UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO – AGOSTO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio de Riesgos y Vulnerabilidades de la Red LAN y Equipos del Infocentro San Juan.

EGRESADO:

Cristina Kriley Miranda Vera

TUTORA:

Ing. Nelly Karina Esparza Cruz

AÑO 2019

Introducción

A medida que la tecnología avanza el gobierno se ha preocupado en ofrecer su acceso en las zonas rurales, con el objetivo de que esta se accesible para todos y que no exista una brecha tecnológica para este tipo de población.

Los Infocentros son centros de información que están al mando del Ministerio de Telecomunicaciones (MINTEL), quienes ofrecen servicios tecnológicos a la ciudadanía al igual que un cyber café, pero de manera gratuita. En el Infocentro de la parroquia San Juan al igual que otros Infocentros, ofrecen a sus usuarios cursos de diferentes temáticos, como medio de capacitación para ellos.

Debido a que cualquier persona, puede hacer uso de este servicio que ofrece el gobierno, este acceso libre estas tecnologías son altamente vulnerables, ya que no existe un control que garantice la seguridad de los equipos, así como también la información de sus usuarios.

Al encargado del infocentro se lo conoce como facilitador, quien gestiona todos los recursos del mismo, y también de garantizar que todo funcione correctamente. Este gestiona los datos de las personas que asisten el lugar, con la finalidad de obtener un reporte de concurrencia, de la misma manera la gestión de los usuarios que asisten a los cursos gratuitos que ahí se imparten.

Los datos que se gestionan en estos Infocentros es muy importante para los usuarios que asisten al lugar, y esta debe mantenerse segura y que cumpla con los objetivos de calidad del resguardo de la información, mantenido su integridad y confiabilidad.

El siguiente estudio de caso pretende realizar un análisis de los riesgos y vulnerabilidades de la RED LAN y equipos Infocentro "San Juan", perteneciente al Cantón Pueblo Viejo. Es por eso que para el desarrollo del presente análisis se utilizará la metodología MAGERIT

versión 3 de análisis y gestión de riesgos relacionada directamente con el uso de tecnologías de la información. Se usará la herramienta de software PILAR, la cual está diseñada para realizar el análisis de riesgos siguiendo la metodología MAGERIT.

Se realizado una entrevista de preguntas cerradas para recolectar la información necesaria para identificar a los activos y a la vez determinar la valoración de los riesgos que estos pueden tener sino se lleva un debido control de seguridad informática.

El Infocentro de San Juan cuenta con 7 computadoras a disposición de la ciudadanía y una que ocupa la función de servidor. Todas estas tienen como sistema operativo UBUNTU, con procesador Intel coreI3, 4 gigabytes de RAM y 250 gigabytes de almacenamiento.

Dentro de los activos que presenta la red LAN del Infocentro, están los equipos de red, el cableado, instalaciones, información y personal. Estos activos necesitan un nivel de protección pertinente para asegurar la integridad y confidencialidad de los procesos que se realizan.

Dichos activos deben someterse a una etapa de valoración para identificar la importancia de cada uno de ellos, con el objetivo de facilitar la protección de los mismos. También es necesario identificar las amenazas que existen el lugar, las cuales son físicas que afectan a la infraestructura o a los equipos y lógicas que intermedian a la información o al software.

Las herramientas de software que se escogieron para hacer efectivo el presente análisis fueron ***Nmap***, la cual sirve para escanear los puertos abiertos.

Gracias a este análisis en le Infocentro se puede determinar cuáles son las vulnerabilidades que presenta dicha red y sugerir acciones necesarias para salvaguardar la información contenida en el sistema.

Este trabajo mantiene una sublínea de investigación que se ubica en procesos de transmisión de datos y telecomunicaciones.

Desarrollo

La seguridad de la información digital para una organización depende de diferentes frentes: el físico, referente al alojamiento de la información; el social, relacionado con el grado de discrecionalidad del personal que la manipula, y el lógico, que se refiere a la configuración de sus niveles de accesibilidad y disposición.

Para esta investigación se identificó que hay varias anomalías en la seguridad informática debido a que no se gestiona completamente la protección de la información en el infocentro de la parroquia San Juan, por la ausencia de conocimientos de sus administradores y por una mala aplicación de los recursos presentes en el mismo.

Con el estudio de los riesgos y vulnerabilidades de la red LAN del Infocentro de la parroquia San Juan, perteneciente al cantón Puebloviejo, provincia de los Ríos, se identificarán las potenciales amenazas, vulnerabilidades y riesgos para la información, infraestructura, equipos y plataformas tecnológica de esta organización con la finalidad de generar un sistema gestión de seguridad para que se mantenga un ambiente tecnológico seguro que brinde a los usuarios los criterios básicos de la seguridad de información los cuales son integridad, confidencialidad y disponibilidad de la información.

Los infocentros son centros de atención tecnológica para la ciudadanía que funcionan al nivel nacional, que la las personas de parroquias rurales tengan acceso a la tecnología y tengan las mismas oportunidades que las personas que viven en las grandes ciudades del país. Estos tienen a disposición de la ciudadanía en general servicios de internet, uso de computadoras, cursos de capacitaciones y otros servicios de mucho beneficio para la sociedad.

A continuación se realiza un análisis FODA del infocentro de San Juan:

Análisis FODA

Fortalezas

- Brinda acceso a la tecnología a zonas rurales.
- Ofrece la gratuidad de sus servicios.
- Está disponible para todos en general.
- Ofrece cursos de capacitación
- Incentiva a sus usuarios para que usen la tecnología.

Oportunidades

- Permite que sus usuarios puedan capacitarse continuamente.
- Se pueden hacer convenios con otras instituciones para ofrecer cursos de capacitación.
- Brindar cursos de capacitaciones de todo tipo.
- Puede captar nuevos servicios
- Integración con otras empresas del estado.

Debilidades

- La información que se maneja en el lugar podría ser vulnerada.
- No existen políticas de seguridad necesarias para salvaguardar la información
- No se toman las medidas de seguridad informática necesarias.
- La información puede ser robada o adulterada.
- Los equipos se pueden deteriorar.

Amenazas

- Si no se toman medidas los equipos de pueden deteriorar.

- La falta de seguridad puede provocar que los usuarios no asistan al lugar, por desconfianza.
- Fallas eléctricas pueden causar daños a los equipos.
- No disponibilidad de los servicios.
- Actualizaciones de software.

Sistema de gestión de seguridad de la información permitirá a la organización solamente tomar las decisiones respectivas para implantar mejores prácticas para garantizar la mejora de la seguridad de la red LAN y reconocer a su vez, el estado en que se encuentra la seguridad de la misma.

El presente caso de estudio no pretende realizar ningún tipo de cambios en las configuraciones en las topologías, enlaces o en los equipos, ni tampoco realizar la compra la compra de equipamientos adicionales como routers, switchs o modificaciones físicas en la infraestructura. Tampoco contempla cotizaciones especializadas de seguridad en redes LAN.

La metodología y la herramienta para hacer el estudio de los riesgos y vulnerabilidades en los equipos y red LAN del infocentro de San Juan son: La metodología MAGERIT en su versión 3.0 y el Software Pilar Versión 5.2.

El modelo de negocio de las empresas de hoy se está encaminando al uso de las tecnologías de la información y las comunicaciones (TIC), aumentando el uso de medios informáticos por parte de los usuarios y las probabilidades de ser vulnerables por medio de delincuentes informáticos, es por eso que las organizaciones buscan las alternativas para asegurar su información estableciendo políticas de seguridad en sus infraestructuras tecnológicas.

La información es el activo más valioso de las organizaciones y es por eso que debe ser protegida de una manera adecuada, ya sea que se encuentre en forma digital o física, porque no importa en la forma que se encuentre la información o el medio por el cual esta se almacenada o compartida esta debe siempre estar salvaguardada apropiadamente. (Velthuis, Mario, Garcia Rubio, & Muñoz Reja, 2017)

La seguridad informática es un conjunto de normas y procedimientos que son aplicados para salvaguardar un sistema informático. Su finalidad es garantizar que todos los recursos que conforman el sistema informático sean utilizados para el fin que fueron creados sin ninguna intromisión. (Areitio & Areitio, 2014)

Entre los principios de la seguridad informática tenemos:

Confidencialidad. -Es la capacidad que posee el sistema para evitar que personas y organizaciones no autorizadas puedan acceder a la información (González, 2010).

Integridad. -Hace referencia a la validez y consistencia de cada elemento de información que se encuentra almacenada en un sistema informático.

Disponibilidad. -Es una característica de la información que nos garantiza que esta se encuentra disponible, en el momento que sea requerida, para quien tiene la autorización de acceder a la información (Echenique García, 2014)

La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información.

Las políticas de seguridad informática son el conjunto de operaciones y lineamientos que se definen por parte de los administradores de la seguridad informática, para proteger los sistemas y también la información, es decir, son las especificaciones de lo que se puede o no hacer en las áreas de operación de los sistemas con el fin de proteger a los activos.

Un activo es todo lo que tenga valor para una organización. El más importante es la información que se gestiona en ella.

Los conceptos de vulnerabilidad, amenaza y riesgo están relacionados entre sí haciendo parte de la concepción de la seguridad en distintos ámbitos, que también han sido aplicados en referencia a la seguridad informática y de la información.

Una vulnerabilidad informática son las posibilidades que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la presencia de un factor que pueda posibilitar una amenaza o un ataque. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado. (Solarte, 2015)

Una amenaza informática está relacionada con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización. (Urbina Baca, 2016)

Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para

salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento. (Voutssas, 2010)

Las salvaguardas son las acciones de protección definidas para que la organización tome las decisiones en referencia a las amenazas encontradas en sus activos.

En la evaluación de los riesgos se identifican las vulnerabilidades que se encuentran en la red LAN de la institución y gracias a esto se determinan las causas potenciales de riesgos con el objeto de minimízalos. Para esto se siguen pasos generales para realizar la evaluación de los riegos: identificación y análisis de riesgos.

En la identificación de los riesgos se determinan los factores que se consideran como amenazas en el sistema de información, los cuales se identifican mediante encuestas a los administradores con el objetivo de descubrir las amenazas presentes en el ambiente informático.

En el análisis de los riesgos se realiza una predicción de lo que puede suceder en el futuro si no se toman las medidas necesarias en cuanto a las amenazas detectadas en la identificación de los riesgos, basándose en hechos estadísticos, con el objetivo de terminar el impacto, y tomando alternativas de solución.

La metodología MAGERIT es un método formal que sirve para investigar los riesgos que soportan los sistemas de información existentes en cada una de las organizaciones para recomendar las medidas apropiadas que poco a poco deberían adoptar todas las organizaciones.

Para realizar el estudio de los riesgos y vulnerabilidades de la red LAN y de los equipos del infocentro San Juan, siguiendo la metodología MAGERIT, el proceso se desarrolla en cinco fases las cuales se detallan a continuación:

Fase 1.- Activos.

En esta etapa se identifican los activos más relevantes de la organización objeto de estudio. Entre los activos más importantes que la metodología MAGERIT muestra las siguientes categorías:

- [HW] Hardware
- [SW] Software
- [D] Datos
- [L] Instalaciones.
- [P]m Personal, entre otros.

Fase 2.- Amenazas

En esta fase se procede a identificar las amenazas a los que se ven afectados, los activos que únicamente se aplicarán sobre los activos que estén debajo del nivel de la capa de datos o inferior. Además, en el catálogo de elementos de la metodología MAGERIT se hacen conocer algunos tipos de amenazas.

Fase 3.- Salvaguardas

Las salvaguardas son las contras medidas que se definen como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Herramienta EAR Pilar

PILAR es una herramienta EAR (Entorno de Análisis de Riesgos) que soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT. Las siglas de PILAR provienen de “Procedimiento Informático Lógico para el Análisis de Riesgos” creado por el Centro Nacional de Inteligencia. (Quirumbay & Johanna, 2019)

"PILAR contiene una biblioteca estándar y su función es de realizar valoraciones de seguridad informática de las empresas que manejan esta herramienta y permite realizar el Análisis y Gestión de Riesgos Informáticos en varias dimensiones (confidencialidad, integridad, disponibilidad y autenticidad); también realiza el Análisis de Impacto y Continuidad de Operaciones, donde se realiza el análisis de las interrupciones de servicio teniendo en cuenta la duración de la misma". (EAR/PILAR, 2013)

La versión que se utilizará será la 7.3.1 "Análisis y Gestión de Riesgos" – "Análisis Cualitativo" se escogió este tipo de análisis ya que permite realizar el análisis de los activos asignándoles un valor relativo; se trabajará con la herramienta a modo de prueba ya que no se cuenta con la licencia. (Quirumbay & Johanna, 2019)

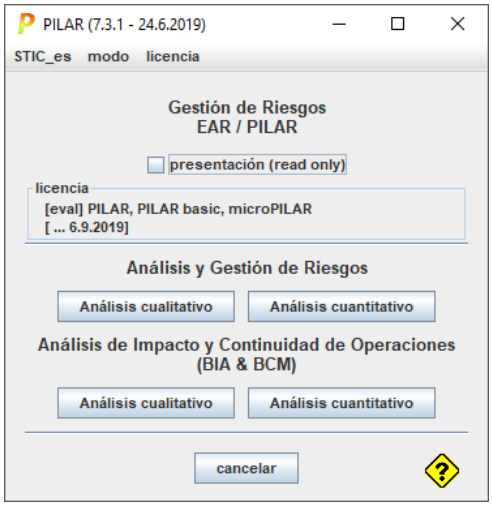


Fig. 1. Interfaz de EAR Pilar.

Creación de proyecto en pilar

A continuación, se inicia con las fases establecidas para el estudio de riesgos informáticos en los activos del infocentro de San Juan.

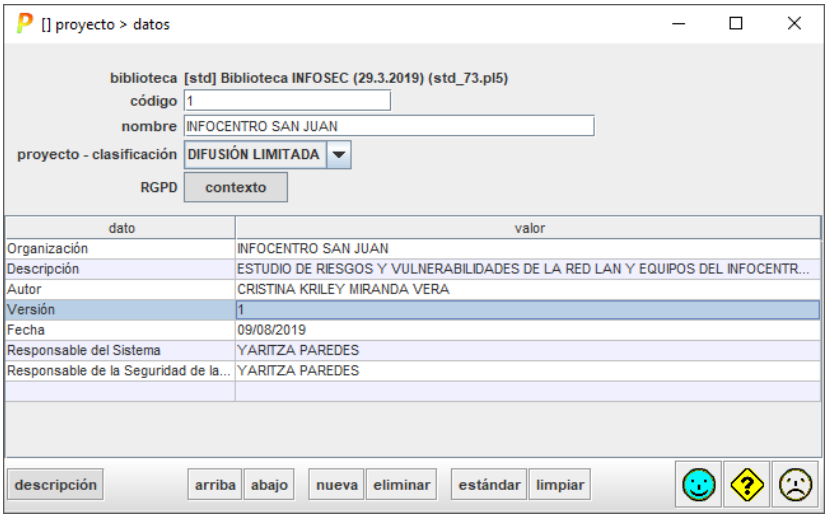


Fig. 2. Creación de proyecto de análisis en Pilas

Para la identificación de los activos se realizaron una serie de actividades tales como visitas a las instalaciones y utilizar diferentes técnicas para el levantamiento de información, entre ellas: la Inspección visual a las áreas de tecnología a la encargada del área del infocentro.

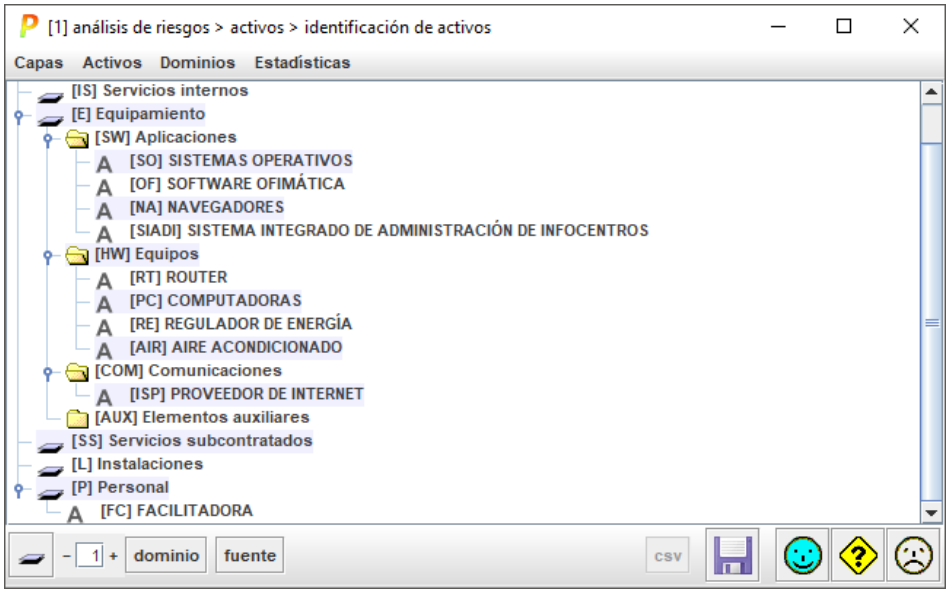


Fig. 3. Identificación de activos con Pilar

Se realizó un inventario de activos de los cuales los principales son:

[SO] SISTEMAS OPERATIVOS: Este activo agrupa al sistema operativo que está presente en todas las computadoras del infocentro en este caso es UBUNTU.

[OF] SOFTWARE OFIMÁTICO: Este activo agrupa todos los paquetes ofimáticos instalados en los terminales del infocentro y open office los cuales poseen sus respectivas licencias.

[NA] NAVEGADORES: Agrupa todos los navegadores instalados en los equipos del del infocentro como son: Mozilla Firefox y Google Chrome.

[SIADI] SISTEMA INTEGRADO DE ADMINISTRACIÓN DE INFOCENTROS: Es el sistema que gestiona los procesos que se realizan en el infocentro como registro de usuarios del mismo, uso de internet, gestión de cursos entre otros. Es una aplicación web que funciona solamente en los infocentros.

[RT] ROUTER: Dispositivo que se encarga de direccionar el tráfico de red hacia los terminales, cuenta con WIFI, el cual es repartido a todas las computadoras del infocentro las cuales cuentan con una antena para conectarse de forma inalámbrica. El router posee filtrado MAC.

[PC] COMPUTADORAS: Agrupa a todas las computadoras presentes en el infocentro. Existen ocho computadoras de las cuales dos están fuera de servicio.

[REGULADOR DE ENERGÍA]: Agrupa todos los reguladores de energía eléctrica que existen en el infocentros, así mismo existen 8.

[AIRE ACONDICIONADO]: Representa al aire acondicionado que ambienta el infocentro.

[ISP] PROVEEDOR DE INTERNET: Es el que brinda el servicio de internet al infocentro. Al ser este, empresa pública el proveedor es CNT.

[WIFI] RED INALÁMBRICA: Provee de internet sólo a los terminales del infocentro.

[LAN] RED LAN: Provee de internet al servidor que usa la faciliadora.

[FC] FACILITADORA: Es la persona encargada de supervisar al infocentro y brindar los servicios que la ciudadanía requiera en el mismo.

Valoración de activos

Después de ingresar los activos y clasificarlos se realiza la ponderación mediante un análisis cualitativo de los mismos. Se realiza la ponderación en base a cinco aspectos fundamentales que son:

"[I]" (INTEGRIDAD DE LOS DATOS): Que pondera el impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta.

"[C]" (CONFIDENCIALIDAD DE LOS DATOS): Que pondera el impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas.

"[A]" (AUTENTICIDAD DE LOS DATOS): Que pondera el impacto que tendría en la organización el hecho de que no se pueda saber a ciencia cierta quién ha accedido a la información que se maneja para prestar el servicio.

"[T]" (TRAZABILIDAD DE LOS DATOS): Que pondera el impacto que tendría en la organización el hecho de que no se pueda saber qué se ha hecho con la información que se maneja para prestar el servicio o no se pudiera conocer quién hace qué y cuándo con el servicio.

"[D]" (DISPONIBILIDAD): Que pondera el impacto que tendría en la organización el hecho de que se dejara de prestar el servicio.

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor

Tabla 1. Criterios de valoración de activos

En la categoría de equipos los activos más críticos son los terminales y la red LAN debido a que con ellos se presta el servicio a la ciudanía de internet y demás. Se puede observar también que estos tienen alta ponderación en cuanto a disponibilidad ya que son los activo que más usan los usuarios.

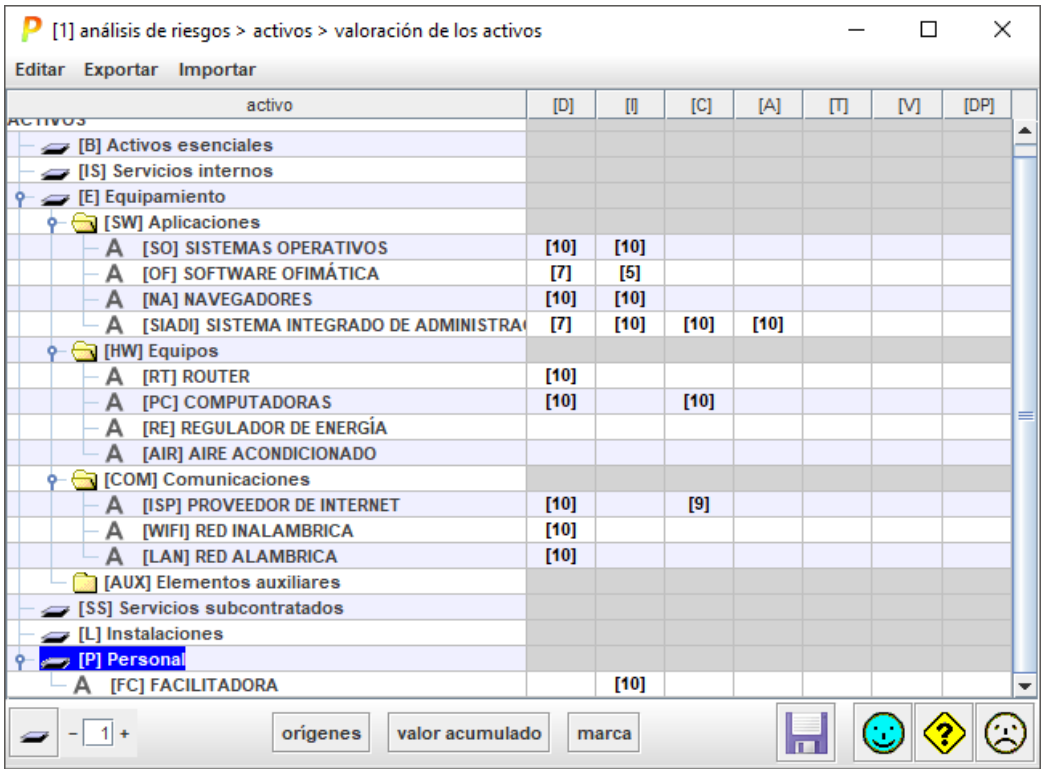
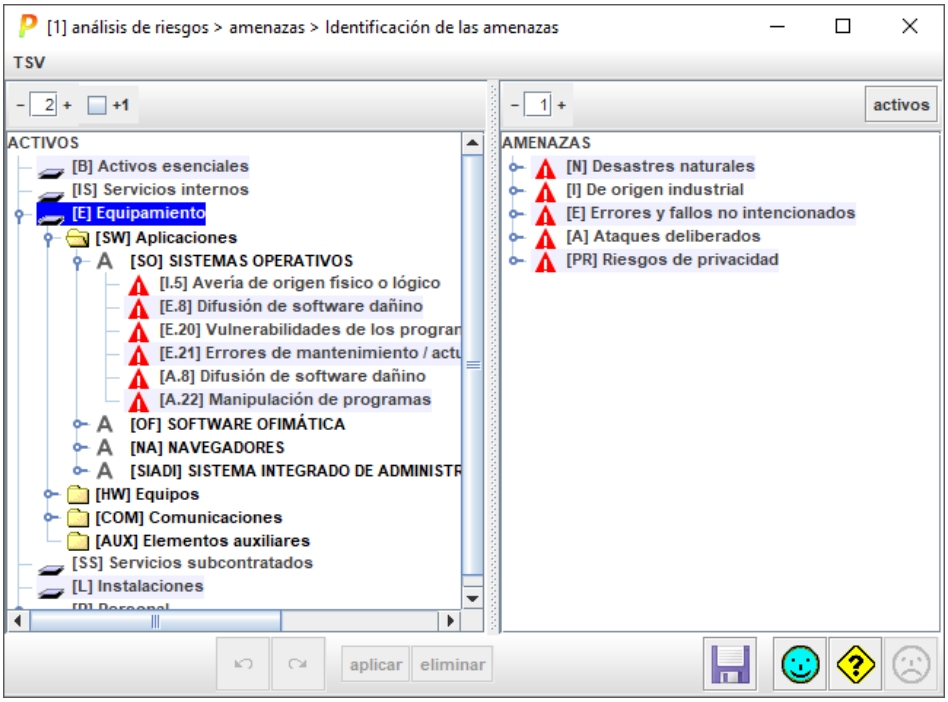


Fig. 4 Valoración de Activos.

Fase 2 amenazas



Frecuencia: Cuando una amenaza se valora, permite definir la posibilidad de que ocurra en función de la cantidad de veces que se puede materializar dicha amenaza en un año (esta es la opción por defecto) y se utilizó la siguiente escala:

Valor	Frecuencia
0,1 -	Una vez cada 10 años
1 -	Todos los años
10 -	Todos los meses
100 -	Todos los días

Tabla 2 valoración de frecuencia

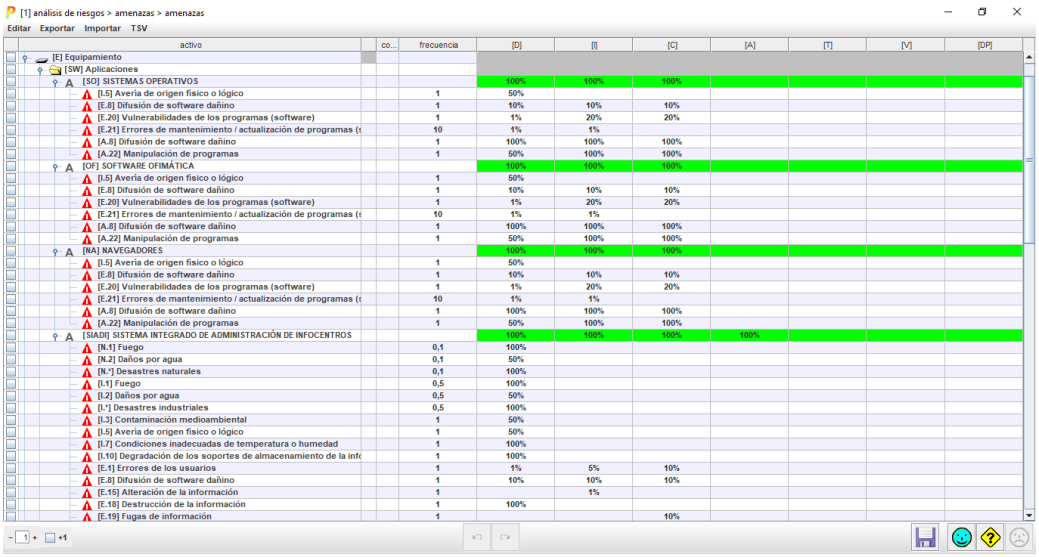


Fig. 5 Valoración de Amenazas

El activo que presenta mayores posibilidades de materialización de amenazas ya que el acceso no autorizado puede materializarse todos los días y tiene varias amenazas con frecuencia de 10 que significa que se pueden materializar en cada mes.

Con respecto a los activos de aplicaciones la amenaza más frecuente es los errores de mantenimiento o actualización de software debido a que se producirían cuando se realice mantenimiento programado sobre los equipos o por a una falla de las aplicaciones de los mismos.

Con respecto a los activos de equipos la amenaza más frecuente es la caída del sistema por agotamiento de recursos, ya que de estos los más esenciales como son los terminales y el router estos se encuentran a la vista de todos, por lo que la amenaza depende de la administración facilitadora.

En los activos de comunicaciones la amenaza más frecuente es la denegación de servicio ya que puede ocasionar la caída de servicios en diferentes partes de la empresa.

Con respecto a los activos de servicios internos las amenazas más frecuentes son la caída del sistema por agotamiento de recursos como se muestra ya que depende de los recursos del

equipo donde se encuentra instalado el servicio y denegación de servicio porque está expuesto a ataques software como hardware.

Identificación de Vulnerabilidades. La identificación de vulnerabilidades se realizó mediante una visita a las instalaciones para realizar una inspección visual de los activos, entrevistas con el personal encargado del manejo de los recursos informáticos y la utilización de herramientas de Nmap para el análisis de puertos abiertos.

Se procedió a la instalación de la herramienta en una de las terminales del Infocentro con previa autorización de la facilitadora. Se realizó el escaneo a toda la red con el objetivo de determinar si no existían intrusos en la misma.

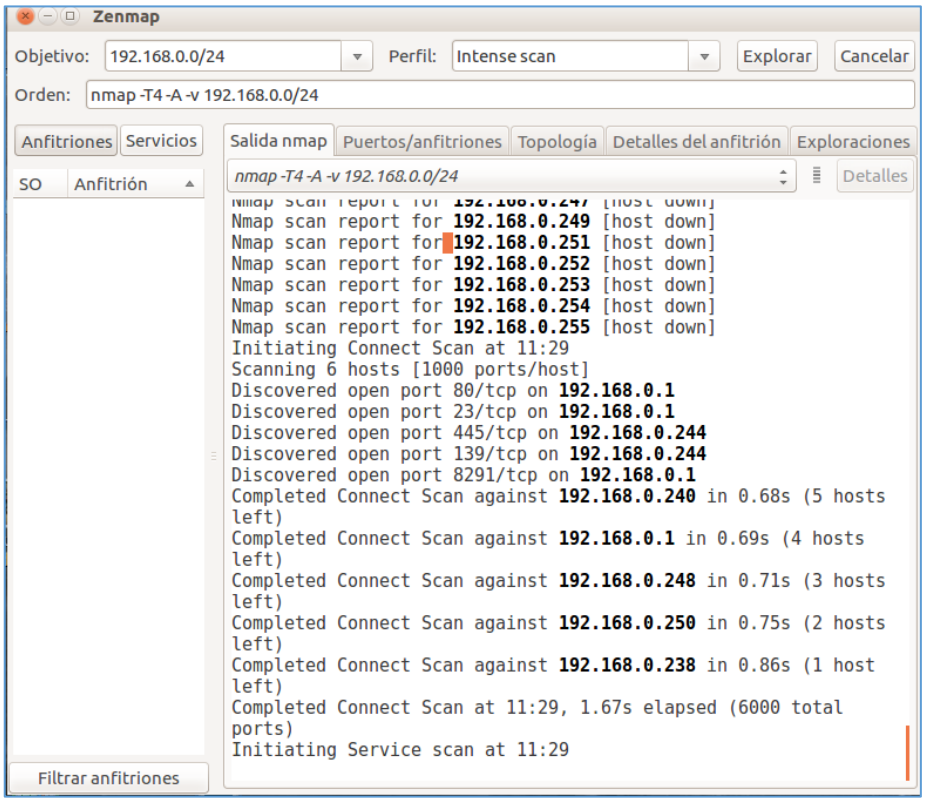


Fig. 6 Inicio de análisis en la red del infocentro

Como se muestra en la figura 6, la herramienta está realizando el escaneo de los equipos conectados en la RED. El proceso tardó diez minutos aproximadamente.

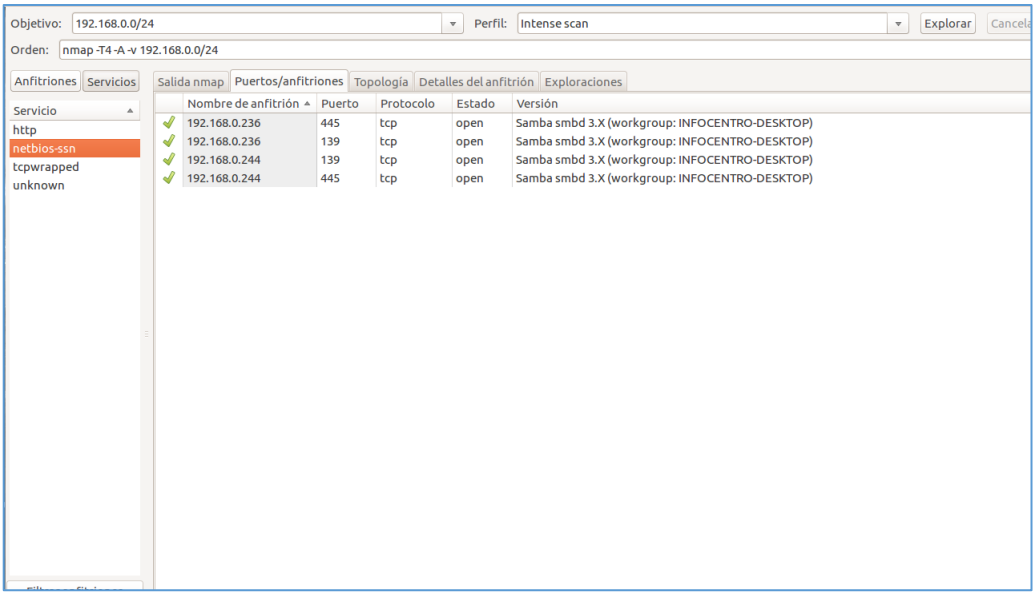


Fig. 7 Fin del escaneo

Al finalizar se pudo observar que no existen puertos peligrosos abiertos en la red del infocentro, solo están abierto los puertos esenciales para los servicios como mensajería y navegación WEB.

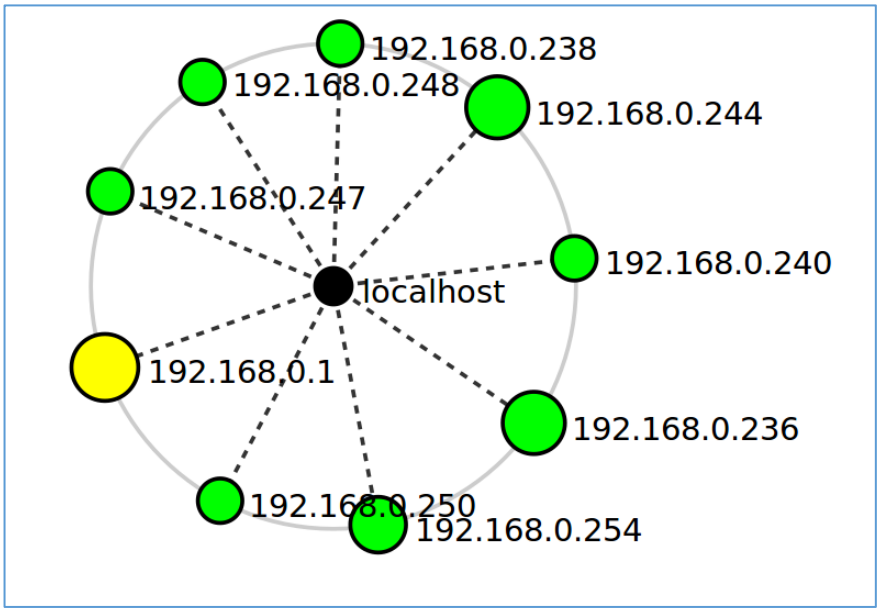


Fig. 8. Estado de la red del infocentro

El estado de la red del infocentros, como lo muestra la figura 8, demuestra que se encuentra segura sin vulnerabilidades existentes. Al tratarse del sistema operativo Ubuntu, permite al Infocentro tener una confiabilidad en el ámbito de amenazas informáticas ya que no

existen generalmente virus para estos sistemas operativos vasados en Linux, caso contrario como lo ocurre con sistemas operativos de Windows.

Fase 3 salvaguardas

El gestor del sistema de información dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

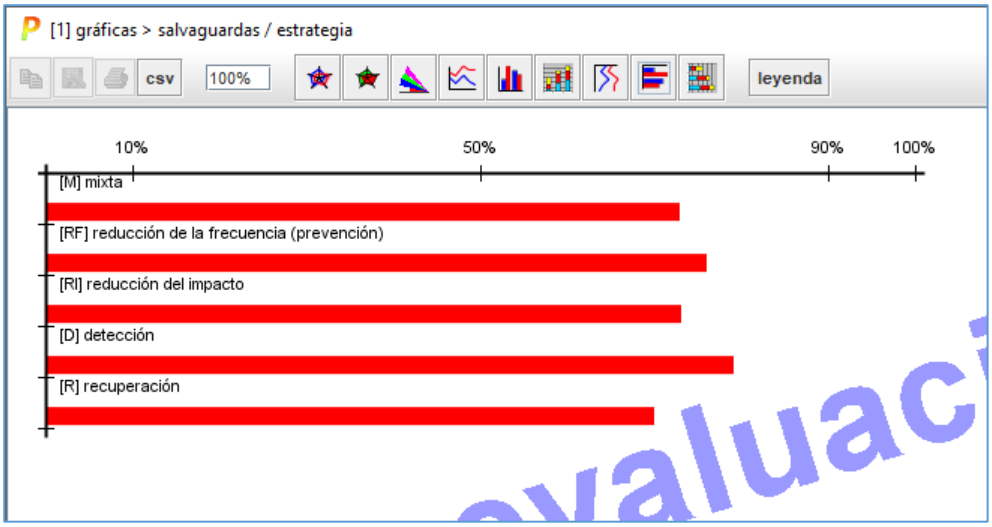


Fig. 9. Salvaguardas

A menudo encontrará muchas soluciones para un problema, con diferentes calidades. En estos casos debe elegir una solución proporcionada a los niveles de impacto y riesgo calculados. Las salvaguardas entran en el cálculo del riesgo de dos formas: Reduciendo la frecuencia de las amenazas. Según el grafico, el porcentaje de mitigar los riesgos físicos en la infraestructura del infocentro se reducen en un 85% aplicando las salvaguardas recomendadas por pilar.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

CONCLUSIONES

MAGERIT es una de las herramientas mas potentes para realizar análisis de riesgos debido que implementa a la normativa ISO/IEC 27001 la cual brinda los parámetros necesarios para mantener una infraestructura tecnológica segura.

En el infocentro de San Juan, se encontraron pequeñas fallas en la infraestructura física de la red. Luego de la recolección de datos se identificaron todas las amenazas que existen en el infocentro y se determino en que medida estas pueden afectar a los activos si no se toman las medidas necesarias.

El escaneo de la red se los realizo con Nmap la cual es una poderosa herramienta para la detección de vulnerabilidades que puede existir en la red. El resultado del escaneo fue favorable para el infocentro ya que no se encontraron mayores riesgos en la red de datos del lugar..

El resultado demostró que no existen vulnerabilidades que atenten a la seguridad de la misma, por lo que el infocentro hace uso de Ubuntu como sistema operativo, que es una de las ventajas de usar software libre basado en Linux, porque si bien es cierto ningún sistema operativo es totalmente seguro, las amenazas en contra de esto sistemas no son muy comunes.

Recomendaciones

Se recomienda implementar salvaguardas preventivas hasta que se implemente el plan de seguridad, con el objetivo de proteger a los activos del infocentro en todo tiempo.

Se recomienda implementar una política y procedimientos de gestión de seguridad tanto del personal que labora en el infocentro como de los usuarios que asisten al mismo.

Fomentar el hábito del uso de la seguridad informática por parte de todos los usuarios del infocentro, con el objetivo de crear políticas basadas valores éticos para formar usuarios responsables en el uso de la informática.

Bibliografía

Techopedia Inc. (2019). *Techopedia*. Obtenido de Threat: https://www.techopedia.com/definition/25263/threat

Areitio, G., & Areitio, A. (2014). *Información, Informática e Internet: del ordenador personal a la Empresa 2.0.* . Editorial Visión Libros.

Ariganello, E. (2016). *REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada.* Grupo Editorial RA-MA.

Conklin, W. A., & Shoemaker, D. P. (2013). *CSSLP Certification All-in-One Exam Guide.* McGraw Hill Professional.

Echenique García, J. A. (2014). Auditoría en informática. . *Compañía Editorial Continental*.

González, J. (2010). *Seguridad Informática*. Madrid. .

Hontañón, R. J. (2016). *Linux Security.* John Wiley & Sons.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard.* Artech House.

ISO27000 ESPAÑOL. (2015). *Control de Accesos*. Obtenido de http://www.iso27000.es/iso27002_9.html

ISO27000 Español. (2015). *El portal de ISO 27002 en Español*. Obtenido de Seguridad física y Ambiental: http://www.iso27000.es/iso27002_11.html

Ivan Mistrik, R. B. (2014). *Relating System Quality and Software Architecture*. Morgan Kaufmann.

Iviricu Roba, L. R., Alvarez Vento, J. R., & Concepción García, L. E. (2016). *Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux.* Pinar del Río.

Kapadia, A., Rajana, K., & Varma, S. (2015). *OpenStack Object Storage (Swift) Essentials.* Birmingham: Packt Publishing Ltd.

Kremling, J., & Parker, A. M. (2017). *Cyberspace, Cybersecurity, and Cybercrime.* SAGE Publications.

ltraReach Internet Corp. (2018). *Ultrasurf*. Obtenido de https://ultrasurf.us/about/

Luque, J. J., & Luque, D. B. (2016). *Montaje de infraestructuras de redes locales de datos. ELES0209.* IC Editorial.

Marian, Q. (2017). *Encyclopedia of Information Ethics and Security*. New York: Idea Group Inc (IGI).

Ministerio del Interior. (2014). *Policia Nacional.* Obtenido de MANUAL DE GESTIÓN ADMINISTRATIVA Y OPERATIVA: http://www.policiaecuador.gob.ec/wp-content/uploads/downloads/2014/06/INSTRUCTIVO-DE-CUIDADO-Y-MANTENIMIENTO-DE-UPC-36-PAGINAS-1.pdf

Pérez, P. M. (2016). *UF1879 - Equipos de interconexión y servicios de red.* Editorial Elearning, S.L.

Quigley, M. (2017). *Encyclopedia of Information Ethics and Security*. New York: Idea Group Inc (IGI).

Quirumbay, G., & Johanna, C. (2019). *Aplicación de la metodología Magerit para el análisis del riesgo informático al departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad utilizando la herramienta Pilar* . Libertad: Universidad de las Fuerzas Armadas ESPE. Carrera de Tecnología en Computación.

Richarte, J. (2018). Fundamentos de redes. *RedUsers*, 24 .

Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL 28(5).*

Study Academy. (2017). *What is Information Security? - Definition & Best Practices*. Obtenido de https://study.com/academy/lesson/what-is-information-security-definition-best-practices.html

TecNoincer. (2017). *ecNoincer*. Obtenido de https://www.tecnoinver.cl/uso-de-protocolos-seguros-para-la-transferencia-de-datos-en-internet/

Urbina Baca, G. (2016). *Urbina, G. B. (). Introducción a la seguridad informática.* . México: Grupo editorial PATRIA.

Urbina, G. B. (2016). *Introduccion a la Seguridad Informatica.* Mexico: Grupo Editorial Patria.

Velthuis, P., Mario, G., Garcia Rubio, F., & Muñoz Reja, I. C. (2017). Calidad de sistemas informáticos. *Alfaomega Ra-Ma,., 004*(05).

Voutssas, M. (2010). Preservación documental digital y seguridad informática. *nvestigación bibliotecológica, 24*(50), 127-155.

Walker, M. (2016). *CEH Certified Ethical Hacker All-in-One Exam Guide, Third Edition.* New York: McGraw Hill Professional.

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2014). *Building Internet Firewalls.* Sebastopol : O'Reilly Media, Inc.

Anexos.

Visita al lugar, para legalizar el permiso al infocentro para realizar el escaneo de la red.

Realización del escaneo de la red usando Nmap como herramienta.