UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2019 – MARZO 2020

EXAMEN COMPLEXIVO DE GRADO O FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCION DEL TITULO DE INGENIERA EN SISTEMAS

TEMA

Análisis de las vulnerabilidades del sistema informático del Almacén Credifacil de la ciudad de Montalvo.

EGRESADA

Lidia Maribel Vera Martínez

TUTOR

ING. Alfredo Cevallos Monar

AÑO 2020

INTRODUCCION

En el transcurso de los años se ha venido observando que la mayoría de las empresas tienen la necesidad de utilizar e implementar sistemas informáticos como una tecnología enmarcada en las actividades comerciales que desempeñan, de esta manera los sistemas informáticos se pueden ajustar a la necesidad que la empresa requiera, los mismo que realizan distintas funciones para obtener un mejor control en los movimientos financieros que se llevan a cabo en la empresa.

Los sistemas informáticos son muy conocidos en la actualidad y a su vez de gran importancia en la sociedad, especialmente en el entorno donde se requiere el manejo de información. La implementación de un sistema informático debe abarcar las medidas de seguridad adecuadas que protejan a los datos almacenados de cualquier situación de vulnerabilidad, esto serán las buenas prácticas de seguridad que deben implementar las empresas.

Por tal motivo se pretende a través de esta información proporcionar un contenido equilibrado al estudio de caso que se enmarca en el análisis de vulnerabilidades del sistema informáticodel almacén CREDIFACIL de la Ciudad de Montalvo para obtener la información necesaria, para el desarrollo de este tema primeramente se realizo una entrevista a la persona encargada de las Tic, en la cual se pudo obtener los lineamientos necesarios a seguir en el proceso investigativo.

Con el incremento del uso de nuevas tecnologías en las empresas y la aparición de los problemas de seguridad, hoy en día es muy importante la utilización de técnicas que permitan controlar la seguridad de los mismos ya que un mal funcionamiento en el sistema informático puede causar pérdidas económicas para la empresa. Por tal razón se decidió estructurar una guía técnica que permita conocer los comportamientos que posee el sistema informático del almacén CREDIFACIL de la ciudad de Montalvo en el momento que se presenten incidencias dentro de la institución, de la misma manera identificar cuáles son los tipos de vulnerabilidades que puedan causar algún tipo de daño al sistema informático.

Para la elaboración de la presente investigación se utilizo la metodología de investigación de campo ya que esta permite la recopilación de información necesaria mediante la entrevista en la cual se pudo deducir las principales vulnerabilidades existente en el sistema informático de la empresa y así lograr cumplir con el objetivo planteado que trata sobre el análisis de vulnerabilidades existentes en el sistema informático del almacén credifacil de la Ciudad de Montalvo.

El desarrollo de este estudio de caso se centra en el almacén credifacil con matriz principal en Montalvo y cuenta con sucursales ubicadas en Caluma, San Miguel y Babahoyo, se utilizo como campo investigativo el almacén matriz en el cual se desempeña actividades de cobranzas y ventas de electrodomésticos, bicicletas, motos y maquinaria forestales ofreciendo una forma de pago ya sea al contado o a crédito.

DESARROLLO

La empresa CREDIFACIL está ubicada en la calle Babahoyo y 24 de mayo de la ciudad de Montalvo Provincia de los Ríos, es una entidad dedicada a las actividades de cobranza y venta de electrodomésticos, bicicletas, motos y maquinaria forestales ofreciendo una forma de pago ya sea al contado o a crédito. En muy poco tiempo esta empresa ha podido establecer tres sucursales en el país ubicadas en la ciudad de Caluma, San Miguel y Babahoyo, así poco a poco ha crecido y logrado ubicarse como una empresa que brinda artículos de calidad que satisfacen las necesidades de sus clientes.

En la actualidad las organizaciones tienen la necesidad de valerse por sistemas de información los mismos que son utilizados para almacenar, procesar y distribuir la información, por tal razón se ha convertido en un recurso primordial en las empresas (Ciza Acero & Bolaños Burgos , 2014)

La problemática presentada en el sistema informático del almacén credifacil de la ciudad de Montalvo surgió a través de que la información obtenida en el sistema informático es bastante sensible y de alta confidencialidad en especial de los proveedores y clientes , durante la entrevista realizada a la encargada de la administración del almacén se pudo constatar que en los últimos meses se han presentado fallas en el sistema informático ya que estos están propenso a robo de la información y son muy vulnerables a la existencia de virus ya que estos no cuentan con la seguridad adecuada.

Debido al problema antes mencionado se ha tomado en cuenta algunos objetivos específicos de los cuales tenemos como primer punto identificar la razón por la cual el sistema informático puede presentar algún tipo de riesgo, para luego determinar las causas actuales que provocan fallos existentes y por ultimo conocer las vulnerabilidades que provocan interrupciones y fallos en el sistema informático de la empresa, con la finalidad de de plantear el objetivo que engloba este caso de estudio que es analizar las vulnerabilidades del sistema informático del almacén credifacil de la ciudad de Montalvo.

La función del departamento de sistemas es la de estructurar sus servicios y proyectos con base a requerimientos específicos presentados en la empresa, apoyándose en la tecnología de vanguardia disponible y que está a su alcance pero se debe acotar que el área de sistemas no cuenta con asesoramiento en materia de seguridad informática, no han realizado evaluaciones a la seguridad informática y por lo tanto no existen políticas formales de seguridad.(Gil Vera & Gil Vera, 2017).

El escenario propuesto para el desarrollo de este estudio de caso son las instalaciones del almacén credifacil de la ciudad de Montalvo, en la cual se centro específicamente en el área administrativa en donde se realizan las actividades de venta y cobranzas.

Un sistema informático es el conjunto de partes interrelacionada como hardware, software y la parte de los recursos humanos que permite almacenar y procesar información, un sistema informático.(Arias Buenaño, Merizalde Almeida, & Noriega Garcia, 2013).

Una definición clara de las partes relacionadas del sistema informático son el hardware consiste en el equipo físico de la computadora, el software es una colección de programas en la computadora y datos relacionados diseñado para operar en el hardware y las personas son las encargadas de la utilización del sistema existente en la empresa.

La seguridad informática no se resume en la implementación de herramientas tecnológicas como el firewalls y antivirus, las contramedidas deben de aportar a la mitigación de riesgos y amenazas de manera efectiva deben de ser parte de una adecuada cultura en el manejo de información (Astudillo, Carvajal, Carvallo, & Orellana, 2018).

Para conocer los riesgos de seguridad en una empresa hay muchas normas, prácticas y métodos disponibles para la realización del análisis de vulnerabilidades, para la selección correcta depende de las normas, leyes o reglamentos que se tenga implementado dentro de la empresa, cada institución tiene la libertad de aplicar las normas específicas para lograr un buen cumplimiento de normativas, un ejemplo en particular es la utilización de una norma general de diligencia como es la de la Organización Internacional de Normalización (ISO) 17799, es una norma que ofrece recomendaciones para realizar la debida gestión de seguridad dirigida a las personas responsables de iniciar, implantar o mantener la seguridad en una empresa, esta norma a su vez puede ser costosa y no garantiza que los problemas de seguridad en una empresa sean abordados.

La norma ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de seguridad de la información dirigida a las personas responsables de iniciar, implantar y mantener la seguridad de una organización (Villalon Huerta , 2004).

Un análisis de vulnerabilidades es el que consisteen evaluar los fallos o brechas de la confidencialidad, la disponibilidad y la integridad de un activo (Loaiza Alvarez & Patiño Gomez)

La metodología OCTAVE-S utiliza una valoración para evaluar los riesgos basados en los activos los cuales deben de ser considerados cuidadosamente sobre las vulnerabilidades organizacionales y tecnologías que ponen en riesgo al grupo de activos. Mientras que COBIT versión 4.1 describe la situación de la empresa utilizando matriz de madurez, en la tabla 1se puede observar un cuadro comparativo entre la metodología OCTAVE-S, la norma ISO 17799 y la herramienta COBIT versión 4.1, ver anexo 1.

Luego de analizar las tres metodologías expuesta en este estudio de caso se escogió la metodología OCTAVE-S para implementarlo en la empresa credifacil de la Ciudad de Montalvo, ya que esta se adapta mejor al tamaño, necesidad y resultados que requiere la empresa.

Par realizar un análisis a cerca de las vulnerabilidades del sistema informático se utilizo el método OCTAVE-S (Riesgo critico operacional, evaluación de activos y vulnerabilidades), que es una metodología de análisis de riesgos, la cual se basa en tres principios que son la confidencialidad, integridad y la disponibilidad (Marban Cabrera, Echeverria Chan, Laguna Lopez de Nava, Navarrete Prieto, & Diaz Rincon, 2018).

Considerando la utilización de la metodología octave-s, primeramente se inicio con una visión clara de la organización, es decir se realizo un análisis de la situación actual de la empresa en donde se identifico cada una de las áreas que la conforman, esta información se pudo obtener realizando una entrevista a la persona encargada del almacén credifacil, la cual se pudo constatar que dicha empresa realiza actividades de cobranza y venta, además que las computadoras están conectadas a internet.

Para realizar la correcta evaluación con OCTAVE-S dentro del almacén CREDIFACIL se definió un equipo de trabajo conformado por la persona encargada de las TIC.

El proceso de octave consta de dos partes fundamentales que se describen a continuación:

- Se deberá identificar el perfil de riesgo, es decir, las amenazas y vulnerabilidades presentes en la empresa los cuales afectan directamente a los activos.
- Se realizara un análisis del riesgo encontrado como resultado del riesgo descrito anteriormente para así desarrollar las estrategias adecuadas.

Según lo mencionado anteriormente la metodología octave consta de tres fases sin antes contar con la fase de preparación.(Pintado Cuji & Hurtado Valero)

Fase 1: construir perfiles de amenazas basados en los sistemas informáticos, en esta fase se realiza una evaluación de la visión organizacional de la empresa, también se debe identificar los sistemas informáticos de mayor importancia para evaluar la información actualmente, ver anexo 2.

En esta fase se realiza una evaluación de los aspectos organizacional donde el equipo de trabajo define el impacto de los criterios de la evaluación que se utilizará para realizar una evaluación de riesgos, también se identificarán cuales son los activos organizacionales y se evaluarán las prácticas de seguridad que se practican actualmente en la empresa, ver anexo 3.

En la tabla del anexo 3 se estableció criterios de evaluación sobre el impacto que se da dentro del almacén credifacil a cerca de la seguridad personal de las personas que forman parte de dicha organización.

En la tabla del anexo 4 se identifico los activos organizacionales de la información, sistemas y aplicaciones, dentro de la actividad 2 del proceso 1. Se detalla los activos utilizados en la empresa además se observó que las computadoras personales son comunes a todos los sistemas y funcionan como un conducto para toda la información electrónica importante.

Fase 2: Identificar vulnerabilidades de la infraestructura, en esta fase se evalúa la seguridad de la infraestructura del sistema informático es decir la forma de cómo está la infraestructura, quienes acceden y quiénes son los responsables del mantenimiento e infraestructura, ver anexo 5.
En la tabla 7 se puede observar las vulnerabilidades que pueden causar riesgos a la infraestructura de los activos, ver anexo 6.

Fase 3: Desarrollo de planes y estrategias de seguridad, en esta fase se obtiene los riesgos a los que el sistema informático está expuesto, basándose en la información recopilada de la fase anterior, ver anexo 7.

En la tabla 9 se muestra los resultados según el nivel de confianza este nos permite conocer que tan confiado se está de que una amenaza se vuelva a dar en un futuro, además que puede medir el valor mediante el impacto ocasionado en los activos de la empresa, ver anexo 8.

El uso de la metodología OCTAVE propone dividir en dos grupos el primero es los activos en el cual uno se basa en el sistema como el hardware, software y datos que encontramos en el sistema, y el segundo grupo son las personas que laboran y los encargados del acceso al sistema de la empresa.

El área administrativa dentro del almacén CREDIFACIL es un lugar muy importante para el desenvolvimiento de la empresa ya que esta es la encargada de gestionar actividades como registros de ventas y cobranzas, es decir cualquier problema que se presente en esta área por mínimo que sea, esta representaría un serio problema y se reflejaría un problema para la empresa.

La persona responsable del área de las TI dentro de la empresa se encarga de solucionar a la brevedad posible todos los problemas de virus o fallas existentes en el sistema informático. El mantenimiento de la red, las computadoras, reinstalación de sistemas operativos, instalaciones y actualizaciones de software o programa se realiza mensualmente con el propósito de no obstaculizar las actividades de los empleados en el horario laboral.

Actualmente poseer un sistema informático web es algo muy común y esencia dentro de todas las empresas e instituciones ya sean públicas o privadas de tal manera que les ayuda en agilitar los procesos de cada uno de sus departamentos asimismo le ahorra tiempo y se da un mejor servicio a la ciudadanía y consumen menos recurso que los de escritorio.

El sistema llamado Webconta que es un sistema web de contabilidad general del almacén CREDIFACIL, ver anexo 9. Este sistema web está diseñado en php que es un lenguaje informático utilizado para escribir páginas web y darle forma, además es un lenguaje gratuito en Open Source, lo cual significa que cualquiera puede usarlo para la creación de sitios web (Suarez, 2019).

Para conocer las vulnerabilidades del sistema del almacén CREDIFACIL se utilizó la herramienta NMAP que es una herramienta gratuita de código abiertos para la exploración de vulnerabilidades y la detección de redes. Los administradores de red utilizan NMAP para conocer que dispositivos se están ejecutando en sus sistemas, descubrir los host disponibles y los servicios que ofrecen, encontrar puertos abierto y detectar riesgo en la seguridad del sistema (Marin de la Fuente, 2019)

La herramienta Zenmap es una interfaz gráfica que permite manejar Nmap de una manera sencilla, en donde podemos averiguar que puertos están abiertos, a veces el sistema operativo que utiliza.

Al momento de realizar el análisis respectivo utilizando la herramienta Zenmap en el sistema utilizado en el almacén se pudo obtener los puertos vulnerables propensos a riesgos en la imagen 1 se puede observar los resultados obtenidos luego del análisis respectivo utilizado, además en la tabla 10 se muestra una breve descripción de los puertos abiertos los cuales hacen que el sistema informático sea vulnerable a cualquier riesgo ocasionando perdida de información o perdida al almacén. Ver anexo 10

CONCLUSION

Luego de analizar la problemática existente en el sistema informático del almacén CREDIFACIL de la ciudad de Montalvo, se pudo llegar a la siguiente conclusión:

El sistema informático comprende la parte del hardware, software y el personal, para la realización del análisis de las vulnerabilidades se utilizo la metodología OCTAVE-S para analizar la parte física (hardware y el personal de la empresa) y la herramienta NMAP para analizar el software.

Para conocer que metodología se debería implementar en este estudio de caso se realizo una comparación en donde se evaluó COBIT 4.1, ISO 17799 y OCTAVE-S para realizar un análisis de riesgo en la organización, la utilización de OCTAVE-S, fue la más acertada considerando el tamaño de la empresa, el número del personal, el trabajo que desempeñan y el tipo de negocio que desarrollan en la empresa.

La estructura de OCTAVE-S fue de fácil aplicación una vez que se tuvo en claro las diferentes fases de la metodología, los procesos que se desarrollan en cada fase y las distintas hojas de trabajo para recolectar información de cada proceso.

En el almacén CREDIFACIL la parte del software se pudo conocer los puertos que están vulnerables en los cuales puede existir algún tipo de amenazas que puedan causar daños y pérdidas en el sistema a su vez a la empresa.

Se debe hacer conocer a todo el personal de la empresa el plan de mitigación y hacer que el personal asista a cursos sobre seguridad de tal manera que todos tengan conocimiento y sepan cómo actuar en caso de que se presente una amenaza a cualquier riesgo en la empresa.

Para evitar algún inconveniente con el manejo de software que cuando se realice cambio de personal, se debe tener una capacitación previa sobre el manejo del sistema de acuerdo a su rol a desempeñar para que de esta manera no se les dificulte el manejo del sistema.

El sistema WebConta es un sistema web que necesita de una conexión a internet es necesario tener un buen proveedor de internet para que de esta manera tenga un quede colgando ha demás cabe recalcar que en lo que corresponde a la electricidad es constantemente que se les sabe ir y esto dificulta.

BIBLIOGRAFÍA

Arias Buenaño, G., Merizalde Almeida, N., & Noriega Garcia, N. (2013). Analisis y solucion de las vylneravilidadesde ls sefuridad informatica. 9.

Astudillo, C., Carvajal, F., Carvallo, J. P., & Orellana, M. (2018). Acometer contra un ERP con software libre. *Scielo*.

Ciza Acero, M., & Bolaños Burgos , F. (2014). Las implementaciones de las normas de seguridad de la información. *Recive*.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informatica organizacional: un modelo de simulacion basado en dinamica de sistema. *Redalyc.Org*, 195.

Loaiza Alvarez, J. D., & Patiño Gomez, J. G. (s.f.). Herramientas para el analisis de vulnerabilidades. *Sena*.

Marban Cabrera, M., Echeverria Chan, I., Laguna Lopez de Nava, I. G., Navarrete Prieto, J. A., & Diaz Rincon, H. (2018). Implementacion de la metodologia OCTAVE para el diagnostico de seguridad informatica. *Arista*, 10.

Marin de la Fuente, J. (2019). Nmap mapeador de red. *hangar18*.

Pintado Cuji, K. A., & Hurtado Valero, C. L. (s.f.). Diagnostico de las vulnerabilidades informatica en los sistemas de informacion. *Diagnostico de las vulnerabilidades informatica en los sistemas de informacion para proponer soluciones de seguridad a la rectificadora Gabriel Mosquera*. Universidad Politecnica Salesiana, Guayaquil.

Suarez, M. (2019). Que es PHP. *Superprof*.

Villalon Huerta , A. (2004). *Codigo de buenas practicas de seguridad UNE-ISO/IEC 17799.* S2 Grupo.

ANEXOS

Anexo 1: (Cuadro comparativo entre la metodología de análisis)

	OCTAVE – S	ISO 17799	COBIT 4.1
DEFINICION	Se aproxima al manejo de riesgo de seguridad contiene técnicas, métodos de evaluación. Es aplicada para pequeña empresas.	Norma internacional que ofrece recomendaciones para la seguridad de la información.	Utilizada para el manejo de información mediante la investigación permitiendo que las empresas tengan mejores resultados.
CARACTERISTICAS	➢ Relaciona amenazas y vulnerabilidades. ➢ identifica recursos importantes ➢ Evalúa riesgos	➢ Minimiza los daños a la empresa ➢ Desarrolla normas de seguridad.	➢ Cumplimiento de leyes, reglamento y acuerdos. ➢ Mantiene información de calidad para las decisiones.
IMPLEMENTACION	Se divide en tres fases **Fase 1:** Construir perfiles de amenazas basados en los activos **Fase 2:** Identificar vulnerabilidades de la infraestructura **Fase 3:** Desarrollo de planes y estrategias de seguridad.	➢ Auditoria ➢ Consultoría ➢ implantación	Identifica aéreas de enfoque Crea perfiles de amenazas. Elabora herramientas de apoyo (matriz de madurez)
RESULTADOS	➢ Estrategia de protección que definen el rumbo de la empresa ➢ Lista de acciones a corto plazo	Certificación ISO 27001: Requisitos para establecer y mejorar un Sistema de Gestión de la Seguridad de la información.	Certificaciones: CISA, CISM, CRISC

Tabla 1: Comparación entre la metodología OCTAVE-S, la norma ISO 17799 y la herramienta COBIT versión 4.1
Elaborado por: Lidia Vera Martínez

Según lo expuesto en la tabla comparativa de la tabla 1 se pudo deducir que el método OCTAVE-S se adapta al entorno de riesgo de la empresa, el cual se centra en conocer las vulnerabilidades que se presentan en el sistema informático, pero esta metodología se enfoca mas en las personas y la parte física.

Anexo 2: (Fase 1, Metodología Octave)

FASE 1	PROCESO	ACTIVIDAD
Construir perfiles de amenazas basados en los activos.	**P1:** Identificar la información organizacional	**A1:** Establecer los criterios de evaluación
		A2: Identificar activos organizacionales
		A3: Evaluar las prácticas de seguridad
	P2: Crear perfiles de amenazas	**A1:** selección activos críticos
		A2: Identificar requerimientos de seguridad
		A3: Identificar amenazas a los activos críticos

Tabla 2: proceso y actividades implementadas en la fase 1, Metodología Octave

Elaborado por: Lidia Vera Martínez

Anexo 3: (Impacto del criterio de evaluación, Fase 1)

TIPO DE IMPACTO	BAJO	MEDIO	ALTO
VIDA	Existen perdidas o amenazas significativa de la vida del personal	La vida del personal se ve amenazada	No han existido perdidas de vida del personal dentro de la institución.
SALUD	Degradación mínima o inmediatamente tratable dentro de la empresa	Discapacidad temporal o temprana o recuperable del personal	No ha existido deterioro permanente de la salud del miembro del personal
SEGURIDAD	Seguridad cuestionada	Seguridad afectada por el ingreso de virus al sistema	No existe seguridad violada es decir no se ha producido ningún tipo de robo de la información de la empresa.

Tabla3: Impacto del criterio de evaluación, actividad 1 del proceso 1 en la empresa

Elaborado por: Lidia Vera Martínez

Anexo 4: (Identificación de activos organizacionales)

SISTEMA	INFORMACIÓN	APLICACIONES Y SERVICIOS	OTROS ACTIVOS
¿Qué sistemas necesita para realizar su trabajo en la empresa?	¿Qué información necesita para realizar su trabajo?	¿Qué aplicaciones y servicios necesita para realizar su trabajo?	¿Qué otros activos están relacionados directamente con estos activos?
Computadoras personales y de escritorio	Pagos Presupuestos	Correo electrónico Acceso a internet	periféricos
Servidor de correo electrónico	Información de correos Información de clientes	Acceso a Internet	Computadoras personales y de escritorio
Servidor Web (Portal de Gerencia)	Información de la empresa Información de clientes Presentaciones, Documentos Gerenciales	Acceso a Internet	Computadoras personales y de escritorio

Tabla 4: Identificación de activos organizacionales: Información, Sistemas y Aplicaciones, dentro de la actividad 2 del proceso 1

Elaborado por: Lidia Vera Martínez

Anexo 5: (Fase 2, Metodología Octave)

FASE	PROCESO	ACTIVIDAD
Identificar vulnerabilidades de la infraestructura	**P3:** Examinar la infraestructura del sistema informático	**A1:** Examinar rutas de acceso
		A2: Analizar procesos relacionados con la tecnología

Tabla 6: Procesos y actividades implementados en la fase 2, Metodología Octave

Elaborado por: Lidia Vera Martínez

Anexo 6: (Vulnerabilidades de la infraestructura)

AMENAZAS	RESULTADOS
Defecto de software	No ha existido software mal instalados o sin actualizar
El sistema se cae	Sin acceso al sistema ocasionando detención de las operaciones
Defecto del hardware	No hay existencia de defectos en el hardware
Código malicioso	Existencia de virus que afectan el sistema ocasionando perdida de información
Problemas con el suministro de energía	Existencia de descargas eléctricas poco frecuentes
Problema de telecomunicaciones	Sin acceso a internet no se puede utilizar el sistema
Desastres naturales	No han existidos amenazas por desastres naturales

Tabla 7: Identificar vulnerabilidades de la infraestructura fase 2, Metodología Octave

Elaborado por: Lidia Vera Martínez

Anexo 7: (Fase 3, Metodología Octave)

FASE	PROCESO	ACTIVIDAD
Desarrollo de planes y estrategias de seguridad	**P4:** Identificar y analizar los riesgos	**A1:** Evaluar pactos de las amenazas
		A2: Establecer criterios de evaluación
		A3: Evaluar probabilidades de amenazas
	P5: Desarrollar estrategias de protección	**A1:** Describir las estrategias de protección actual
		A2: Identificar cambios en la estrategia de protección

Tabla 8: Procesos y actividades implementados en la fase 3, Metodología Octave

Elaborado por: Lidia Vera Martínez

Anexo 8: (Nivel de confianza de las amenazas)

AMENAZAS	RESULTADOS	VALOR	CONFIANZA		
			MUY	ALGO	NADA
Defecto del Software	Revelación	B	X		
	Modificación	M	X		
	Perdida	B	X		
	Interrupción	B	X		
El sistema se cae	Revelación	B	X		
	Modificación	A	X		
	Perdida	M	X		
	Interrupción	A	X		
Defectos del hardware	Revelación	B	X		
	Modificación	A	X		
	Perdida	M	X		
	Interrupción	A	X		
Código malicioso	Revelación	A	X		
	Modificación	A	X		
	Perdida	A	X		
	Interrupción	A	X		
Problemas con el suministro de energía	Revelación	B		X	
	Modificación	M		X	
	Perdida	M		X	
	Interrupción	A		X	
Problemas de telecomunicaciones	Revelación	B		X	
	Modificación	M		X	
	Perdida	A		X	
	Interrupción	A		X	
Desastres naturales	Revelación	B		X	
	Modificación	M		X	
	Perdida	M		X	
	Interrupción	A		X	

Tabla 9: Resultados en que tan seguro se está de que ocurra una amenaza.

Elaborado por: Lidia Vera Martínez

Anexo 9: (Sistema Webconta, sistema web de contabilidad general)

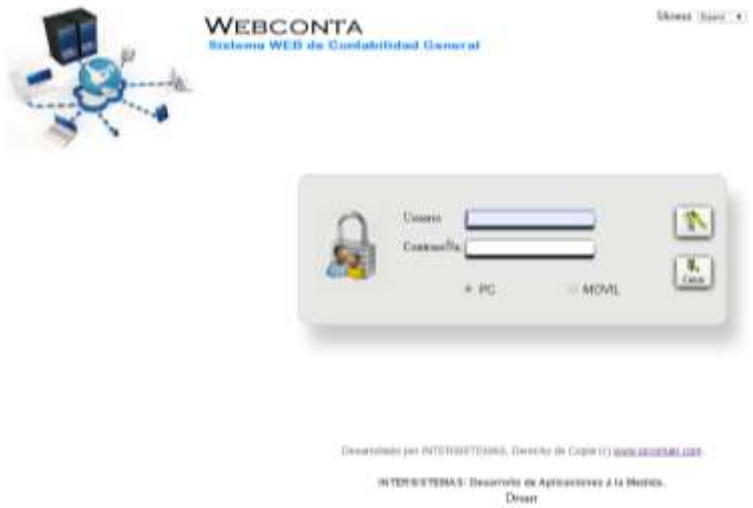

Imagen 1: Pantalla principal del sistema utilizado en el almacén CREDIFACIL de la Ciudad de Montalvo

Elaborado por: Lidia Vera Martínez

Anexo 10: (Análisis con ZENMAP y descripción de puertos)

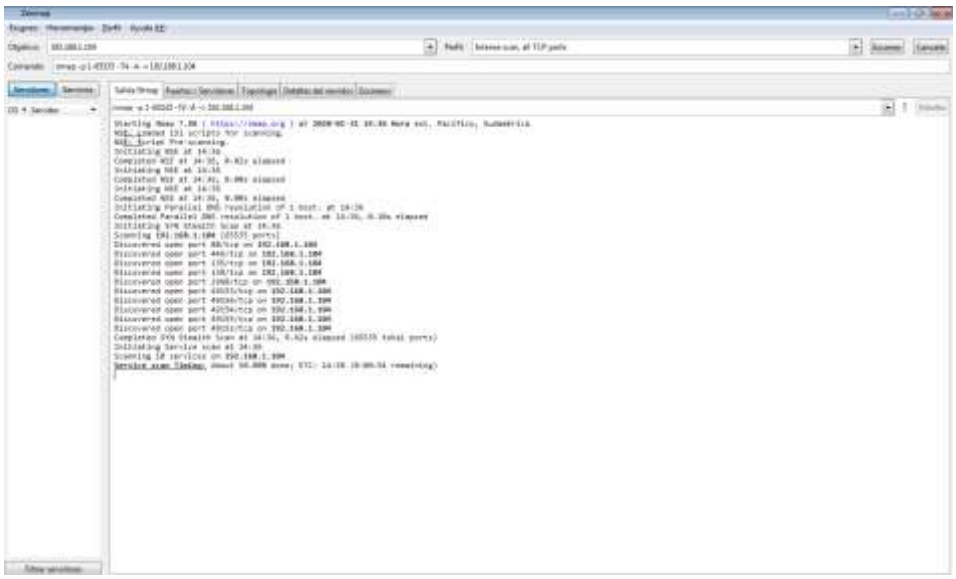

Imagen 2: Resultados del análisis realizado para conocer los puertos abiertos en el sistema

Elaborado por: Lidia Vera Martínez

PUERTOS ABIERTOS	DESCRIPCION
80/tcp	Servidor web con el que se puede acceder a páginas web. Con este abierto, el usuario se puede conectar con programas de chat como el Messenger.
445/tcp	El sistema operativo los abre para permitir su empleo de diversas aplicaciones
135/tcp	
139/tcp	Puerto utilizado por troyanos para acceder al ordenador
2968/tcp	Pueden ser utilizados por cualquier aplicación

Tabla 10: Descripción de puertos abiertos encontrado con ZENMAP.

Elaborado por: Lidia Vera Martínez

Anexos 11 formato de entrevista a la encargada de la administración del almacén credifacil de la ciudad de Montalvo.

Entrevista

La presente entrevista fue realizada a la encargada de la administración del almacén credifacil de la ciudad de Montalvo. Esta entrevista se realizo con el objetivo de obtener información acerca de las normativas y funcionamiento del sistema de la empresa cuyos resultados se utilizara como soporte al estudio de caso "ANÁLISIS DE LAS VULNERABILIDADES DEL SISTEMA INFORMATICO DEL ALMACEN CREDIFACIL DE LA CIUDAD DE MONTALVO perteneciente a la Egresada Srta. Lidia Maribel Vera Martínez de la carrera de sistemas de la Universidad Técnica de Babahoyo.

Cuestionario:

1. Cuál es la principal función del sistema?

La principal función del sistema en el almacén credifacil es realizar actividades de ventas y cobranzas.

2. ¿Cuáles han sido los principales errores que se han presentado?

Entre los errores que se han presentado han sido en muchas ocasiones que el sistema deja de funcionar y esto ocasiona que se cierre, y esto ocasiones retrasos al momento de utilizarlo.

3. ¿Piensa usted que los problemas suscitados han sido provocados por los sistemas informáticos o por el mal manejo de los empleados?

Los problemas suscitados en el sistema informático en la parte física en ocasiones son provocada por los empleados y en el sistema de venta por el ingreso de virus lo cual dificulta seguir con las actividades de la empresa.

4. ¿Ud., ha adquirido capacitación del manejo del sistema informático en los últimos meses?

No, en los últimos meses no se ha realizado ningún tipo de capacitaciones a cerca del uso del sistema informático.

5. Considera usted que en la actualidad se utiliza el sistema para el fin que fue desarrollado.

No ya que al momento no se le está dando uso al sistema ya que no contamos con el personal adecuado para su manejo ni se realizan todas las actividades que están presentes en el sistema.

6. ¿Cada que tiempo se realiza mantenimiento general en los equipos para garantizar el buen funcionamiento de los mismos?

El mantenimiento se realiza cada seis meses y en ocasiones antes ya sea por fallas presentes en el sistema informático

7. ¿Cuándo fue el último análisis de vulnerabilidades que hizo la organización?
No, en realidad no se ha implementado ningún análisis al sistema para conocer a que riesgos es vulnerables

8. Cuáles serían los inconvenientes del sistema
Una de las mayores desventajas es que al ser una plataforma web es necesario de disponer de internet y también al momento de irse la energía no disponemos del acceso al sistema y produce muchos retrasos en los trámites.