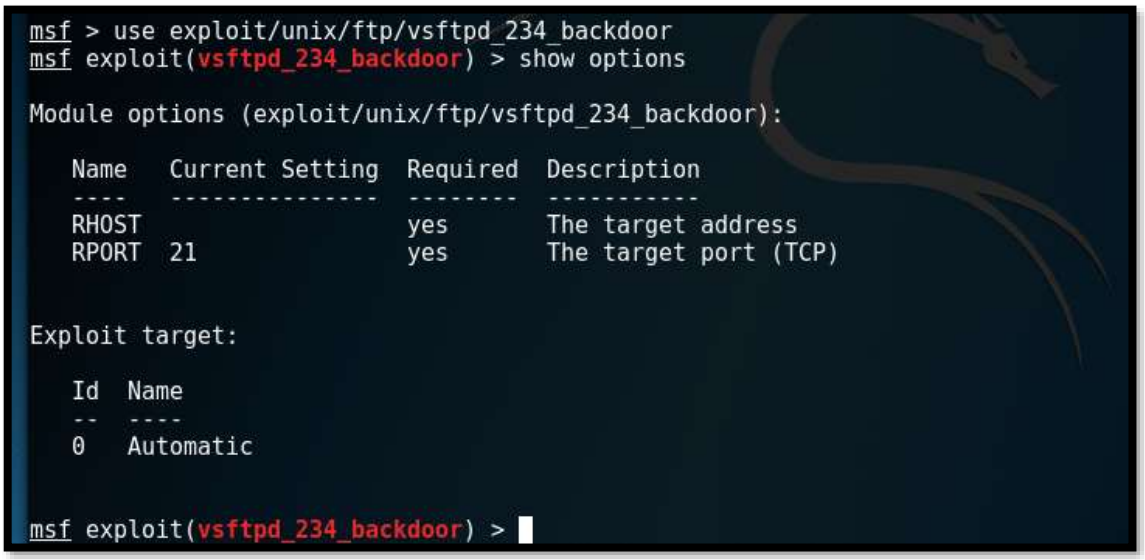
Figura 21 Puerto 21 Escaneado



Fuente. El Autor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit (“vulnerabilidad”) > show options

Figura 22 Análisis Puerto 21



Fuente. El Autor

Ejecución del ataque: se centraran en el puerto 21 con el servicio ftp que es el más sencillo de atacar.

ANEXO C. CARTA DE AUTORIZACIÓN DE ACCESO A LA INFORMACIÓN.

H.S ENERGITEL

NIT.93.405.573-6

CONSTANCIA DE AUTORIZACION

Yo Diana Marcela Palacino Rayo con CC. 1.106.776.008 De Chaparral quien desempeña el cargo de Coordinadora de Proyecto autorizo al señor Hilbert Leonardo Sánchez Gamboa con CC 93.405.573 de Ibagué para acceder al sistema de información y bases de datos confidenciales de H.S Energitel con propósitos de investigación para cumplir requisitos aplicados al proyecto de grado de la Especialización en Seguridad Informática que adelanta en la universidad nacional abierta y a distancia (Unad).

Se expide certificado a solicitud del interesado en Ibagué, 17 de Marzo de 2018.

Diana Marcela Palacino Rayo
Coordinado de Proyecto

Calle 143 con Cra 14 vía el Salado, Portales del Norte Mz: O Casa 14 - E-Mail: Hilbert_326@yahoo.es - Cel: 3015035819 - Ibagué Tolima

ANEXO D. PROPUESTA DE PROYECTO DE ELECTRIFICACIÓN CONJUNTO LAS JUANAS (ROBO DE CONTRATO).

H.S ENERGITEL

NIT.93.405.573-6

Ibagué, 30 de Julio de 2016

Señor
Mauricio Garcia

REF: MANTENIMIENTO CORRECTIVO EN PREDIO, RED ELECTRICA EN M.T 13.2 KV DE DISTRIBUCION DE ENERGIA.

Respetado Señor

Atendiendo su amable solicitud, estamos haciendo llegar nuestra mejor propuesta.

1. OBJETO

Mantenimiento correctivo del sistema eléctrico del predio ubicado en la Condominio las Juanas, con el fin de corregir red de M.T que pasa por el medio de la propiedad.

2. ALCANCE

Cumplir con la necesidad de ofrecer las condiciones de confort y normalización del sistema de acuerdo con los requerimientos especiales de la edificación.

3. FORMA DE PAGO MANO DE OBRA

70% al iniciar obra y 30% al terminar.

4. VALOR MANO DE OBRA

El valor de la oferta es de trece millones pesos m/cte $ 13.000.000.

Calle 143 con Cra 14 via el Salado, Portales del Norte Mz: O Casa 14 - E-Mail:diana.palacino@energitel.com – Cel: 3114943745 – Ibagué Tolima

5. VALOR DE MATERIALES

Valor materiales más IVA $ 13.300.636,04

6. ENTREGA DE LA OBRA

La obra tiene un plazo de aproximadamente 10 días para la entrega, para ello se debe tener en cuenta las consecuencias del estado climático que nos puede llegar a ocasionar inconvenientes para la entrega.

7. GARANTIA

La garantía es sobre el mantenimiento correctivo de la instalación y puesta en marcha y/o normalización del sistema en cuestión.

8. ACTIVIDADES DE MANTENIMIENTO CORRECTIVO

- Desenergizada de los circuitos a 13.2 kV.
- Desmontaje y montaje de red de M.T.
- Construcción e instalación de estructuras para variación de la topología de la red de M.T existente.
- Instalación y conexión de 3 circuitos a 13,2 kv de transformadores existentes.
- Construcción de 2 estructuras en H.
- Construcción de 1 estructura de retención sencilla.
- Construcción de 2 estructuras de paso.
- Adecuación de 2 estructuras existentes.
- Energizada y normalización de los circuitos a 13.2 kV.

SITUACIONES NO CUBIERTAS POR LA GARANTIA

1. Problemas causados por la invasión de elementos extraños al producto como: arena, insectos, roedores o similares.
2. Problemas causados por incendios, fluctuaciones de voltaje de la empresa **Enertolima** en el nivel de MT, BT, vandalismo, robo o similares.
3. Manipulación inadecuada (operación) de las instalaciones eléctricas por particulares.

Calle 143 con Cra 14 vía el Salado, Portales del Norte Mz: O Casa 14 - E-Mail:diana.palacino@energitel.com – Cel: 3114943745 – Ibagué Tolima

COSTOS MATERIALES

CODIGOS	DESCRIPCION DE MATERIALES	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
13914	POSTE DE FIBRA DE VIDRIO DE 10 METROS 510 KGF	6	$ 878.378,58	$ 5.270.271,48
13915	POSTE DE FIBRA DE VIDRIO DE 10 METROS 750 KGF	1	$ 1.100.216,43	$ 1.100.216,43
9815	CABLE ACERO GALVANIZADO SUPERGX EXTRARESISTENTE DE 3/8"	235	$2.312,23	$ 543.374,64
10708	CRUCETA METAL. GALV. ENCALIENTE 2.4 MTS 3"x3"x5 /4" (PERFORACION UNIVERSAL)	8	$ 77.471,02	$ 619.768,16
9692	CRUCETA METAL. GALV. ENCALIENTE 3 MTS 3" X 3" X 1/4" (PERFORACIÓN UNIVERSAL)	2	$ 95.808,49	$ 191.616,97
9692	ESPARRAGO ROSCADO GALV + 4 TUERCAS - 4 GUASAS - 4 ARANDELAS 5/8 " X 12"	20	$4.422,80	$ 88.456,00
9644	ARANDELA GALVANIZADA CUADRADA 4" X 4" CON PERFORACION 5/8"	13	$2.207,76	$ 28.700,91
9657	TORNILLO GALV + TUERCA-ARANDELA-GUASA 5/8" X 1 0"	8	$2.366,98	$ 18.935,87
9733	GRAPA PRENSORA (PRENSAHILOS) EN ACERO FORJADO GALVANIZADO 3 PERNOS PAR	52	$5.620,20	$ 292.250,40
9789	TUERCA DE O.D GALVANIZADA ALARGADA 5/8"	18	$4.547,56	$ 81.885,99
11768	VARILLA DE ANCLAJE DE 3/4 X 2.0 MTS	13	$ 35.678,00	$ 463.814,00
10056	ABRAZADERA GALVANIZADO MAS T CENTRAL 5/8" 2 SALIDAS 140 MM (5" - 6")	4	$ 10.713,87	$ 42.855,47
10470	DIAGONAL METALICA GALVANIZADA DE 68 CMS RECTA EN ANGULO 1 1/2" X 3 /16"	20	$8.850,70	$ 177.014,00
9834	AISLADOR TIPO TENSOR 13.2KV (ANSI 54-2)	13	$6.164,39	$ 80.137,01
10259	FUSIBLE 15 KV TIPO H 2 AMP	4	$1.632,12	$ 6.528,48
10101	FUSIBLE 38 KV TIPO H 3 AMP	4	$2.151,76	$ 8.607,04
10253	FUSIBLE 15 KV TIPO H10 AMP	4	$1.789,50	$ 7.157,98
11232	GRAPA DE RETENCION 6.000 LBS TIPO PISTOLA (6-3/0AWG) REF 701	15	$ 14.904,78	$ 223.571,70
9837	AISLADOR SUSPENSION POLIMERICO (RETENCION O ELASTOMERICO 13.2 KV)	15	$ 23.842,01	$ 357.630,08
9721	ESPIGO PIN EXTREMO POSTE PARA 13.2 KV A 15 KV	8	$8.254,98	$66.039,82
13084	AISLADOR TIPO PIN 13.2 KV	8	$ 48.720,00	$389.760,00
10934	VIGUETA DE CONCRETO 0.60X0.15X0.15 MTS- CON CANASTILLA METALICA.	13	$ 13.018,63	$169.242,13
9692	GUARDACABO GALVANIZADO 3/8 IN T-3	12	$ 598,90	$7.186,77
12796	TORNILLO GALVANIZADO CIT (112 TORNILLOS SIN TUERCA) ½" X1 ½"	22	$1.500,00	$33.000,00
9817	CABLE ALUMINIO DESNUDO 7 HILOS TIPO ACSR NO. 2 AWG	1900	$1.136,69	$1.823.496,00
	TOTAL			$12.080.482,33

VALOR TOTAL DE LA OBRA

Costo Mano de Obra	$ 13.000.000,00
Costo Materiales + IVA	$ 13.300.636,04
Total Obra	**$ 26.300.636.04**

En espera de sus comentarios.

Atentamente,

Diana Marcela Palacino Rayo
Coordinado de Proyecto

Calle 143 con Cra 14 via el Salado, Portales del Norte Mz: 0 Casa 14 - E-Mail:diana.palacino@energitel.com – Cel: 3114943745 – Ibagué Tolima

ANEXO E. PROYECTO DE DISEÑO VERDE MENTA (PERDIDA DE INFORMACIÓN)

H.S Energitel

Ibagué, 21 de Mayo de 2016

REF: PROPUESTA DISEÑO ELECTRICO.

Se brinda propuesta para la elaboración y aprobación del diseño eléctrico del conjunto Verde Menta.

RESPETADO ARQUITECTO FERNANDO GARCIA

Atendiendo su amable solicitud, estamos haciendo llegar nuestra mejor propuesta.

1. OBJETO

Realizar diseño eléctrico del conjunto Verde Menta aprobado ante la electrificadora del Tolima Enertolima.

2. DOCUMENTACION REQUERIDA PARA APROBAR DISEÑO

- Certificado de factibilidad de conexión del proyecto (PPC).
- **Autorización del propietario del proyecto.**
- Oficio de aceptación de elaboración del estudio de conexión.
- **Certificado de existencia y representación legal.**
- **Certificado de libertad y tradición autorizado.**
- **Certificado de estratificación.**
- **Licencia de construcción.**
- **Permiso de servidumbre.**
- Memorias de cálculo.
- **Recibo de pago de energía.**
- Carta remisora de solicitud de revisión radicado u oficio de respuesta de observaciones.
- Resumen del proyecto.
- Copia magnética del plano: plano en AutoCAD, coordenadas y perfiles.
- Planos.
- **Plano arquitectónico de la construcción.**

Calle 143 con Cra 14 vía el Salado, Portales del Norte Mz: O Casa 14 - E-Mail: diana.palacino@energitel.com - Cel: 3114943745 – Ibagué Tolima

H.S Energitel

3. FORMA DE PAGO

Al iniciar se requiere el 70% del costo del diseño y el otro 30% al entregarlo aprobado.

4. VALOR TOTAL DEL DISEÑO

El valor de la oferta es de cinco millones de pesos m/cte. **$ 5.000.000**

VALOR DISEÑO	$ 5.000.000

5. RECOMENDACIONES

Después de aprobado y entregado el diseño eléctrico se debe ejecutar la obra en un plazo no máximo de 6 meses según directrices de Enertolima.

En espera de sus comentarios.

Atentamente,

Diana Marcela Palacino Rayo
Coordinado de Proyecto

Calle 143 con Cra 14 via el Salado, Portales del Norte Mz: O Casa 14 - E-Mail: diana.palacino@energitel.com – Cel: 3114943745 – Ibagué Tolima

ANEXO F. PÉRDIDA DE INFORMACIÓN DE CLIENTES

EMPRESAS	PERDIDA INFORMACIÓN
NESITELCO S.A	Numeros de contacto.
TELMACOM	Numeros de contacto, e informes de relacion de mantenimientos.
ELECTROTODO	N/A
SEICLIMTIZAR	Numero de contacto del gerente general.
DIGITAL	Plantilla excel para ejecucion de informes.
GMEI GRUPO MULTISERVICIOS ENERGETICOS INTEGRALES	Plantilla excel para ejecucion de informes.
HACIENDA EL PILAR	Numeros de contactos.
PAILAQUINTA	Portafolio de servicios.
Be7 STUDIOS	Rutina de actividades para mantenimiento de MG (motogenerador).
MUEBLES MORALES	Propuesta preliminar para mejoramiento de proteccionesgenerales.
BLESS	Numeros de contacto.
GIMNASIO DE LOS DIOSES	Video para presentacion de propuesta.
CAPILLA BARRIO RESTREPO	Informacion de proveedores de suministro de materiales.
PURIFIL	Listas de chequeo preliminares.

ANEXO G. ACTA DE REUNION Y EVALUACION MENSUAL

H.S ENERGITEL	ACTA DE REUNIÓN	**CÓDIGO**:100.PC.PR 01.F 01
		VERSIÓN: 1
		PÁGINA: 1 de 2

ACTA

ASISTENTES	Diana Marcela Palacino Coordinador de Proyecto Néstor Gaitán Molina Supervisor de Zona Prayor José Castañeda Supervisor de Control Operativo Álvaro Alexander Ávila Supervisor de sistemas
NOMBRE DE QUIEN SOLICITA LA REUNIÓN	H.S ENERGITEL
AUSENTES	*Ninguno*
FECHA DE REUNION	19 de Agosto de 2016
LUGAR DE REUNION	Oficina principal de ENERGITEL Cra.14 No. 143 Esquina
AREAS INVOLUCRADAS DE LA COMPAÑIA	Control Operativo, Área TI, Distribución de Energía.

AGENDA Y/O TEMAS A TRATAR DURANTELA REUNION(Utilice el espacio que considere necesario)

Perdida de la propuesta de proyecto de electrificación Conjunto las Juanas para el periodo de Julio de 2016.

Hora de Inicio 7:30 a.m.

Temas principales

Perdida de la propuesta del proyecto de electrificación Conjunto las Juanas y proyecto de diseño eléctrico conjunto Verde Menta.

Observaciones:

La propuesta del proyecto de electrificación rural del conjunto las Juanas se elaboró soportado en la información levantada en terreno en el mes de junio del presente año donde se dispuso de personal técnico operativo y un profesional de electrificación rural denominado supervisor de zona para la realización del diseño e informe final del proyecto.

El informe final del proyecto quedo a cargo del supervisor de zona Néstor Gaitán, quien tiene el manejo total y absoluto de la información del proyecto las Juanas.

Según investigación realizada por el personal de control operativo se evidencio que el informe suministrado por personal de Electrotodo al conjunto las Juanas es de procedencia del computador del supervisor de zona el cual según el área de TI, el día 5 de agosto de 2016 en horas de la mañana se reunieron en las instalaciones de Energitel, personal de Electrotodo quien nos prestaría apoyo en la ejecución del contrato las Juanas con el supervisor de zona y en ausencia de Néstor Gaitán el personal de Electrotodo accedió al dispositivo portátil

adquiriendo el informe del proyecto las juanas.

Perdida de información, proyecto Verde Menta para diseño eléctrico, por valores invertidos por verificaciones en terreno, cálculos de cargas, visitas técnicas, viáticos y ejecución de informes.

Compromisos:

El área de TI, procede a verificar y ajustar las contraseñas de los equipos de cómputo tipo escritorio y portátiles de todo el personal.

Se debe realizar seguimiento al evento de perdida de información en cuestión (proyectos las Juanas y Verde Menta).

En próximas reuniones con cualquier tipo de proveedor se debe atender al personal ajeno a la compañía en la sala de juntas y queda prohibido dejar personas solas en las oficinas a menos de que se deje un encargado como vigía para tener un control más seguro de nuestra información.

En la próxima reunión de seguimiento para el mes de agosto se evaluaran los puntos antes mencionados y las acciones implementadas de mejora.

Hora final del inventario: 04:00 p.m.

ASISTENTES

(Inserte las filas que sean necesarias)

Nombre	Cargo	Empresa	Firma
Diana Marcela Palacino	Coordinadora de Proyecto	H.S ENERGITEL	
Prayor José Castañeda	Supervisor de Control Operativo	H.S ENERGITEL	
Néstor Gaitán Molina	Supervisor de Zona	H.S ENERGITEL	
Álvaro Alexander Ávila	Supervisor de sistemas	H.S ENERGITEL	