UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
MEDELLÍN

INFORME FINAL DE LA PRÀCTICA EMPRESARIAL

Seguridad Informática: herramientas de mantenimiento y vulnerabilidades.

Elaborado por,

Laura Maritza Holguín Zapata

Asesor asignado,

Camilo Andrés Flórez Velásquez

Universidad Santo Tomás Sede Medellín

Facultad de Ingeniería de Telecomunicaciones

Julio de 2019

CONTENIDO

1. Resumen

La seguridad informática es una disciplina de las ciencias computacionales e informática que se enfoca en la protección y privatización de los sistemas. Podemos encontrar dos tipos de enfoques en seguridad: La seguridad lógica que se encarga de resguardar contenidos e información y la seguridad física que se aplica a los equipos es decir al hardware, teniendo presente que los ataques no únicamente se dirigen al software de los equipos.

Las amenazas en la seguridad pueden ser de naturaleza externa o interna, y las formas más comunes bajo la cual se presentan estos ataques es por medio de virus infiltrados en archivos, que pueden corromper la información de otros archivos sin autorización del usuario. Las amenazas externas son más fáciles de combatir, y bajo esta situación, no es fácil para el perpetrador concretar su ataque, en cambio las amenazas internas son más peligrosas, puesto que el perpetrador no es detectado por los sistemas de seguridad preparados contra ataques provenientes del exterior de la red corporativa. Un atacante mediante un virus puede tener el poder de cambiar códigos fuente de programas, o incluso utilizar las imágenes que estén guardadas dentro del equipo para crear contenido perjudicial.

Los ataques más normales a nivel corporativo, que ponen en riesgo la información de la entidad, son los gusanos, troyanos, el espionaje o suplantación. Estos ataques mencionados imponen el reto de mantener los datos de forma segura y confidencial, que a su vez deben ser respaldados desde áreas de la empresa, como las de networking, que deben brindar un constante apoyo lógico por medio de soluciones tecnológicas, como por ejemplo un firewall, que permita identificar las posibles amenazas.

2. Introducción

Con el desarrollo constante de la tecnología, la economía y el volumen de información, es notorio el incremento de las vulnerabilidades de los sistemas informáticos que hacen parte de nuestro diario vivir. Las vulnerabilidades son la consecuencia de bugs o fallos en los diseños de los sistemas, y también son el resultado de las limitaciones tecnológicas pendientes por ser resueltas por los especialistas en seguridad informática, y que hasta el momento impiden contar con un sistema de manejo de la información ciento por ciento seguro.

La detección, evaluación y eliminación de vulnerabilidades es el factor más importante en el área de seguridad informática dentro de una compañía, pues no solo los sistemas operativos sufren ataques sino también aplicaciones, correos, servidores, impresoras, entre otros. Es por esto que medidas como las auditorías informáticas tienen la finalidad de evaluar el nivel de efectividad de la tecnología que se está utilizando en una empresa, y en paralelo a esto, se revisan los procesos de planificación, organización y aplicación en proyectos de comunicación, redes, aplicaciones y seguridad de información, para proponer y aplicar las soluciones más adecuadas acordes con las necesidades y posibilidades de la empresa o entidad.

Por lo tanto, es evidente que la finalidad del área de la seguridad informática es proteger las redes de datos, las aplicaciones, servicios e información que hacen parte de los sistemas con los que estamos involucrados diariamente, además como la cantidad de información que manejan las organizaciones es cada vez más grande, entonces es necesario el constante estudio para identificar y apropiar las nuevas tecnologías para la protección de la información, para su respectivo uso en el mejoramiento continuo de los indicadores de seguridad de la información, teniendo presente el gran número de personas que hacen uso de los computadores y de los servicios disponibles de la red, para la administración de grandes volúmenes de datos.

3. Breve Descripción de la Empresa

- **Razón Social de la empresa donde se ejecutó la práctica**: Emtelco S.A.S
- **Objeto Social de la empresa Emtelco S.A.S**: La sociedad tiene como objeto principal, prestar servicios de tercerización de procesos de negocios (BPO) por su sigla en inglés y Contact Center, incluyendo sin limitarse a ello, los siguientes:

  Gestión de procesos de soporte en front office y back office.

  Procesos de gestión y administración de información.

  Gestión de procesos tecnológicos.

  Procesos de gestión del talento humano.

  Gestión de servicios de contabilidad y finanzas.

  Alquiler de infraestructura física y/o técnica y/o tecnológica asociada a los servicios de la sociedad.

- **Área de la empresa donde se ejecutó la práctica**: Área de Seguridad Informática.
- **Equipo de trabajo de la Unidad donde se desarrolló la práctica**:

  El equipo humano que participó directamente en el desarrollo de la práctica empresarial alrededor de la temática de seguridad informática, son los siguientes profesionales:

  - Coordinador: Ingeniera Laura María Vélez.
  - Analista senior de seguridad informática: Dylan Manuel Muñoz Ayazo.
  - Analistas junior de seguridad informática: Julián esteban Serna Córdoba, Andrés Daniel Muñoz.

4. Planteamiento del Problema de Investigación y su Justificación en Términos de Necesidades y Pertinencia.

Hoy en día la seguridad informática es uno de los aspectos más importantes a tener presente en las empresas, ya que el uso masivo de las tecnologías de la información ha incrementado sensiblemente el número de equipos informáticos a proteger contra vulnerabilidades; además el fenómeno de los ciberataques es cada vez más común, con la consecuencia de exponer información vital de la empresa a terceros, con unos niveles de complejidad más robustos, que ponen a prueba el nivel de desarrollo tecnológico de los sistemas de seguridad.

Las empresas competitivas se caracterizan por contar con sistemas de seguridad informática que garantizan la protección, integridad, confiabilidad, autenticidad y disponibilidad de la información. Lo mencionado implica el uso de recursos y plataformas tecnológicas con un alto nivel de disponibilidad, que brinden una cobertura segura y confiable; y el establecimiento y la aplicación de políticas, criterios, lineamientos y normativas que minimicen los riesgos, como por ejemplo el control en los horarios de los empleados, restricciones en el uso de aplicaciones y servicios, autorizaciones-denegaciones, planes de emergencia y protocolos, todo con la finalidad de elevar los estándares de seguridad.

Por lo tanto es evidente la necesidad de comenzar a disponer de profesionales en seguridad informática, capacitados para efectuar actividades de evaluación, planificación, aplicación y evaluación típicamente enmarcadas en las auditorias, para alertar a la empresa de los posibles riesgos informáticos, aplicando métodos orientados a proveer mejores codificaciones en el procesamiento de datos.

5. Plan de trabajo – Desarrollo práctica profesional

Para aportar a la solución de la situación problémica exhibida en la sección anterior, se proponen los siguientes objetivos general y específicos:

Objetivo General

Determinar los parámetros generales para que la información que maneja Emtelco, bien sea propia, en custodia, o compartida con terceros, cumpla con los siguientes criterios:

Sea protegida contra modificaciones no autorizadas realizadas con o sin intención, sea accedida y usada solo por aquellos que tienen necesidad legítima para la realización de sus funciones del cargo y del negocio, y esté disponible cuando sea requerida y sea utilizada exclusivamente para los propósitos para los cuales fue obtenida.

Objetivos Específicos

Fundamentar el desarrollo, implantación, mantenimiento y cumplimiento de la Seguridad de la Información por medio de un Sistema de Gestión de Seguridad que la despliegue.

Proteger la imagen, el buen nombre, patrimonio e intereses de Emtelco y sus clientes.

Fundamentar la gestión de riesgo en los activos para la protección de la información.

Establecer los lineamientos de seguridad de la información.

Fortalecer la cultura alrededor de las temáticas asociadas a la protección de la información en Emtelco.

6. Metodología Implementada

La información y los procesos que la acompañan, requieren protección frente a las amenazas que ponen en riesgo la disponibilidad, integridad, confidencialidad y autenticidad de la información que se hace necesaria para lograr y mantener los objetivos de una empresa. Esta información generalmente es procesada e intercambiada por medio de redes de datos y equipos informáticos que están sometidos a constantes amenazas de seguridad que pueden tener origen dentro de la organización como son accesos no autorizados a información, incendios, o cualquier accidente o proceder de fuentes externas ya sea por medio de virus, denegación de servicios o códigos maliciosos.

Gracias a la seguridad informática es posible disminuir los posibles riesgos de una forma significativa, conociendo y gestionando de manera ordenada los mismos, teniendo en cuenta procedimientos adecuados para implantar controles de seguridad como políticas, procesos y estructuras respaldados a su vez por hardware y software que ayuden con los objetivos específicos de cada empresa de manera que se mantenga siempre el riesgo por debajo de un nivel asumible.

7. Resultados

A continuación se proceden a ilustrar los resultados obtenidos durante el desarrollo de la práctica en la empresa Emtelco S.A.S, donde se evidencia el levantamiento de información crítica para la fundamentación de las políticas y lineamientos de la empresa frente a la seguridad informática.

Considerando que la seguridad informática es una rama de la seguridad de la información su importancia radica principalmente en la prevención de ataques ya sea a cuentas bancarias, información, contraseñas o información esencial acerca de una empresa. La seguridad informática no debe ser confundida con seguridad de la información ya que esta se enfoca en la realización de auditorías de sistemas, planificación de continuidad de negocio, ciencia forense digital y administración de sistemas y la informática abarca medidas de seguridad como software de antivirus, firewalls, y controles de entorno que pueden ser tareas realizadas de manera automática o depender de la activación manual como funciones de software, scripts de Java o recursos de computadora o internet.

Un intruso puede modificar o cambiar códigos de fuente de programas, utilizar imágenes, o cuentas de correo para usar de forma perjudicial y así lograr la intrusión. La búsqueda de las vulnerabilidades es uno de los aspectos más importantes de la seguridad informática, es por esto que existen aplicaciones y herramientas que permiten analizar aplicaciones en búsqueda de vulnerabilidades como escáneres que determinan si hay amenazas como reportarlas y solucionarlas.

Algunos elementos importantes para tener en cuenta en la consolidación de un sistema de seguridad informática son los siguientes:

- Integridad: Hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros. Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina. Un aspecto relacionado con la integridad es la autentificación, cualidad que permite identificar al generador de la información y que se logra con los correctos accesos de usuario y con otros sistemas como la recientemente mencionada firma electrónica. Para algunos, incluso, la autentificación sería el “cuarto pilar” de la Seguridad de la Información.

- Confidencialidad: Otra característica o condición de la información es la disponibilidad, se dice que la información posee esta propiedad cuando puede ser accedida y obtenida en completitud en cualquier momento que se requiera, es decir, que la información sea accesible. Para garantizar la disponibilidad y disminuir los riesgos existen todo tipo de medidas como centros de datos con plantas de energía independientes, servidores espejo, replicación de datos, redes de almacenamiento, enlaces redundantes, etc. Dependiendo de los costos que una organización esté dispuesta a asumir y la importancia que la disponibilidad suponga para la misma.

- Disponibilidad: La información permanece inalterada y es accesible para aquellas personas que cuentan con una previa autorización, pero si al mismo tiempo alguien sin los permisos adecuados puede acceder de forma clandestina a la información esta propiedad se pierde. La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

  En la figura 1 se enseña un pequeño esquema que ilustra la necesidad de articular estos elementos, para alcanzar las metas de seguridad planteadas:

Figura 1. Elementos de confidencialidad, integridad y disponibilidad en confluencia con la seguridad de la información. Recuperado en el mes de julio de 2019, del sitio web www.google.com.

- Autenticidad: Si bien la integridad nos indica si los archivos han sido modificados, la autenticidad no permite saber si los archivos son reales y son enviados por la persona correcta.

Medidas y herramientas para el mantenimiento de la seguridad informática y prevención de ataques

A continuación se procede a ilustrar las medidas y herramientas tecnológicas actualmente empleadas para el mantenimiento y consolidación de la seguridad informática a nivel empresarial.

- **Software de antivirus**

  El software de antivirus permite detectar, prevenir, bloquear, desinfectar y tomar medidas contra virus o software malintencionado. Con el transcurso del tiempo este tipo de software también ha añadido a la lista de sus funciones reconocer malware como: gusanos, troyanos, spyware, etc.

A pesar de que un software de antivirus puede trabajar de diversas formas, este no es totalmente efectivo, (demostrado por Frederick Cohen en 1987 cuando determinó que no existe ningún algoritmo perfecto para la detección de virus), se utilizan dos métodos para la protección:

Monitorización: Se realiza un monitoreo constante de la actividad de los archivos del sistema que posiblemente estén infectados.

Análisis: Se analizan los archivos del equipo comparándolos con una base de datos de programas malignos, constantemente se actualiza con información de nuevas infecciones realizando consultas traídas de la nube.

El software realiza un proceso que compara los archivos del disco duro con un "glosario" de virus ya conocidos. Si cualquier pieza de código en un archivo del disco duro coincide con un virus conocido, el software de antivirus entra en acción y ejecuta una de las siguientes acciones posibles:

Reparar el archivo: El antivirus trata de reparar el archivo infectado eliminando el virus.

Ponerlo en cuarentena: El antivirus intenta proporcionar protección contra el virus, haciendo inaccesibles los programas a este archivo, impidiendo su propagación y ejecución.

Eliminar el archivo: El antivirus elimina el archivo (siempre nos preguntará antes si deseamos hacer esto).

Analizar la conducta de los archivos del sistema: El antivirus efectuará un seguimiento de todos los programas que están en funcionamiento. Por ejemplo, si un programa intenta realizar una actividad sospechosa, como escribir datos en un programa ejecutable, el antivirus alerta al usuario de este hecho y le informa sobre las medidas que debe tomar.

- **Software dentro del área de seguridad informática**

Validación de equipos: incluye la cantidad de dispositivos registrados en la empresa y el grupo al que pertenece, se pueden observar datos como el nombre, tipo de sistema operativo, dirección IP, última conexión, última actualización, estado (es visible en la red), etc.

Permisos: Desde el software se le pueden otorgar a otros equipos permisos tales como: USB, DVD, CAM o Bluetooth

Actualizaciones e instalaciones no Microsoft: El software muestra las actualizaciones de los equipos, después de pasar un límite las maquinas son enviadas a actualizar, así se puede tener un control del estado de las mismas.

Gestión dispositivos móviles: se otorgan permisos para páginas, aplicaciones, se generan códigos en caso de que el dispositivo presente bloqueo, al igual que para los computadores el software permite validar actualizaciones.

Creación de pruebas: Cuando es necesario verificar el funcionamiento de aplicaciones y afectaciones futuras a otras aplicaciones, son seleccionados equipos para realizar estas pruebas y así no afectar a toda la operación.

- **Tipos de escaneo**

Escaneo automático: El software es configurado automáticamente para que analice archivos o carpetas específicas y que ejecute un análisis completo del equipo en ciertos intervalos de tiempo.

Escaneos manuales: este tipo de escaneo es recomendado para archivos que se reciben de fuentes externas.

- **Firewall**

Un firewall o cortafuegos es un mecanismo de hardware o software que permite gestionar la totalidad de tráfico entrante y saliente entre 2 redes u ordenadores de una misma red interna y en segmentos diferentes. El tráfico entrante o saliente debe cumplir con una serie de reglas que se pueden especificar para que el tráfico pueda acceder o salir de la red u ordenador si cumple con políticas ya definidas. En caso de no cumplir las reglas el tráfico será bloqueado. Un firewall evita intrusiones no deseadas en la red u ordenadores.

El firewall se puede interpretar como un “vigilante” que permite el tráfico entre la red interna y externa o solo controla el tráfico interno desde las diferentes VLAN. Los firewall pueden ser un programa (software) o un equipo (hardware) que funcione como intermediario entre la red local y una o varias redes externas. Los principales usos de un firewall son: controlar todas las conexiones de una red, ya sea privada o pública y registrar el tráfico en la internet de una máquina con el objetivo de proteger una red informática privada impidiendo el acceso de IP´s no autorizadas y así evitar que se produzca el robo de información confidencial o la instalación de un virus en una máquina.

El firewall tiene como esencia preservar la seguridad y controlar todo el tráfico de una compañía y en Emtelco los usos principales son los siguientes:

Gestión de control de navegación para todas aquellas consultas que van hacia la internet, la gestión de control de navegación a sitios por los que se pueda compartir información (chats, correos) debido a que se manejan datos sensibles, la gestión de control de accesos a información como datos personales o bancarios, el monitoreo de ataques y del historial de navegación.

Los Tipos de firewall existentes son:

Hardware: Normalmente se encuentra instalado en el router empleado para acceder a Internet, por lo tanto sirve para proteger los ordenadores de una red que hagan uso del mismo. En este caso para una compañía el firewall se encarga de filtrar paquetes, examina el encabezado de un paquete y determina su origen y destino. Esta información es comparada con una serie de reglas que ayudan a determinar si el paquete debe ser reenviado o eliminado.

Software: Este tipo de firewall viene con el sistema operativo del ordenador por lo tanto sólo protege un equipo. Este caso es común cuando el equipo solamente se encuentra ejecutando en una máquina virtual Dropbox, VMware, etc. El firewall de software se encarga de rastrear el tráfico para bloquear aquél que no está autorizado.

En la figura 2 se ilustra la disposición de un firewall en la estructura de la red:

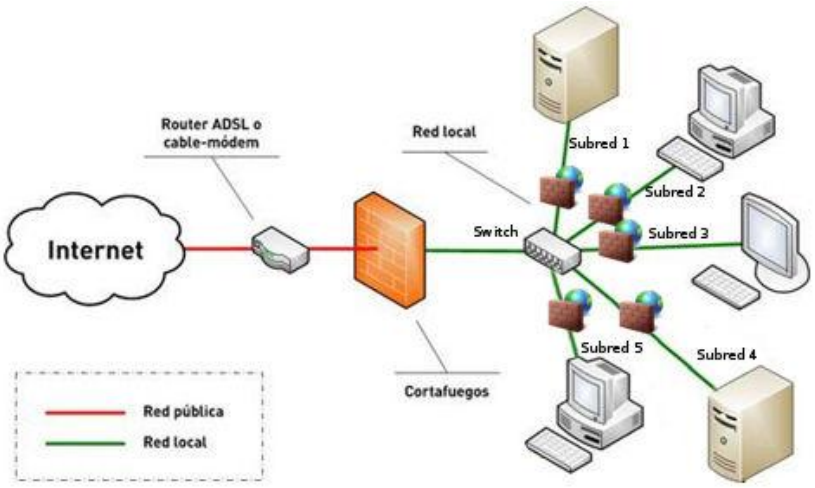

Figura 2. Ubicación del firewall en una red estándar. La imagen fue recuperada del sitio web https://geekland.eu/que-es-y-para-que-sirve-un-firewall/.

El firewall o cortafuegos se encuentran en el punto de unión entre 2 redes. En la imagen se puede observar el punto de unión de una red pública (la internet) y una red privada.

También podemos observar que cada subred dentro de la red puede tener otro firewall, y cada uno de los equipos a su vez puede tener su propio firewall por software. De esta manera, en caso de ataques podemos controlar las consecuencias y evitar que los daños de una subred se propaguen a otra. Si el tráfico cumple con las reglas que se han configurado en los firewall el tráfico podrá entrar o salir de nuestra red.

Las funciones del firewall son las siguientes:

- Administrar los accesos de los usuarios a los servicios privados de la red como aplicaciones de un servidor.
- Registrar todos los intentos de entrada y salida de una red por medio de logs.
- Filtrar paquetes por: origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.
- Filtrar por tráfico o filtrado de protocolo. Este tipo de filtro permite aceptar o rechazar el tráfico en función de protocolos como http, https, Telnet, TCP, UDP, SSH, FTP, etc.
- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que supere un determinado límite.
- Controlar las aplicaciones que tengan acceso a Internet o sea restringir el acceso a ciertas aplicaciones, como por ejemplo Dropbox, YouTube, redes sociales, etc. a un determinado grupo de usuarios.
- Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

Un firewall en principio es probable que no pueda proteger contra ciertas vulnerabilidades internas. Por ejemplo cualquier usuario puede borrar el contenido de un ordenador sin que el firewall lo evite, introducir un USB en el ordenador y robar información, etc.

Los firewall solo nos protegen frente a los ataques que atraviesen el firewall. Por lo tanto no puede repeler la totalidad de ataques que puede recibir nuestra red o servidor.

Un firewall da una sensación de seguridad falsa. Siempre es bueno tener sistemas de seguridad redundantes por si el firewall falla. Además no sirve de nada realizar una gran inversión en un firewall descuidando otros aspectos de nuestra red ya que el atacante siempre intentará buscar el eslabón de seguridad más débil para poder acceder a nuestra red. De nada sirve poner una puerta blindada en nuestra casa si cuando nos marchamos dejamos la ventana abierta.

- **Control del entorno de trabajo**

Directorio activo: El Servicio de Directorio Activo es una herramienta de Microsoft que permite la organización y gestión de recursos de una red, facilita un único inicio de sesión y un repositorio central de información para toda la infraestructura de la compañía, esto simplifica la administración de usuarios, equipos, puestos, impresoras, servidores y permisos, proporcionando además la obtención de un acceso mejorado a los recursos en red. Es un servicio de Directorio Activo, en el cual se puede resolver nombres de URL's o de determinados recursos. Las cuentas de usuarios son almacenadas en la base de datos SAM (Security Accounts Manager), el Directorio Activo también mantiene información sobre servidores, estaciones de trabajo, recursos, aplicaciones, directivas de seguridad, etc.

El directorio activo cuenta con dos funciones que durante la práctica han sido las más utilizadas: las unidades organizativas y las directivas de grupo. A continuación se procede a describir estas dos importantes funciones:

Unidades organizativas (OU): Son objetos dentro del Directorio Activo cuya función es agrupar todos los recursos lógicos de la red de la compañía, por medio de esta herramienta se pueden clasificar políticas de seguridad, permisos de administrador y gestionar la administración de los recursos. En otras palabras se delega una autoridad administrativa a usuarios, computadoras, archivos compartidos o impresoras. Al usar unidades organizativas se pueden crear contenedores dentro de un dominio que represente las estructuras jerárquicas y lógicas dentro de su organización.

Las OU permiten: disminuir el número de dominios necesarios en una red, autorizar la aplicación de directivas de seguridad y permisos administrativos a varios usuarios como uno solo por medio de grupos de navegación, usar unidades organizativas para crear un modelo administrativo que se pueda ampliar, implementar autoridad administrativa para todas las unidades organizativas de un dominio o solo para una de ellas.

El administrador de una unidad organizativa no necesita tener autoridad administrativa sobre cualquiera otra unidad organizativa del dominio.

Las OU son creadas para mostrar el organigrama específico de una empresa u organización. Desde el punto de vista de la estructura por función, las OU son hechas de acuerdo con las diferentes funciones que la empresa tenga internamente sin importar el lugar en donde se encuentren los empleados. Es importante aclarar que la estructura refleja los diferentes países o ciudades donde la organización se encuentra. En la actualidad la estructura híbrida es la más utilizada en las empresas.

Directiva de grupo (GPO)

Al igual que las unidades organizativas, la directiva de grupo es un objeto dentro del Directorio Activo que permite a través de un conjunto de reglas controlar el entorno de trabajo o configuraciones específicas a cuentas de usuario y cuentas de equipo. La directiva de grupo proporciona una gestión centralizada y configuración de sistemas operativos, aplicaciones o configuración de los usuarios. La Directiva de Grupo controla lo que los usuarios pueden y no pueden realizar en un sistema informático como acceso a un disco duro o limitar el tamaño que pueda tener un archivo. La GPO permiten: restringir el acceso a carpetas, bloquear el acceso al administrador de tareas, establecer el título del explorador de internet, ocultar el panel de control, deshabilitar el uso de regedit.exe y regedt32.exe y establecer qué paquetes se pueden instalar en un equipo.

- **Vulnerabilidades**

Contraseñas predeterminadas: esta vulnerabilidad se da comúnmente por dejar contraseñas en blanco o usar las predeterminadas por el fabricante, estas están asociadas a hardware a redes y dispositivos de almacenamiento.

Llaves compartidas: Los usuarios que no cambian sus llaves se someten a que cualquiera que tenga esta llave compartida tenga acceso a la información confidencial que tenga pues los servicios generalmente empaquetan las llaves con propósitos de desarrollo y evaluación.

Suplantación de IP: las maquinas remotas actúan como nodos en las redes locales y encuentran vulnerabilidades en los servidores e instalan un programa para obtener el control sobre los recursos de la red. Esta suplantación es un método complicado ya que el atacante debe predecir los numero de secuencia TCP/IP para controlar la conexión los sistemas destinados.

Interceptación pasiva: Se recolectan datos que pasan entre dos nodos de red interceptando pasivamente la conexión entre los nodos. Este ataque funciona mediante protocolos de transmisión de texto plano como FTP, HTTP o Telnet.

Vulnerabilidad de servicio: El atacante busca una falla en los servicios de red comprometiendo el sistema y los datos que este pueda contener, los servicios más vulnerables son los basados en HTTP mediante la ejecución de comandos remotos.

Vulnerabilidad de aplicaciones: estas vulnerabilidades son más propensas a encontrarse en el escritorio o aplicaciones de trabajo que ejecutan un código arbitrario, es necesario informar a los usuarios de los riesgos que se corren al instalar software no autorizado o cuando se abren correos no solicitados.

8. Conclusiones

Es importante efectuar un ejercicio de vigilancia tecnológica en temas de seguridad informática, ya que es un proceso continuo que exige capacitación, concientización y buenas prácticas tanto de los profesionales encargados del área de informática, como de los empleados de las diferentes secciones de Emtelco.

Con la planificación de nuevos ataques, Emtelco debe priorizar los elementos asociados a la seguridad informática: la empresa no se puede dar el lujo de considerar la seguridad informática como un proceso secundario, por lo tanto es necesario mantener la atención en las vulnerabilidades, su evolución tecnológica, y la aplicación juiciosa de las auditorías, para así encontrar las herramientas adecuadas para hacer frente a los ataques.

Las aplicaciones de seguridad informática suelen concentrarse en gran medida, alrededor de las constantes copias de seguridad que se generan en la empresa, lo cual implica que se deben aunar esfuerzos para garantizar que los equipos de cómputo y de red tengan instalados las últimas actualizaciones de sus sistemas operativos y antivirus, y limitar sensiblemente la descarga e instalación de programas de sitios web que no sean de confianza, y que no se encuentren autorizados.

Se sugiere que las capacitaciones efectuadas por la empresa para los funcionarios del área de tecnología, sean debidamente socializadas y compartidas con los practicantes, con la finalidad de incorporar las competencias y destrezas aprendidas en las actividades de la unidad.

Es importante para abordar las necesidades en tecnologías de la seguridad en informática que requiere la empresa, contar con un talento humano más numeroso y robusto que esté en capacidad de abordar diversas temáticas especializadas en seguridad, que muy difícilmente pueden ser manejadas por un pequeño grupo de personas.

9. Referencias

Firma – E. (2019). Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad. Recuperado el mes de mayo del sitio web https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

Equipo de Expertos (s.f.). ¿Qué es la seguridad informática y cómo puede ayudarme?. Recuperado el mes de mayo del sitio https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Lin-o1 Wiki (s.f.). Vulnerabilidad en redes. Recuperado del sitio https://lin01.fandom.com/es/wiki/vulnerabilidad_en_redes

Velasco, R. (2018). Conoce estos escáneres de vulnerabilidades para auditar la seguridad de otras aplicaciones. Recuperado del sitio https://www.redeszone.net/2018/12/01/escaneres-vulnerabilidades-auditar-software/

Tuyu, Tech. (2017). Importancia de la seguridad informática en las empresas. Recuperado del sitio https://www.tuyu.es/importancia-seguridad-informatica/

Aguiló, C.; Aguilera, J. et al. (s.f.). Resumen de Seguridad Informatica. Recuperado del sitio https://sites.google.com/site/resumendediapositivas/resumen-de-seguridad-informatica

Álvares, L.D. (2005). Trabajo de grado: Seguridad en informática (Auditoría de sistemas). México: Universidad Iberomaericana. Recuperado del sitio http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Instituciones (s.f.). Metodología para la gestión de la seguridad informática. Recuperado del sitio https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf