DISEÑO DE MANUAL DE DIAGNOSTICO Y PREVENCION DE VULNERABILIDADES EN REDES DE DATOS PARA PYMES

JULIAN HERNAN BARRETO CUITIVA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C, COLOMBIA
2018

DISEÑO DE MANUAL DE DIAGNOSTICO Y PREVENCION DE VULNERABILIDADES EN REDES DE DATOS PARA PYMES

JULIAN HERNAN BARRETO CUITIVA

MONOGRAFIA

Proyecto de Grado para optar al título de:
Especialista en seguridad informática

Director de proyecto:
Esp. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C, COLOMBIA
2018

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 01 de noviembre de 2017

Dedico este trabajo a mi madre Sara Cuitiva quien me apoyo con sus palabras de aliento en continuar con mis estudios, a mi hija Juliana Barreto y esposa Patricia Aldana quienes me inspiran para salir adelante y continuar fortaleciendo mi formación profesional.

Julian Hernan Barreto Cuitiva

Agradecimientos

Expreso mi profundo agradecimiento a los Ingenieros Salomón González y Daniel Palomo docentes de la UNAD, por impartir conocimiento de calidad y por realizar el correspondiente acompañamiento de forma reiterativa, animándome al logro de culminación de esta monografía y a los compañeros de grado quienes aportaron de alguna forma comentarios acerca del documento.

TABLA DE CONTENIDO

LISTA DE FIGURAS

1. Glosario

AMENAZAS: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc [1]

ATAQUES: es un intento organizado e intencionado causado por una o más personas para causar daño o problemas a un sistema informático o red. [2]

BASTIONADO: el bastionado de sistemas o "Hardening" es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.[3]

CONFIDENCIALIDAD: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. [4]

ESCALAR PRIVILEGIOS: es el acto de explotación de un error, fallo de diseño o configuración de una aplicación, dentro de un sistema operativo o aplicación, para conseguir acceso a recursos del sistema que normalmente están protegidos frente a una aplicación o usuario. El resultado es que una persona con más privilegios de los esperados podría llevar a cabo acciones para las que no está autorizada. [5]

GPO: es un conjunto de una o más políticas del sistema. Cada una de las políticas del sistema establece una configuración del objeto al que afecta.[6]

HARDENING: es el proceso por el cual se asegura un sistema con el fin de evitar vulnerabilidades.

---

[1]Dórela Carrasquel, {en línea} {abril 2017}, Disponible en: https://carrmen.jimdo.com/riesgo-informatico

[2] ecured, {en línea} {abril 2017}, Disponible en: https://www.ecured.cu/Ataque_informático

[3] (seguridad syr, {en línea} {abril 2017}, Disponible en: https://seguridad.syr.es/servicios-seguridad-informatica/bastionado-de-sistemas-y-servidores

[4]SGSI, {en línea} {abril 2017}, Disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[5] (mejor-antivirus, {en línea} {abril 2017}, Disponible en: http://www.mejor-antivirus.es/terminologia-informatica/escalado-de-privilegios.html)

[6] (freyes svetlia, {en línea} {abril 2017}, Disponible en: http://freyes.svetlian.com/GPOS/GPOS.htm)

LOG: archivo donde se guarda el historial de eventos de configuración o manipulación de un objeto del sistema.
MALWARE: programa malicioso que tiene por objetivo dañar un sistema de información o dejar el sistema en mal funcionamiento.

PARCHES: se utilizan para solucionar errores de programación, actualizar los sistemas de información o agregar funcionalidades.

PENTESTING: o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas. [7]

PROTOCOLOS: conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales. [8]

RIESGOS: es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o la amenaza, por separado no representan un peligro, pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.[9]

SNIFFER: es una aplicación especial para redes informáticas, que permite como tal, capturar los paquetes que viajan por una red.[10]

TCP/IP: es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa Protocolo de control de transmisión/Protocolo de Internet. [11]

TELNET: proporciona una interfaz estandarizada, a través de la cual un programa de un host (el cliente de TELNET) puede acceder a los recursos de otro host (el servidor de TELNET) como si el cliente fuera una terminal local conectada al servidor.[12]

7 (Esaú A, {en línea} {abril 2017}, Disponible en: https://openwebinars.net/blog/que-es-el-pentesting)
8 ecured,{en línea} {abril 2017}, Disponible en: https://www.ecured.cu/Protocolos_de_red)
9 (unisdr, {en línea} {abril 2017}, Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf)
10 (culturacion, {en línea} {abril 2017}, Disponible en: http://culturacion.com/que-es-un-sniffer/)
11 (es.ccm, {en línea} {abril 2017}, Disponible en: http://es.ccm.net/contents/282-tcp-ip)
12 .(herramientas web para la enseñanza, {en línea} {abril 2017}, Disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/telnet.html)

2. Resumen

La presente monografía tiene como finalidad presentar un manual básico de seguridad informática para pequeñas y medianas empresas, buscando el aseguramiento de los sistemas de información y poniendo en conocimiento los controles que se deben implementar sin necesidad de invertir altos costos de asesoramiento de un especialista en la materia, como primera medida se tomaron documentos enmarcados en el tema de seguridad con el fin de recopilar información relevante que aportara en la creación de dicho manual, posteriormente se tomó la experiencia profesional, recurso importante para llevar cabo cada uno de las indicaciones y sugerencias que deben optar de acuerdo a las necesidades que tengan en el momento la pymes .

Esta monografía se basa en una investigación cualitativa la cual se desarrolla mediante entrevistas a las diferentes pymes, con el fin de indagar como protegen sus sistemas de información y como es el control o la administración de dichos recursos, como resultado de campo se concluye que la pymes están interesadas en el tema de seguridad informática pero no pretenden invertir altos recursos de asesoramiento, ni tampoco invertir en infraestructura tecnológica, dado que el negocio para ellos no se basa en la tecnología.

3. INTRODUCCION

Las redes informáticas se han convertido en pilar fundamental de trabajo en equipo, es posible compartir toda clase de documentos, música y videos en directo, llamada en vivo y demás servicios, las redes no tienen barrera y permiten tener contacto con los lugares más recónditos de todo el mundo, se han convertido en un elemento necesario de negocio.

Partiendo de la importancia de la comunicación en red, las pymes han optado por implementar sistemas que les permitan automatizar procesos que conlleven a la mejora y crecimiento del negocio, es así que es fundamental la protección de datos y la concientización del buen uso de las tecnologías, sabiendo que en el mundo informático se mueve en grandes masas, la delincuencia informática busca alterar, robar y dañar la información que a diario transita por las redes.

Los controles que se deben implementar en una red, inician básicamente del diagnóstico y revisión de cómo se tiene configurado en la pyme los sistemas actualmente y las políticas del buen uso de los sistemas ,cerrando así la posibilidad de ataques informáticos y difusión de virus, se debe tener en cuenta que la adopción de controles de seguridad parte como primera medida en el buen uso de los recursos informáticos ,y posteriormente la configuración de los mismos por políticas que reduzcan el riesgo de enfrentar un ataque cibernético, la difusión de un malware o virus informático.

4. FORMULACION DEL PROBLEMA

A menudo las empresas pymes no tienen presupuestado invertir un gasto elevado de tecnología en su entorno de trabajo, debido a que no es la necesidad del negocio. Se mueven en su dinámica diaria ,dejando temas tan importantes como la seguridad de la información, se ha comprobado que las empresas pymes contratan mano de obra barata con el fin de reducir costos por este rubro, la tecnología implementada parte del montaje de cinco o más ordenadores en un entorno de red de grupo, con el fin de facilitar y automatizar las labores diarias de sus empleados como: compartir archivos, navegar en internet, utilizar correo electrónico, manejo de ofimática y software que facilite la gestión diaria. El encargado de realizar el montaje de red, muchas veces no cuenta con la formación profesional suficiente y deja de segundo plano las configuraciones iniciales de seguridad en los equipos, abriendo así una gran brecha de inseguridad informática, la cual inicia localmente con ataques informáticos por los mismos empleados y pronto se expande externamente con ataques de tipo malware o delincuencia informática.

Los usuarios no son conscientes del uso y manejo de la tecnología y aun en la privacidad de la información de una compañía. Comparten, extraen, divulgan y descargan información todo el tiempo sin percatarse que pueden estar en peligro de ataques informáticos, exponiendo la reputación de la empresa y vulnerando así la confidencialidad, disponibilidad e integridad de los datos.

Por otro lado, los usuarios avanzados o empleados que realizan prácticas tecnológicas buscan alterar la red, tratan de acceder a equipos de comunicación como Swiches o Routers, con el fin de poner a prueba sus conocimientos y generan un alto impacto a nivel de negocio.

¿Cómo ayudar a realizar un examen de vulnerabilidades y amenazas en la red sin necesidad de invertir altos costos de asesoramiento de un experto de seguridad informática para las pymes?

5. JUSTIFICACION

Los altos costos de inversión en tecnologías de la información ponen a las pymes a pensar en la necesidad de inversión y retorno de inversión por este concepto, las asesorías de seguridad informática no son relevantes, dado que el negocio no es propiamente tecnológico y las pymes no son conscientes de asegurar la información como un activo.

Esta monografía tiene como finalidad realizar un manual de seguridad informática básica, donde se argumentará cómo realizar un examen básico de vulnerabilidades a nivel de red especialmente en equipos de usuarios finales y equipos de comunicación (swiches Routers y modems ,etc) para diagnosticar el estado de los equipos y aplicar los correspondiente controles que permitan salvaguardar la confidencialidad, privacidad e integridad de la información; pilares fundamentales de la seguridad informática.

Alcance:

- La presente monografía tiene como objetivo de estudio la pyme Amapola Diseño, en su entorno tecnológico no cuenta con personal especializado y dedicado para la administración informática.

- La monografía solo realizará sugerencias básicas de configuración en los equipos que actualmente utilicen para el desarrollo de las funciones diarias, teniendo en cuenta las limitaciones de presupuesto.

Limitaciones:

Teniendo en cuenta que la mayor parte de las pymes no están dispuestas a invertir en la adquisición de equipos tecnológicos, se deben ajustar las políticas y sugerencias de seguridad informática con los equipos que cuente para el trabajo diario.

6. OBJETIVOS DEL PROYECTO

6.1 OBJETIVO GENERAL

Diseñar un manual de seguridad informática para diagnóstico y prevención de vulnerabilidades en las pymes con el objetivo de reducir costos de asesoramiento por este concepto.

6.2 OBJETIVOS ESPECIFICOS

Levantar la información conceptual y estado de arte de seguridad en la red de datos, metodologías, herramientas y técnicas de revisión.

Determinar los principales riesgos en seguridad informática que afrontan las PYMES.

Realizar el manual de seguridad informática para el diagnóstico y prevención de vulnerabilidades.

Realizar un plan de pruebas para probar la eficiencia del manual de seguridad informática.

7. MARCO REFERENCIAL.

Como primera instancia se tomarán aportes de las siguientes investigaciones: tesis SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS) de Luis Albares, manual de seguridad en redes de Claudia Bello, estudiantes de áreas tecnológicas para tomar apartes y construir así el entregable materializándolo como un manual básico de acuerdo con los objetivos planteados.

7.1 MARCO CONTEXTUAL: PYMES

De acuerdo a la ley 590 del 10 de julio del 2000 artículo 2 se define como pyme:

Artículo 2°. Modificado por el art. 2, Ley 905 de 2004, Modificado por el art. 75, Ley 1151 de 2007, Modificado por el art. 43, Ley 1450 de 2011. Definiciones. Para todos los efectos, se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, comerciales o de servicios, rural o urbana, que responda a los siguientes parámetros:

1. Mediana Empresa:

a) Planta de personal entre cincuenta y uno (51) y doscientos (200) trabajadores;

b) Activos totales por valor entre cinco mil uno (5.001) y quince mil (15.000) salarios mínimos mensuales legales vigentes.

2. Pequeña Empresa:

a) Planta de personal entre once (11) y cincuenta (50) trabajadores;
b) Activos totales por valor entre quinientos uno (501) y menos de cinco mil (5.001) salarios mínimos mensuales legales vigentes.

3. Microempresa:

a) Planta de personal no superior a los diez (10) trabajadores;

b) Activos totales por valor inferior a quinientos uno (501) salarios mínimos mensuales legales vigentes.[13]

7.2 MARCO TEÓRICO

Mecanismos de inspección

Es necesario revisar periódicamente los estados de ingreso al servidor esto se hace mediante un log en el cual se evidencia los accesos no autorizados y ponen en alerta al administrador del sistema.

Intento de penetración

Es un análisis que permite detectar vulnerabilidades en un sistema informático, el alcance de esta revisión se extiende a: Equipos de Comunicación, Servidores, estaciones de trabajo, aplicaciones, base de datos, servicios informativos, portales web, acceso físico a documentación e Ingeniería social.

Para realizar un intento de penetración es necesario realizar las siguientes tareas:
Reconocimiento del recurso disponible mediante herramientas de análisis
Identificación de vulnerabilidades.
Explotación manual o automática de vulnerabilidades para detectar su alcance
Análisis de resultados.

El análisis conlleva al atacante a saber de:

- Versiones desactualizadas de software
- Versiones de software con vulnerabilidad conocidas
- Contraseñas triviales
- Usuario por defecto
- Configuraciones por defecto
- Utilización de servicio inseguro
- Recursos compartidos desprotegido
- Errores de asignación de permisos

Metodologías de prueba de penetración:

[13]Régimen legal en Bogotá,{en línea} {abril 2017}, Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=12672

Una prueba de penetración o pentesting es un proceso por el cual se verifica el nivel de seguridad de un sistema informático mediante pruebas controladas o ataques con el fin de encontrar vulnerabilidades que un atacante puede aprovechar para controlar, robar y manipular la información. Esta prueba, aunque es especializada se debe realizar una vez los sistemas estén implementados y próximos a salir a producción.

Tipos de Pentesting ; Existen en el mercado varios tipos de pentesting pero los más comunes y aceptados son:

Prueba de caja Negra(Black-Box):

El equipo de pruebas no tiene información por anticipado sobre la red de la organización, solo se cuenta con una dirección IP de un sitio web o ftp, el objetivo de esta prueba es tratar de irrumpir en la página web o servidor con el fin de sacar información como puertos de conexión TCP/IP abiertos, atacando el servicio de forma maliciosa.

Prueba caja Blanca(White-Box):

El equipo de pruebas cuenta con acceso para evaluar las redes, servidores, equipos finales y aplicaciones web, además cuenta con los diagramas de conexión para evaluar con total conocimiento cualquier equipo de la compañía, el objetivo solo va encaminado a evaluar equipos específicos o servicios con el fin de revisar el nivel se seguridad implementado.

Prueba de caja Gris(Grey-Box):

El equipo de pruebas tiene información parcial de los equipos de la compañía y tiene como objetivo simular un ataque de un empleado inconforme, se debe dotar al equipo de trabajo de los privilegios necesarios para realizar esta prueba

Hardening

Se basa en la configuración robusta a nivel de seguridad con el fin de impedir cualquier ataque informático, en la actualidad el software que se instala viene con configuraciones por defecto, abren automáticamente puertos innecesarios, contraseñas genéricas y en sí, una multitud de parámetros los cuales no son controlados a la vista, si no que se instala y se configura por defecto poniendo en riesgo el sistema y posteriormente la información, como medida de aseguramiento es necesario realizar un proceso de configuración personalizada (hardening) que busque el aseguramiento de cualquier sistema de información, este proceso como se menciona es personalizado y la entidad debe documentar y especificar muy bien las funciones de cada empleado con el fin de bloquear lo que no está permitido y dar acceso exclusivamente al rol de cada trabajador, esto además

optimizara el recurso humano para que se enfatice en su trabajo y no distraiga su atención en otros temas relacionados con el sistema.

"¿Qué podemos conseguir realmente?
Inmunizar el sistema contra ataques conocidos
Maximizar el tiempo necesario para llevar a cabo un ataque en la plataforma
Evitar el robo de información en el sistema " [14]

Como punto base para la iniciación del proceso hardening se debe tener en cuenta las siguientes revisiones técnicas:

De acuerdo a lo descrito por TARLOGIC[15] lo recomendado es seguir las siguientes líneas base de seguridad en la organización

Bastionado de sistemas (hardening)

Línea base de seguridad para usuarios: esta configuración tiene por objetivo asegurar el equipo con bloqueos físicos (desconexión de cables) de puertos de medios extraíbles USB y CD, además configurando el equipo para denegar el acceso a la consola de comandos, con el fin de evitar que el usuario manipule comandos que puedan afectar la red[16]
Línea base de seguridad para usuarios VIP: Existen usuarios privilegiados en función de su rol dentro de la empresa. Estos usuarios tienen requisitos de seguridad, privacidad y confidencialidad diferentes según la información a la que acceden.[17]

Línea base de seguridad para servidores: Bastionado de sistemas dependiendo del rol que desempeñan (Directorio activo, servidor web, servidor de bases de datos).[18]

Uno de los lineamientos base del servicio de la Empresa tarlogic a nivel de seguridad de servidores es estudiar a fondo el software que utiliza la empresa a nivel interno y externo con el fin de analizar el perfil de usuario que administra y definir desde este punto de partida el rol que debe tener, ajustando así las correspondientes protecciones adaptadas al sistema.[19]

Para la definición y configuración de directivas de aseguramiento de sistema operativo se realiza mediante estándares de seguridad, además es necesario que

[14] Acosta Jose. Protección de sistemas Operativos, 2010.
[15] Empresa dedicada a servicios de seguridad informática.
[16] Tarlogic. expertos en ciberseguridad {en línea}.
[17] Ibid., p.17.
[18] Ibid., p.17.
[19] Ibid., p.17

el especialista de seguridad informática o administrador de servidor tenga el suficiente conocimiento en el tema de restricciones.

Uno de los aportes que se debe tener en cuenta es el comando telnet como conexión insegura dado a la alta probabilidad de robo de credenciales de ingreso al sistema, este protocolo normalmente es utilizado para conexiones a equipos remotos con el fin de administrar mediante consola las funcionalidades de los equipos, no obstante es un riesgo informático bastantemente alto porque el tráfico de credenciales o datos no viaja cifrado sino este viaja en texto plano logrando así por el atacante robar las credenciales por medio de un sniffing o herramienta de análisis de tráfico poniendo así la compañía en un alto impacto de indisponibilidad e integridad de la información.

Una de las propuestas por Claudia bello en su manual de seguridad de redes[20] es la siguiente:

Disponer de un dispositivo programado mediante una clave secreta. El sistema que acepta el login envía un “challenge”, que el usuario digita en su dispositivo. Esto le devuelve la password adecuada para el código “challenge” enviado. Pero esa pasword que circulo por la red es válida solo para esa sesión, el hacker, si observo la sesión, deberá descifrar cual es el algoritmo utilizado para que en base al “challenge” variable y una clave secreta que no circulo por la red se obtenga la password de única vez. La siguiente tabla muestra un estudio de problemas de seguridad basado en redes distribuidas.[21]

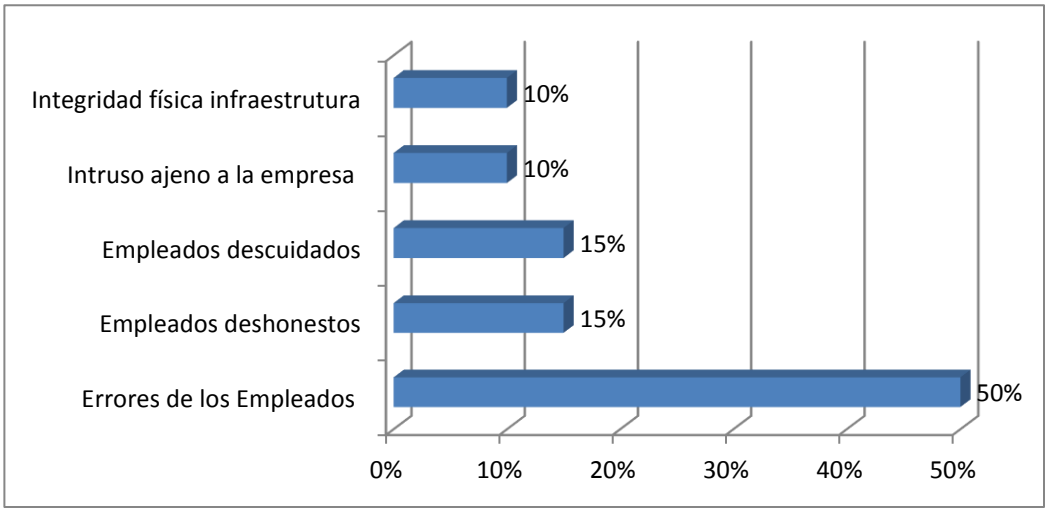

Figura 1. Nivel de ataque en una empresa

[20] Bello Claudia, Manual de seguridad de redes
[21] Ibid., p.18

Fuente: Autor

De acuerdo a la tabla (fig. 1) porcentual se concluye que el 80% de los problemas son generados por los empleados de la organización y los cuales se pueden tipificar en tres grandes grupos

- Problemas de Ignorancia
- Problemas de ocio
- Problemas de Malicia

En los proyectos de seguridad informática de la universidad nacional autónoma de México se enuncia en esta norma los tipos de ataques y las técnicas de seguridad a nivel de red

Ataques pasivos: como su nombre lo indica este ataque no levanta ninguna sospecha del usuario dado a que no modifica ningún archivo del sistema ,el objetivo de este ataque es monitorear el tráfico que cursa de un nodo A aun nodo B con el fin de capturar información trasmitida entre nodos, esta información se convertirá más adelante en recurso principal para el atacante luego de realizar un análisis del tráfico capturado, obteniendo así información relevante como usuarios y contraseñas de acceso a recursos importantes para la compañía ,obtención del origen y destino de la comunicación, leyendo las cabeceras de los paquetes monitorizados.[22]

Ataques Activos: a diferencia del ataque pasivo, este ataque tiene por objetivo modificar la información con el fin de hacer caer al usuario en falso sitios y capturar la información de una forma más eficiente y rápida, este tipo de ataque está catalogado entre:

Suplantación de identidad
El atacante clona o copia páginas web con el fin de engañar al usuario y así capturar la información privada, este ataque es conocido con phishing.

Las técnicas para no caer en este tipo de ataques son:

criptografía ,es necesario cifrar la conexiones mediante certificados de confianza con el fin de compartir la misma información en un sitio seguro desde el equipo origen hacia el servidor .Además se aconseja que los usuarios manejan un tipo de contraseña complejo con el fin de que el atacante le sea más difícil ,descifrar la contraseña; además es aconsejable verificar correctamente los sitios visitados y capacitar a los usuarios en no confiar en sitios sospechosos o no creer en mensajes de correo donde le soliciten los datos personales.

[22] Facultad de ingeniería, {en línea} {abril 2017}, Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AtaqPasivo.php

7.3 MARCO CONCEPTUAL

Para llevar este proyecto se debe tener en claro los pilares fundamentales de la seguridad informática

- Confidencialidad: consiste en proteger la información contra lectura no autorizada incluye específicamente piezas individuales que pueden inferir en otros elementos de la información

- Integridad: consiste en tratar la información de manera confiable, que por ningún motivo la información puede ser dañada y manipulada sin previo aviso o manipulación por entes no propietarios

- Autenticidad: Garantizar que el usuario X es el quien dice ser, se deben implementar mecanismos de autenticación en los equipos con el fin de evitar suplantaciones

- SSH: Secure Shell interprete de órdenes seguras, este protocolo mediante cifrado de conexión permite que el atacante no interprete las credenciales enviadas a un sistema remoto protegiendo así el acceso de forma segura

- Cifrado: trasformar la información por letras, números y símbolos, con el fin ocultar y asegurar la confidencialidad y autenticidad de la información ante personas ajenas, el cifrado se utiliza para guardar y ocultar los mensajes privados enviados por la red informática.

- ACL : Listas de control de acceso o firewall ,estas lista son utilizadas para permitir o denegar tráfico entrante en una red de área local con el fin de bloquear acceso no permitidos por la entidad.
- Política Usuario Local y dominio: determinar el perfil del usuario en un equipo local tales como permiso de ejecución, permisos de configuración, permisos de acceso

- Controles de seguridad, a nivel tecnológico se dividen en tres (Físicos, técnicos y administrativos)[23]
- Virus informativos, software que tiene por objetivo alterar el normal funcionamiento de un sistema sin el conocimiento o permiso del usuario[24]

---

[23] Manual de seguridad,{en línea} Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html

[24]Base de conocimientos Ictea ,{en línea} Disponible en: http://www.ictea.com/cs/knowledgebase.php?action=displayarticle&id=2175

- Riesgos, se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos.[25]

- Vulnerabilidades, es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. [26]

- Pruebas de penetración, es un a practica para poner a prueba un sistema de información con el fin de encontrar vulnerabilidades que pueda explorar un delincuente informático.

7.4 MARCO LEGAL

De acuerdo a la ley 1273 de 2009 en la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[27]

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

[25] Dórela Carrasquel, {en línea} {abril 2017}, Disponible en: https://carrmen.jimdo.com/riesgo-informatico/

[26]Symantec,{en.linea}Disponible en:https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[27] Ley 1273 de 2009,{en línea} {abril de 2017} Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena[28] de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

[28] Ibid., p.21.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.[29]

[29] Ibid., p.21.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.[30]

7.5 MARCO METODOLOGÍCO

Esta monografía se basará en una investigación tipo cualitativo, tomando como recursos las fuentes de información de las pymes tales como: entrevistas a los dueños del negocio y personal que interactúe permanentemente con los sistemas de información utilizados por la compañía, con el objetivo de analizar los datos obtenidos y la observación del entorno físico de trabajo, como resultado se obtendrán los insumos necesarios para sugerir controles de seguridad que permitan salvaguardar la información de la empresa.
En paralelo se aplicará una investigación exploratoria con el fin de identificar hallazgos donde se evidencie el riesgo informativo.

7.5.1 Universo y muestra. Como visita en campo se recolectará información con preguntas a trabajadores de la pyme acerca del rol que desempeña a diario, solo se tendrá en cuenta si el mismo hace uso de los recursos tecnológicos.

[30] Ibid., p.21.

7.5.2 Fuentes de recolección de información Para el desarrollo de la investigación se tomarán en cuenta las siguientes fuentes primarias:
Mediante visitas a las pymes se realizará una revisión de uso de las tecnologías con el correspondiente acompañamiento del encargado o dueño de la empresa en donde de observará como están organizados los equipos de cómputo. Esta visita se complementará con entrevistas, cuestionarios y una lista de chequeo donde se dará como resultado el estado actual de la pyme.

7.5.3 Técnicas e instrumentos Para llevar a cabo la investigación se utilizará las siguientes herramientas:

- Visitas técnicas: se evaluará el estado de la pyme en cuando a distribución y uso de equipos de tecnología, teniendo en cuenta además la seguridad física que se tiene implementada.
- Entrevista, al encargado de la organización o dueño de negocio
- Cuestionarios, a los empleados que hagan uso de los sistemas de información.
- Lista de chequeo para verificar que tipo de controles se tiene en el momento
- Pruebas de penetración, con el fin de identificar vulnerabilidades.
- Mediante observación se comprenderá los procesos y usos de la tecnología en su forma de trabajo diario.

7.5.4 Metodología de desarrollo Para el desarrollo del manual de diagnóstico y prevención de vulnerabilidades en las pymes se ejecutará con los objetivos propuestos:

Objetivo 1: Levantar información conceptual y estado del arte de seguridad en redes de datos

Actividad: investigar en línea manuales de seguridad informática, vulnerabilidades conocidas en sistemas Windows (uso de la consola cmd ,usuarios con privilegios elevados, acceso no controlado a páginas web), conceptos de ataques cibernéticos, conceptos generales de redes (configuración de Switch ,configuración de wifi ,configuración de contraseñas de conexión remota) y técnicas de revisión.

Objetivo 2. Determinar los principales riesgos de seguridad informática de empresa PYMES

Actividad: Listar los riesgos más comunes a los que se ven enfrentados las empresas a nivel de red y sistemas operativos, las causas y consecuencias de un ataque a los activos digitales, la forma de reducir los riesgos informáticos.

Objetivo 3. Realizar manual de seguridad informática para el diagnóstico y prevención de vulnerabilidades

Actividad: Luego de reunir todos los conceptos generales y una vez teniendo identificado los riesgos más comunes se procederá a diseñar el manual de seguridad informática el cual tendrá todas las pautas necesario para identificar y eliminar las brechas de seguridad más comunes en los sistemas de información de las PYMES.

Objetivo 4: Realizar un plan de pruebas para evaluar la eficiencia del manual de seguridad informática.

Actividad: Realizar un checklist donde se evalúen los diferentes puntos expuesto en el manual de seguridad informática con el fin de validar la eficiencia y aseguramiento de los diferentes dispositivos de sistemas presentes en las PYMES (Anexo D)

7.5.5 Metodologías de pruebas de seguridad informática: En la actualidad existen ataques cibernéticos que atentan con los bienes informáticos y sobre todo hay una alta exposición de ataques a empresa pymes, dado a que las mismas no tiene la conciencia y no asumen costos de aseguramiento técnico. La seguridad informática es fundamental. Debe existir en cada una de las empresas por pequeñas que sean un control que permita mitigar los riesgos informáticos a los que se ven sometidos día a día.

¿Pero cómo saber si una organización tiene medidas de seguridad robustas y suficientes?, la prueba de penetración es una herramienta de diagnóstico eficaz que revela de qué manera un ciberdelincuente podría lograr entrar a un sistema de información no autorizado de la organización; se tienen las siguientes herramientas las cuales tienen como objetivo revisar que tan vulnerable esta un servicio permitiendo adoptar los correspondientes controles para asegurar los recursos informáticos.

Herramientas de diagnóstico y penetración

Zenmap

Nmap ha sido una herramienta multiplataforma gratuita favorita entre los administradores. Ahora viene con la interfaz gráfica Zenmap para ayudar a hacer su trabajo de escanear la red más fácil.

Con el Asistente de Comandos, los administradores de seguridad ven las opciones de línea de comandos en la parte superior de la pantalla para cada perfil (nuevo o

predefinido). Ellos pueden editarlos de forma interactiva antes de ejecutarlos. Esta característica de interacción ayuda a ahorrar tiempo normalmente requerido para corregir errores de tipeado y/o de configuración.

Al generar un perfil se puede configurar varias opciones de exploración entre estas: ping trazas y demás configuraciones avanzadas que el especialista desee explorar para pruebas de penetración. Este perfil normalmente se guarda con el fin de más adelante editarlo y agregar nuevas técnicas de ataque o validar que puertos o conexión fueron modificadas por el servidor analizado[31]

Colasoft Capsa

Esta herramienta analiza y monitorea el tráfico de red además analiza el consumo de ancho de banda, permite ver la conversación entre paquetes y analizar los puertos abiertos en las conexiones.

La versión gratuita permite monitorear 10 IP por un rango de 4 horas, la versión profesional cuesta 695 dólares y permite analizar múltiples IP´S.

OpenVAS

Potente software de escaneo de vulnerabilidades que permiten centrar los servicios en tarjetas de red, busca mediante análisis en red encontrando las llamadas brechas de seguridad, permitiendo asegurar las plataformas de servicios desde equipos de usuario básico, hasta equipos servidores.

- Tiene cuatro características destacadas:
- Escaneos concurrentes a diferentes nodos
- Escaneos automatizados temporalizados
- Servicio web integrado para realizar todas las configuraciones
- Multiplataforma

Microsoft Baseline Security Analyzer

Herramienta de Microsoft, analiza las principales vulnerabilidades del sistema, convirtiéndose en una herramienta muy útil para analizar equipos desactualizados

[31]Techtarget ,{en línea} Disponible en: http://searchdatacenter.techtarget.com/es/consejo/Cuatro-herramientas-de-pen-testing-para-mejorar-la-seguridad-empresarial

y configuraciones erróneas comunes, como contraseñas débiles, vulnerabilidades de servidores con servicios de sql server y IIS

La instalación es sencilla, solo se debe seguir el asistente de instalación en sistemas operativos Windows

8 PRINCIPALES RIESGOS INFORMATICOS EN UNA PYMES

De acuerdo al auge y la necesidad primordial del uso de equipos de comunicación de red de datos, para la comunicación de servicios como: videos, correos, imágenes, documentos y demás servicios de red que deba tener una empresa para el esquema de productividad diaria, se hace necesario el diagnostico e implementación de controles que permitan la conexión y buena administración de dichos equipos, con el fin de detectar y evitar inseguridades y posibles accesos por empleados de la misma empresa o usuarios externos con vínculos de visitantes, de acuerdo al análisis propuesto, es necesario evaluar como primera medida los recursos más relevantes de la compañía y así evaluar el impacto que tendrán o el riesgo a que están expuestos frente ataques de tipo informático, es necesario focalizar los siguientes puntos vulnerables para controlar y cerrar las brechas de seguridad :

- Puntos de acceso
- Las redes no son segmentadas y los usuarios tienen acceso a cualquier equipo en la red donde pueden descargar y cargar información sin ningún control o entrometerse en sistemas no autorizados vulnerando la confidencialidad de los datos.
- Sistemas mal configurados.
- Los servidores son mal configurados por los administradores, funciones como telnet son protocolos inseguros y fáciles de atacar
- Problemas de software, muchas veces los administradores del sistema no actualizan los equipos con los correspondientes parches de seguridad poniendo así un alto riesgo de ataque.

- Amenazas internas, los usuarios tienen acceso total al sistema pueden escalar privilegios y poner en riesgo la confidencialidad de la información instalando software para analizar tráfico para realizar ataques de captura de contraseñas en la red.
- Seguridad física, tanto los equipos de comunicación como los servidores deben estar alejados de los usuarios para evitar posibles intrusiones, estos equipos

deben contar con una seguridad robusta, con contraseñas complejas, deben estar en un cuarto seguro y con restricción de acceso a personal no autorizado.

Luego de realizar una investigación en diferentes sitios web como el periódico el tiempo, en su sesión de análisis de editor[32] , profitline[33] página especializada en servicios tercerizados y al realizar varias entrevistas a pequeñas empresas se evidencia errores que ponen en riesgo la seguridad de la información, estos se presentan a continuación:

- Carecen de actualizaciones en el hardware, los equipos van quedando obsoletos y no hay presupuesto para invertir en la actualización de hardware, muchas pymes estas trabajando con sistemas operativos desactualizados dado a que el hardware no permite la instalación de un sistema actualizado por requerimientos técnicos.

- El software no tiene licencia de uso. Como muchos colombianos en este país se trata de buscar software pirata, poniendo en riesgo la empresa porque no se cuenta con una licencia de funcionamiento y soporte de aplicaciones, enfrentándose así a un foco de virus informático por el mal uso del software.
- Falta de mantenimiento preventivo, los equipos van generando archivos basura a diario de páginas consultadas por los usuarios, documentos guardados y borrados, posibles malware y virus etc., esto pone lento el sistema y puede sufrir fallos graves con pérdida de información

- No tiene un asesoramiento técnico a la hora de adquirir un equipo o servidor, se compran de acuerdo a los bajos costos que ofrecen en el mercado generando consecuencias graves al momento de instalar o adquirir un software no compatible con el hardware adquirido

- No está documentado el sistema: equipos, servidores, aplicaciones, correo, contraseñas wifi, seguridad perimetral, etc. Cuando se va a realizar cualquier soporte no hay documentación prevista que ayude resolver de forma inmediata y acertada los diferentes incidentes que se puedan presentar, esto ocasiona altos tiempos de solución en un servicio crítico y perdida de información por la no utilización y temporal de los sistemas de gestión diaria.

- Cuando es necesario cambiar una configuración o activar accesos para los nuevos usuarios, en las Pymes este problema es recurrente se otorgan permisos al usuario y no se tiene un control que permita saber quiénes deben tener acceso a ciertos recursos y quienes no, esto conlleva a que los mismos empleados

[32]Una pizca de duda / Análisis del editor,{en línea} {Noviembre de 2017} Disponible en http://www.eltiempo.com/archivo/documento/CMS-13418602

[33] Cinco errores comunes de seguridad{en línea }{Noviembre de 2017} http://profitline.com.co/5-errores-comunes-seguridad-informatica-cometen-las-pymes/

manipulen información confidencial sin corresponder a sus labores, además conlleva a que compartan con extenso mediante correos o medios extraíbles a personas ajenas a la entidad.

- No se realiza copia de seguridad o son insuficientes y no hay un plan de recuperación ante desastres. Este problema es muy casual en las pymes, no existe un control de copias de seguridad de la información semanal que aseguren la disponibilidad de la información, cada vez que un equipo sufre un daño de tipo software o hardware las pymes solían recuperar la información invirtiendo costos innecesarios por no controlar esta actividad

9. CONCLUSIONES

En el diseño del manual (Anexo A) se ha comprobado el uso y la configuración de políticas de seguridad de Windows, asegurando los equipos de cada usuario con el fin de evitar ataques informáticos.

Se ha evidenciado que la mayoría de ataques se producen por las malas prácticas de configuración que realiza el administrador del sistema, y se ha entendido que es necesario generar contraseñas fuertes con el fin de que el atacante le sea más complicado ingresar al sistema de información.

Existe en el mercado una gran variedad de herramientas de protección, las cuales se pueden utilizar de acuerdo a la necesidad.

Siempre se debe estar a la vanguardia de la actualización de los sistemas operativos para obtener el soporte constante del fabricante.

10. DIFUSIÓN

Este manual está al alcance de cualquier Pymes que quiera optar por realizar un análisis básico a los equipos conectado a una red de trabajo, aplicando los controles expuestos en el manual, estará disponible principalmente en el repositorio de la UNAD y la página slideshare la cual integra redes sociales como linkedin , se puede realizar búsquedas en google específicas como “Manual Seguridad Informática Pymes” ,dando como resultado el proyecto propuesto .

11. REFERENCIAS BIBLIOGRÁFICAS

ÁLVAREZ BASALDÚA, Luis Daniel," seguridad en informática (auditoría de sistemas)". {en línea}. {18 de marzo de 2017}. Disponible en: <http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf >

ACOSTA, David. Estándares de Configuración Segura Hardening en pci. {En línea}. {25 de marzo de 2017}. Disponible en: <http://www.pcihispano.com/estandares-de-configuracion-segura-hardening-en-pci-dss>

Acosta, José Manuel Protección de Sistemas Operativos {En línea}. {25 de marzo de 2017}. Disponible en: <https://www.docsity.com/es/proteccion-de-sistemas-operativos/400856/>

BISOGNO, María Victoria, "Metodología para el Aseguramiento de Entornos Informatizados" {en línea}. {18 de marzo de 2017}. Disponible en: http://materias.fi.uba.ar/7500/bisogno-degradoingenieriainformatica.pdf

BELLO, Claudia," Manual de Seguridad en Redes" {en línea}. {18 de marzo de 2017}. Disponible en: < https://es.slideshare.net/csandovalrivera/manual-de-seguridad-en-redes >

CABALLERO QUEZADA, Alonso Eduardo, "Hacking con Kali Linux" {en línea}. {18 de marzo de 2017}. Disponible en: http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ, Régimen Legal de Bogotá D.C. {En línea}. {25 de marzo de 2017}. Disponible en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>

TARLOGIC. Bastionado de sistemas (hardening). {En línea}. {25 de marzo de 2017}. Disponible en: <https://www.tarlogic.com/servicios/bastionado-de-sistemas-hardening/>

TECNOZERO, {En línea}. {29 de Abril de 2017}. Disponible en https://www.tecnozero.com/blog/que-problemas-informaticos-encontramos-en-la-pyme/

11.ANEXOS

ANEXO A: MANUAL DE SEGURIDAD INFORMÁTICA PARA LAS PYMES

ANEXO B: RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

RESUMEN ANALÍTICO ESPECIALIZADO	
1. Título.	Manual de seguridad Informática para Pymes
2. Autor:	Barreto Cuitiva, Julian Hernan
3. Edición	**Editorial Universidad Nacional Abierta y a distancia Unad especialización en seguridad de la información**
4. Fecha	21 de mayo de 2017
5. Palabras Claves,	aseguramiento equipos de usuarios, aseguramiento de redes LAN, Aplicación de políticas grupales de grupo, plan de pruebas, diagnóstico de seguridad y prevención de ataques informáticos
6. Descripción.	el documento se basa en dos fases de análisis de seguridad, diagnóstico y prevención además presenta un cuadro de pruebas que se debe ejecutar como primera medida para ir aplicando los controles descritos en el manual
7. Fuentes.	Aunque para la construcción del manual se buscaron varias fuentes en internet, el trabajo final se basó en la experiencia profesional en la aplicación de controles de seguridad informática en grandes empresas llevándola a la explicación básica para aplicabilidad en pymes

RESUMEN ANALÍTICO ESPECIALIZADO	
8. Contenidos.	el manual parte del objetivo principal que es el apoyo que se debe brindar a las pymes en cuanto a aseguramiento tecnológico ,teniendo como alcance la aplicabilidad del manual en cualquier equipo de usuario final u tercero que se conecte a la red local con el fin de asegurar la conectividad en red ,el manual contiene dos fases diagnóstico y prevención ,la fase de diagnóstico tiene por objetivo buscar vulnerabilidades o malas configuraciones iniciales realizadas a los equipos de cómputo ,de debe evaluar con las herramientas propuestas en el manual con el fin de buscar puertos de conexión abiertos o servicios que por desconocimiento están compartidos en la red ,la fase de prevención tiene por objetivo prevenir y asegurar la infraestructura técnica brindando una mayor seguridad de le información ,en esta fase se describe la forma de cómo asegurar los equipos mediante políticas de grupo ,además se especifica la creación de usuario y roles en el equipo local de cada usuario especialmente recomendando la complejidad de la contraseñas el bloqueo de unidades extraíbles ,el bloqueo del símbolo de sistema ,registro de Windows ,restringiendo el acceso a páginas de internet y auditando los intentos fallidos de ingreso al sistema ,además se especifica las mejores prácticas de configuración de equipos de comunicación Switch y router para la buena administración remota ,se propone la separación de redes de trabajo por vlan o redes virtuales con el fin de separar las áreas de trabajo en redes diferentes ,por último se propone un plan de pruebas el cual se debe evaluar como primera revisión e ir adoptando los controles necesarios de acuerdo al manual

RESUMEN ANALÍTICO ESPECIALIZADO	
9. Metodología.	Basados en empresas pequeñas y viendo la necesidad que tiene las pymes en asegurar los activos informática sin considerar altos costos de asesoría en seguridad informática se decide a crear un manual básico y comprensible de seguridad de la información con el fin de que sea aplicado en cualquier equipo pc y equipos de comunicación con la premisas de asegurar la confidencialidad, disponibilidad e integridad de la información y evitando el riesgo de ataque informático ,este proyecto se lleva a cabo con los siguiente pasos consiguiendo el producto final “manual de seguridad informática para Pymes” . 1. Propuesta de objetivos del proyecto • Levantamiento de conceptos y estado del arte de la seguridad informática • Determinación de principales riesgos se seguridad de información en una pyme. 2. Ejecución de pruebas de diagnóstico: con herramientas gratuitas y demos, se verifica el software disponible en la web con el fin de verificar funcionamiento y validar la efectividad de la herramienta, en pruebas de penetración y auditoria. 3. Ejecución de pruebas preventivas, se valida varias vulnerabilidades que se obtienen en las pymes luego de realizar configuraciones erróneas en los sistemas, se busca como asegurar siguiendo las mejores prácticas de seguridad de la información basándose en los manuales obtenidos en las distintas páginas de internet foros y trabajos escritos. 4. Finalmente, se realiza la construcción del manual de seguridad informática realizando el paso paso de las mejores prácticas de aseguramiento de equipos de comunicación y equipos de usuario.

RESUMEN ANALÍTICO ESPECIALIZADO	
10. Conclusiones.	En el diseño de este manual se ha comprobado el uso y la configuración de políticas de seguridad de Windows asegurando los equipos de cada usuario con el fin de evitar ataques informáticos. Hemos podido evidenciar que la mayoría de ataques se producen por las malas prácticas de configuración que realice el administrador del sistema y se ha entendido que es necesario generar contraseñas fuertes con el fin de que el atacante le sé a más complicado ingresar al sistema de información. Existe en el mercado una gran variedad de herramientas protección las cuales se pueden utilizar de acuerdo a la necesidad. Siempre se debe estar a la vanguardia de la actualización de los sistemas operativos para obtener el soporte constante del fabricante.
11. Autor del RAE.	Julian Hernan Barreto Cuitiva

ANEXO C: FORMATO ENCUESTA INICIAL DE SEGURIDAD

Datos de la Empresa

Fecha Hora

Nombre Empresa	
Sector	
Número de empleados	
Nombre del encuestado	
Cargo	

Uso de Computadores y redes

	si	no
¿Cuantos equipos hay en la empresa?		
¿La empresa dispone de una red LAN?		
¿Utiliza en la empresa carpetas compartidas?		
¿Utiliza software Libre?		

Tiene la empresa alguno de los siguientes mecanismos de seguridad de la información:

1	Mecanismo de autenticación para ingreso a los computadores	
2	Copias de seguridad de la información	
3	Antivirus	
4	Firewall (software o hardware)	
5	Uso de medios extraíbles (USB, CD, Disco externo etc.)	

Internet

	si	no
la empresa cuenta con conexión a internet		

Que tipo de conexión utilizan

1 Banda Ancha ADSL
2 Conexión por llamada RDSI
3 Banda ancha por red de cable

Que uso le dan a el internet

1 búsqueda de información
2 uso de correo
3 marketing y publicidad de la empresa
4 para comunicarse con los empleados
5 Licitaciones
6 pago de servicios

uso de equipos

cuantos empleados ocupan exclusivamente los computadores

los empleados cuanta con usuarios personalizados

si no

los empleados son administradores locales de cada equipo si no

el empleado tiene acceso a internet sin limitaciones si no

los empleados hacen uso de unidades extraíbles si no

ANEXO D: PLAN DE PRUEBAS

Se define el siguiente formato el cual tendrá los ítems a evaluar, como prueba inicial se deberá realizar las pruebas sin aplicar ninguna política de seguridad con el fin de diagnosticar el estado actual de la pyme posteriormente se Debe aplicar los controles según manual para asegurar los equipos de usuario y la red de la Pymes.

Plan de pruebas						
	Éxito del ataque			Observaciones	Aplicar Control	Pag
Ítem a Evaluar	sin éxito	parcial	Exitoso			
Acceso a equipo en modo administrador o invitado, combinando contraseñas comunes			X	Se obtiene acceso con una cuenta de administrador con contraseña admin, luego de probar con varias opciones	Creación de cuentas de Red	15
Uso de medios extraíbles en cualquier equipo			X	Lo puertos del equipo no estaban bloqueados, se obtuvo acceso para copiar archivos del equipo	Configuración de directivas de grupo para medios extraíbles USB cd etc.	19
Navegación a sitios con alto riesgo de virus			X	Se obtiene acceso internet sin restricción	Navegación a paginas no autorizadas	23
Acceso a equipos de comunicación por Telnet		X		Se accede a un equipo switch por el comando telnet, pero no se conoce la contraseña. Para obtenerla se deberá correr un sniffer	Aseguramiento redes LAN	31
Manipulación de comando cmd			X	Desde los equipos se puede manipular cualquier comando	directiva impide que los usuarios del equipo local manipulen	21
conexiones remotas a equipos de otras dependencias			X	Se accede remotamente desde cualquier red	Aseguramiento redes LAN	29
acceso por consola a puertos abiertos tcp/ip			X	Se accede a puerto TCP 21 ftp	Bloqueo de puertos con software de Firewall	8